



**IMPLEMENTATION GUIDANCE FOR 10 CFR PART 37 PHYSICAL PROTECTION OF
BYPRODUCT MATERIAL CATEGORY 1 AND CATEGORY 2 QUANTITIES OF
RADIOACTIVE MATERIAL**

Manuscript Completed:

Date Published:

Prepared by

E. Bowden-Berry, M. Cervera, P. Goldberg, S. Hawkins, M. Horn, K. Jamgochian, R. MacDougall, D. Piskura, G. Purdy, R. Ragland, N. St. Amour, F. Sturz, and G. Warren

Division of Materials Safety and State Agreements

Office of Federal and State Materials and Environmental Management Programs

U.S. Nuclear Regulatory Commission

Washington, DC 20555-0001

ABSTRACT

This technical report contains information intended to provide guidance and assist applicants and licensees in implementing Title 10 *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." This document describes the methods acceptable to the United States Nuclear Regulatory Commission (NRC) in implementing the regulations.

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 numbers 3150-~~xxxx~~.

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.

TABLE OF CONTENTS

ABSTRACT	i
ACKNOWLEDGMENTS	iv
ACRONYMS AND ABBREVIATIONS	v
PURPOSE OF REPORT	1
<u>Subpart A – General Provisions</u>	2
§ 37.1 <u>Purpose</u>	2
§ 37.3 <u>Scope</u>	4
§ 37.5 <u>Definitions</u>	6
§ 37.7 <u>Communications</u>	26
§ 37.9 <u>Interpretations</u>	27
§ 37.11 <u>Specific exemptions</u>	28
§ 37.13 <u>Information collection</u> requirements: OMB approval	33
<u>Subpart B – Background Investigations and Access Authorization Programs</u>	34
§ 37.21 <u>Personnel access authorization</u> requirements for category 1 or category 2 quantities of radioactive material	34
§ 37.23 <u>Access authorization program requirements</u>	44
§ 37.25 <u>Background investigations</u>	65
§ 37.27 <u>Requirements for criminal history records checks</u> of individuals granted unescorted access to category 1 or category 2 quantities of radioactive material	79
§ 37.29 <u>Relief from fingerprinting, identification, and criminal history records</u> <u>checks</u> and other elements of background investigations for designated categories of individuals permitted unescorted access to certain radioactive materials or other property	90
§ 37.31 <u>Protection of information</u>	98
§ 37.33 <u>Access authorization program review</u>	105
<u>Annex A: Additional Guidance for Evaluating an Individual’s Trustworthiness and</u> <u>Reliability for Allowing Unescorted Access to Certain Radioactive Material</u> ...	108
<u>Annex B: Sample Consent Form for Background Investigations</u>	112
<u>Subpart C – Physical Protection Requirements During Use</u>	114
37.41 <u>Security program</u>	114
37.43 <u>General security program requirements</u>	122

37.45	LLEA coordination and notification	145
37.47	Security zones	156
37.49	Monitoring, detection, and assessment	168
37.51	Maintenance and testing	183
37.53	Requirements for mobile devices	189
37.55	Security program review	196
37.57	Reporting of events	199
	Annex C Examples of Reportable Suspicious Activities under § 37.57(b)	206
Subpart D – Physical Protection in Transit		208
37.71	Additional requirements for transfer of category 1 and category 2 quantities of radioactive material	208
37.73	Applicability of physical protection of category 1 and category 2 quantities of radioactive material during transit	213
37.75	Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material	217
37.77	Advance notification of shipment of category 1 quantities of radioactive material	226
37.79	Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment	237
37.81	Reporting of events	255
	Annex D Template for Advance Notifications of Shipments of Category 1 Quantities of Radioactive Material under § 37.77(b)	267
Subpart E – [Reserved]		269
Subpart F – Records		270
37.101	Form of records	270
37.103	Record retention	271
Subpart G – Enforcement		272
37.105	Inspections	272
37.107	Violations	273
37.109	Criminal penalties	275
Appendix A – Category 1 and Category 2 Radioactive Materials		276

ACKNOWLEDGMENTS

The working group thanks the individuals listed below for assisting in the review and update of the report. All participants provided valuable insights, observations, and recommendations.

Nuclear Regulatory Commission Staff

Bowden-Berry, Elva
Cervera, Margaret
Goldberg, Paul
Hawkins, Sarenee
Horn, Merri
Jamgochian, Kris
MacDougall, Robert
Piskura, Deborah
Purdy, Gary
Ragland, Robert
St. Amour, Norman
Sturz, Frederick
Warren, Geoffrey

Organization of Agreement States

Harris, James (Kansas Department of Health and Environment)
James, Stephen (Ohio Department of Health)

Conference of Radiation Control Program Directors

Costello, Frank (Pennsylvania Department of Health)
Dansereau, Robert (New York State Health Department)

Acronyms and Abbreviations

AEA	Atomic Energy Act of 1954, as amended
ALARA	as low as reasonably achievable
Am	americium
Bq	Becquerel
CFR	Code of Federal Regulations
Ci	Curie
CHRI	Criminal history records information
CIS	U.S. Customs and Immigration Services
Cs	cesium
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
EPAct	Energy Policy Act of 2005
FAST	Customs and Border Patrol's Free and Secure Trade
FBI	Federal Bureau of Investigation
ft	feet
g	grams
HR	Human Resources
IAEA	International Atomic Energy Agency
IC	Increased Controls
IDS	intrusion detection system
Kg	kilogram
lb	pound
LLEA	local law enforcement agency
LVS	License Verification System
M&D	Manufacturing and Distribution
MOU	Memorandum of Understanding
NAC	National Agency Check
NLT	no-later-than
NRC	U.S. Nuclear Regulatory Commission
OMB	Office of Management and Budget
Pdf	portable document format
PII	Personally Identifiable Information

Q&As	questions and answers
RDD	radiation dispersion device
RED	radiation exposure device
RO	reviewing official
RSO	radiation safety officer
SIG	Safeguards Information
SIG-M	Safeguards Information – Modified Handling
T&R	trustworthiness and reliability
TBq	Terabecquerels
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credentials
UPS	United Parcel Service

PURPOSE OF REPORT

This document provides guidance to a licensee or applicant for implementation of Title 10 *Code of Federal Regulations* (10 CFR) Part 37, “Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material.” It is intended for use by applicants, licensees, and U.S. Nuclear Regulatory Commission (NRC) staff, and will also be available to Agreement States. The approaches and methods described in this document are not requirements, but are provided for information only. Methods and solutions different from those described in this document are acceptable if they meet the requirements of Part 37, and licensees are free to propose alternative ways of demonstrating compliance with these requirements.

The guidance in this document is provided in the form of questions and answers (Q&As) for each section (and as applicable, subsection) of the regulation. Except for definitions under § 37.5, the section reference and associated text appear in the box at the top of the page that begins each set of Q&As, and a brief explanation of the rule text follows just below the box. The Q&As that follow are designed to provide guidance on implementation of the rule language in the box. Questions and answers are provided for those definitions that are specific to Part 37.

If you are reading an electronic version of this guidance document, you may navigate more easily by clicking on the hyperlinks for each section listed in the Table of Contents. Hyperlinks also appear in responses to the questions to enable you to go directly to source material or sections of rule text referenced in the response.

Certain States, called Agreement States, have entered into agreements with the NRC that give them the authority to license and inspect byproduct, source, and special nuclear materials, in quantities not sufficient to form a critical mass, which are used or possessed within their borders. Any licensee or applicant, other than a Federal entity, who wishes to possess or use licensed material in one of these Agreement States should contact the responsible officials in that State for guidance on implementing the security provisions.

SUBPART A – GENERAL PROVISIONS

§ 37.1 Purpose.

§ 37.3 Scope.

§ 37.5 Definitions.

§ 37.7 Communications.

§ 37.9 Interpretations.

§ 37.11 Specific exemptions.

§ 37.13 Information collection requirements: OMB approval.

§ 37.1 Purpose

This part has been established to provide the requirements for the physical protection program for any licensee that possesses an aggregated category 1 or category 2 quantity of radioactive material listed in Appendix A to this part. These requirements provide reasonable assurance of the security of category 1 or category 2 quantities of radioactive material by protecting these materials from theft or diversion. Specific requirements for access to material, use of material, transfer of material, and transport of material are included. No provision of this part authorizes possession of licensed material.

EXPLANATION:

These regulations establish the security requirements for the possession and use, transfer, and transportation of aggregated category 1 and category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: What is the purpose of Part 37?

A1: Part 37 imposes security requirements for the possession and use of category 1 and category 2 quantities of radioactive material. Part 37 establishes the objectives and minimum requirements that licensees must meet to protect against theft or diversion. These requirements are intended to protect the public against the unauthorized use of a category 1 or category 2 quantity of radioactive material by reducing the risk of the theft or diversion of the material.

Q2: What is a category 1 or category 2 quantity of radioactive material?

A2: Category 1 and category 2 quantities of radioactive material are considered to be risk-significant, and refer specifically to 16 radioactive materials (14 single radionuclides

and 2 combinations). These materials are: americium-241; americium-241/beryllium; californium-252; curium-244; cobalt-60; cesium-137; gadolinium-153; iridium-192; plutonium-238; plutonium-239/beryllium; promethium-147; radium-226; selenium-75; strontium-90 (yttrium-90); thulium-170; and ytterbium-169. Irradiated fuel and mixed oxide fuel are not included even though they may contain category 1 or category 2 quantities of radioactive material; these materials are covered by other regulations. The thresholds for category 1 and category 2 quantities of radioactive material are provided in Table 1 of [Appendix A](#) of Part 37.

Q3: How do I know when I have an “aggregated” quantity of this radioactive material?

A3: See Q&As related to the definition of “aggregated” under [§37.5, Definitions](#), and [§ 37.47, Security Zones](#).

Q4: What does it mean to say that “No provision of this Part authorizes possession of licensed material?”

A4: This sentence simply clarifies that Part 37 only establishes requirements for the security of category 1 or category 2 quantities of radioactive material. These requirements are separate from the requirements for the issuance of a license to possess these quantities of radioactive material. Generally-applicable requirements for issuance of a license to possess byproduct material are established in Part 30, and required conditions for issuance of licenses for specific uses of byproduct material are in Parts 31 through 36 and Part 39. Similarly, generally-applicable requirements for the issuance of licenses to possess special nuclear material are in Part 70. The list of radioactive materials of concern in Appendix A of Part 37 contains radioisotopes typically licensed under both Parts 30 and 70. Part 37 does not relieve licensees from compliance with these Parts. Part 37 merely establishes additional requirements for the secure possession of a category 1 or category 2 quantity of these materials.

Q5: I’m a mobile radiographer licensed to possess 60-curie sources of iridium. These sources cannot easily be made into a weapon, and there are many better and more easily accessible choices for making a radiation dispersion device (RDD) or a radiological exposure device (RED). Why do I have to have a security program to secure this low-risk source?

A5: The NRC has determined that the category 2 thresholds for the radioisotopes listed in Appendix A to Part 37, including iridium-192, are the levels that warrant additional protection measures. In addition, The Radiation Source Protection and Security Task Force, an interagency task force established by the Energy Policy Act of 2005 (EPAAct), concluded in its 2006 report to Congress and the President (ADAMS accession number ML062190349) that the appropriate radioactive sources were being protected. The Task Force also concluded that the International Atomic Energy Agency (IAEA) Code of Conduct serves as an appropriate framework for considering which sources warrant additional protection. For its 2010 report to Congress and the President (ADAMS accession number ML102230141), the Task Force conducted a reevaluation of the list of radionuclides that warrant additional security and protection. The Task Force found “that the Category 1 and 2 quantities remain valid for sealed and unsealed sources as the list and threshold levels of radionuclides that could result in a significant RED or RDD event and therefore warrant enhanced security and protection.”

§ 37.3 Scope

§ 37.3(a)

Subparts B and C of this part apply to any person who, under the regulations in this chapter, possesses or uses at any site, an aggregated category 1 or category 2 quantity of radioactive material.

EXPLANATION:

This section establishes which licensees are subject to Subparts B and C.

QUESTIONS/ANSWERS:

Q1: Who is covered by Subpart B, “Background Investigations and Access Authorization Program” and Subpart C, “Physical Protection Requirements During Use?”

A1: Subpart B and Subpart C requirements apply to any licensee that possesses or uses an aggregated¹ category 1 or category 2 quantity of radioactive material at any site. This includes a wide range of licensees, including pool-type irradiator licensees; manufacturer and distributor licensees; medical facilities with gamma stereotactic radiosurgery devices; self-shielded irradiator licensees (including blood irradiators); teletherapy unit licensees; radiographers; well loggers; broad scope users; radioisotope thermoelectric generator licensees; fuel cycle licensees; research and test reactors; commercial power reactors; some fixed gauge licensees; and licensees that ship or prepare for shipment a category 1 or category 2 quantity of radioactive material. For additional Q&As on the applicability of Subpart B, see those on [§ 37.21](#). For additional Q&As on the applicability of Subpart C, see those on [§ 37.41\(a\)](#).

Q2: Do Part 37 requirements apply to unsealed radioactive material as well as material sealed in a source or device? For example, do the requirements apply to materials possessed by a nuclear laundry or radioactive waste processor?

A2: Yes. Part 37 applies to both sealed and unsealed radioactive materials in quantities equal to or greater than category 2. There is no distinction between unsealed and sealed radioactive material when implementing Part 37 requirements. A nuclear laundry or radioactive waste processing licensee, for example, must implement these requirements if it possesses radioactive material in an aggregated quantity that meets or exceeds a category 2 threshold.

Q3: How do I determine whether Part 37 applies to me?

A3: See Q&As related to the definition of “aggregated” and category 1 and category 2 quantities of radioactive material under [§37.5, Definitions](#), and [§ 37.47, Security Zones](#).

¹ As defined in § 37.5 below, “aggregated” means 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.

§ 37.3 Scope

§ 37.3(b)

Subpart D applies to any person who, under the regulations of this chapter:

- (1) Transports or delivers to a carrier for transport in a single shipment, a category 1 or category 2 quantity of radioactive material; or
- (2) Imports or exports a category 1 or category 2 quantity of radioactive material; the provisions only apply to the domestic portion of the transport.

EXPLANATION:

This section establishes which licensees and activities are subject to Subpart D.

QUESTIONS/ANSWERS:

Q1: Who is covered by Subpart D, Physical Protection in Transit?

A1: Subpart D requirements apply to any licensee that transports or delivers to a carrier for transport a category 1 or category 2 quantity of radioactive material. A licensed importer or exporter of this material must comply with Subpart D and other applicable requirements of Part 37 only for the portion of the shipment carried out within the borders of the United States or its territories.

Q2: Are there any modes of transportation not covered by Part 37?

A2: Yes. Part 37 does not address air or water transport. Transport of radioactive material within airports and by air is regulated by the Federal Aviation Administration. Transport of radioactive material within ports and by waterway is regulated by the U.S. Coast Guard.

The rule also does not address transshipments of category 1 or category 2 quantities of radioactive material through the United States. Transshipments are shipments that originate in a foreign country, pass through the United States, and then continue on to another country.

The rule does not address transport of spent fuel except in quantities of 100 grams (g) (0.22 pounds (lb)) or less in net weight, exclusive of cladding or other structural or packaging material, and that have a total external radiation dose rate in excess of 1 Gray (100 rad) per hour at a distance of 1 m (3.3 feet (ft)) from any accessible surface without intervening shielding. Transportation of larger quantities of spent fuel is covered by Part 73, which establishes requirements under [§ 73.37](#) that apply to the transport of spent fuel quantities in excess of 100 g that exceed the 1-Gray/hour dose rate.

§ 37.5 Definitions

As used in this part:

Access control means 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.

QUESTIONS/ANSWERS:

Q1: Does this definition of access control also cover individuals with access to safeguards information-modified handling (SGI-M)?

A1: No. This definition covers only the control of access to security zones, which are defined below as 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. A licensee's access control program under Part 37 is not required to include SGI. Although similar, the requirements for access to radioactive materials under Part 37 are not the same as the requirements under Part 73 for access to SGI-M ([§ 73.23](#)).

Q2: Does an individual who complies with Part 37 requirements for unescorted access to radioactive material automatically comply with Part 73 requirements for authorized access to SGI or SGI-M?

A2: No. As noted in response to Q.1 above, the requirements for access to radioactive materials under Part 37 are not the same as the requirements for access to SGI or SGI-M under Part 73. Therefore, an individual who complies with the requirements for unescorted access to radioactive materials under Part 37 does not automatically comply with the requirements for access to SGI or SGI-M. However, licensees may use the information developed from background investigations for unescorted access to radioactive material to determine the trustworthiness and reliability of an individual for access to SGI-M, and *vice versa*.

Act means the Atomic Energy Act of 1954 (68 Stat. 919), including any amendments thereto.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Aggregated means 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.

QUESTIONS/ANSWERS:

Q1: Does the definition of aggregated include unsealed sources and bulk material?

A1: Yes. The definition includes radioactive material “in any form.” The intent is to include all material whether it is in the form of a source (sealed or unsealed) or is in a container of some sort, such as feed material that might be used to create a source.

Q2: If I have one source with radioactive material that equals or exceeds a category 2 quantity, is that source considered “aggregated” under this definition, even if I possess no other radioactive materials?

A2: Yes. Even if your source is inside a device, it must be considered aggregated under this definition because it contains a category 2 or greater quantity of material that is accessible by the breach of a single physical barrier.

Q3: What is a physical barrier?

A3: Under [§ 37.47\(c\)\(1\)](#), a physical barrier is a natural or man-made structure or formation sufficient for the isolation of a category 1 or category 2 quantity of radioactive material within a security zone.

Q4: How does the term “bulk material” in NRC’s definition of “aggregated” align with the U.S. Department of Transportation’s (DOT’s) terminology for bulk packaging?

A4: The two terms are unrelated. The DOT regulation using this terminology applies only to the packaging and transportation of bulk material, not the radiation safety or security of the material itself. NRC considers bulk material to be radioactive material that is not a discrete source or a sealed source as these terms are defined in 10 [CFR 30.4](#). Bulk material is radioactive material that is not encased in a capsule designed to prevent leakage or escape of the material.

Q5: Does the “total activity” in the definition of aggregated refer to the activity of all the radioactive material the licensee possesses, or just the activity that would be accessible by the breach of a single physical barrier?

A5: “Total activity” in this definition refers only to the activity of the radioactive material that would be accessible by the breach of a single physical barrier. A licensee may possess quantities of radioactive material with a total activity several times greater than the category 2 threshold, but a category 2 or greater quantity is considered “aggregated” only if it is located within an area isolated by a single physical barrier. Material with radioactivity in category 2 quantities or greater may be used or stored by the licensee at several locations and not be considered aggregated as long as access to each location is controlled by at least one physical barrier.

Q6: When I’m storing radioactive material, does the phrase “physical barrier” used in the definition of “aggregated” apply to each storage container, or to the area within which I’m storing these containers? May I count each drum as an independent physical barrier so that all the drums together need not be considered aggregated?

A6: The answer to this question depends on the circumstances, including the quantity of radioactive material inside the storage containers. If a storage container

contains a category 2 quantity of radioactive material, the concept of physical barrier is not a factor as Part 37 would apply. The security zone established could be an area surrounding the single drum. If you have several drums that contain radioactive material, the material in all of the drums would be added together to determine if you have a category 2 or greater quantity. The drums by themselves should not be considered a physical barrier because the material could easily be removed from the security zone by tipping the drums over and rolling them to an unsecured location. Thus, without additional barriers, material stored together in individual drums would be considered aggregated, and if you have a category 2 or greater quantity, Part 37 would apply. If the lids to the drums are secured (e.g., padlocked or welded), however, and the drums are individually secured to the floor with bolts, chains, or cables to prevent them from being easily removed, the sources would not be considered aggregated and Part 37 would not apply.

Q7: When I'm storing a category 2 or greater quantity of radioactive material in the form of multiple mobile devices inside a locked storage container or storage area, can each of these devices be considered a "physical barrier" under the definition of "aggregated?" If so, would the devices within that locked container or storage area be considered protected by at least two "independent physical controls" and meet the additional security requirement for mobile devices under § 37.53(a)?

A7: The answer to both questions is no. The definition of "aggregated" specifically covers a category 2 or greater quantity of radioactive material "in any form, *including any devices that contain the radioactive material* [emphasis added]." The devices themselves cannot be considered independent physical controls because, for the purpose of unauthorized removal, access to a mobile device is effectively access to the material inside the device. In this case, the "physical barrier" in the definition of "aggregated" is the locked container, or the locked room or cage surrounding the area within which you're storing these mobile devices. If this locked container, room, or cage is the only physical barrier to gaining access to the category 2 or greater quantity of material in the devices, this material is "aggregated" under this definition, and under § 37.53(a), the devices must be protected by at least one additional independent physical control when they are not under the direct control and constant surveillance of the licensee.

Q8: When I'm transporting several devices that individually are less than a category 2 quantity, but together are more than that, does the phrase "physical barrier" used in the definition of "aggregated" apply to each device, or only to the shipping container I use to transport the devices? Can I count the individual devices containing the material as barriers along with the shipping container, so that I would have more than one physical barrier and the shipment would not have to be considered aggregated?

A8: No. The concept of physical barriers does not apply to transportation. If someone steals a truck transporting sources, he or she would have access to all of the material regardless of any shipping container barriers. If you are transporting a category 2 or greater quantity of material in a single conveyance, the requirements of Subpart D apply.

Q9: If I conduct my licensed operations on a sufficiently large site, can I use the physical distance between the locations of my devices or materials as a physical barrier, so that I would not have to consider them aggregated?

A9: Yes, but the necessary physical distance separating the locations where materials and/or devices are used or stored will vary for each licensee, and the burden will be on you as the licensee or license applicant to show that this distance is sufficient to qualify as a physical barrier. To demonstrate compliance, you would probably need to consider such site-specific factors as: whether the devices are continuously monitored, or so integrated into the facility's operation that the removal of a device would provoke a prompt investigation and response; the ease of moving your materials and/or devices; the availability of tools and equipment, including vehicles, to accomplish this movement; the likely minimum travel time from location to location; and the delay associated with these factors compared to the delay afforded by alternative physical barriers such as a lock and chain or a lockable cage or room. To avoid unanticipated delays or changes in your plans or operations, you should consult your regulatory agency in advance about your intent to use physical distance as a physical boundary, rather than waiting for an inspection to identify the issue. You should also keep in mind that physical distance would not count as a physical barrier during times when sources are removed from their devices for maintenance or replacement and aggregated within a common physical barrier for temporary storage.

Q10: How far apart must my devices or materials be located for them not to be considered "aggregated?"

A10: No single minimum distance between locations of materials or devices can or should be prescribed in a regulation applied to all licensees' situations. As noted in the preceding Q&A, you will have to identify the minimum distance you believe should be counted as a physical barrier based on an analysis of site-specific conditions. The analysis will be subject to NRC inspection.

Agreement State means any state with which the Atomic Energy Commission or the Nuclear Regulatory Commission has entered into an effective agreement under subsection 274b. of the Act. *Non-agreement State* means any other State.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Approved individual means an individual whom the licensee has determined to be trustworthy and reliable for unescorted access in accordance with subpart B of this part and who has completed the training required by § 37.43(c).

QUESTIONS/ANSWERS:

Q1: Is an individual approved for access to radioactive materials automatically also approved for access to SGI or SGI-M as well?

A1: No. To be approved for access to SGI or SGI-M, such an individual would have to meet applicable requirements of Part 73 and have a need to know safeguards information to perform his or her duties. Similarly, an individual approved for access to SGI or SGI-M would also need to have access to category 2 or greater quantities of

radioactive material to perform job-related duties in order to be approved for unescorted access to these materials.

Q2: Who approves an “approved individual?”

A2: The rule requires a reviewing official (RO) designated by the affected licensee to approve an individual for unescorted access to category 1 or category 2 quantities of radioactive material. The RO must determine that the individual seeking such access is trustworthy and reliable before granting that individual unescorted access. See definition of “reviewing official” below.

Q3: What does it mean to be “trustworthy and reliable”?

A3: See definition of “trustworthiness and reliability” below, and Q&As pertaining to [§ 37.25](#), *Background Investigations*.

Q4: What does it mean to “complete” the training required by [§ 37.43\(c\)](#)? Does an individual have to pass a test to have successfully “completed” the training?

A4: No. Testing is not required, but evidence that the trainee took and passed a reasonable test of the knowledge, skill, or ability objectives of the training is one possible measure of the likelihood that a trainee will be able to carry out his or her assigned security responsibilities. No individual subject to the training requirements may be permitted unescorted access to a category 1 or category 2 quantity of radioactive material before completing the training requirements appropriate for that individual’s potential job responsibilities, however. See Q&As for [§ 37.43\(c\)](#).

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

QUESTIONS/ANSWERS:

See Q&As for [§ 37.25](#), *Background Investigations*.

Becquerel (Bq) means one disintegration per second.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Byproduct material means—(1) Any radioactive material (except special nuclear material) yielded in, or made radioactive by, exposure to the radiation incident to the process of producing or using special nuclear material;

(2) The tailings or wastes produced by the extraction or concentration of uranium or thorium from ore processed primarily for its source material content, including discrete surface wastes resulting from uranium solution extraction processes. Underground ore bodies depleted by these solution extraction operations do not constitute “byproduct material” within this definition;

(3)(i) Any discrete source of radium-226 that is produced, extracted, or converted after extraction, before, on, or after August 8, 2005, for use for a commercial, medical, or research activity; or

(ii) Any material that—

(A) Has been made radioactive by use of a particle accelerator; and

(B) Is produced, extracted, or converted after extraction, before, on, or after August 8, 2005, for use for a commercial, medical, or research activity; and

(4) Any discrete source of naturally occurring radioactive material, other than source material, that—

(i) The Commission, in consultation with the Administrator of the Environmental Protection Agency, the Secretary of Energy, the Secretary of Homeland Security, and the head of any other appropriate Federal agency, determines would pose a threat similar to the threat posed by a discrete source of radium-226 to the public health and safety or the common defense and security; and

(ii) Before, on, or after August 8, 2005, is extracted or converted after extraction for use in a commercial, medical, or research activity.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Carrier means a person engaged in the transportation of passengers or property by land or water as a common, contract, or private carrier, or by civil aircraft.

QUESTIONS/ANSWERS:

Q1: Can a licensee be a carrier?

A1: Yes. Any person as defined in [10 CFR 30.4](#), including a corporation, may engage in transportation of radioactive materials as a common, contract, or private carrier.

Q2: What's the difference between a "carrier" and a "transporter," a term also used in this rule?

A2: There is none. For the purposes of this Part, the NRC uses the terms interchangeably.

Category 1 quantity of radioactive material means a quantity of radioactive material meeting or exceeding the category 1 threshold in Table 1 of Appendix A to this part. This is determined by calculating the ratio of the total activity of each radionuclide to the category 1 threshold for that radionuclide and adding the ratios together. If the sum is equal to or exceeds 1, the quantity would be considered a category 1 quantity. Category 1 quantities of radioactive material do not include the radioactive material contained in any fuel assembly, subassembly, fuel rod, or fuel pellet.

Category 2 quantity of radioactive material means a quantity of radioactive material meeting or exceeding the category 2 threshold but less than the category 1 threshold in Table 1 of Appendix A to this part. This is determined by calculating the ratio of the total activity of each radionuclide to the category 2 threshold for that radionuclide and adding the ratios together. If the sum is equal to or exceeds 1, the quantity would be considered a category 2 quantity. Category 2 quantities of radioactive material do not include the radioactive material contained in any fuel assembly, subassembly, fuel rod, or fuel pellet.

QUESTIONS/ANSWERS:

Q1: How do I determine whether I possess a category 1 or category 2 quantity of radioactive material?

A1: Use the sum-of-the-fractions method, also known as the unity rule, to determine whether you possess a category 1 or category 2 quantity of radioactive material. You may need to implement Part 37 requirements even if you do not possess any single source or single radionuclide in excess of a category 2 threshold. For combinations of materials (including sealed sources, unsealed sources, and bulk material) and radionuclides, you must include multiple sources (including bulk material) of the same radionuclide and multiple sources (including bulk material) of different radionuclides to determine if the requirements apply. For the purposes of this calculation, you are required to consider all of the radioactive material you possess at the site in question. To determine whether you're required to implement the Part 37 requirements, you may use the following formula for the unity rule:

$$R_1/AR_1 + R_2/AR_2 + R_n/AR_n \geq 1.0$$

Where R_1 = total amount of radionuclide 1, AR_1 = category 2 threshold of radionuclide 1, R_2 = total amount of radionuclide 2, AR_2 = category 2 threshold of radionuclide 2, R_n = total amount of radionuclide n, AR_n = category 2 threshold of radionuclide n, etc. ≥ 1.0 .

If the sum of these fractions is greater than or equal to 1, you possess at least a category 2 quantity of radioactive material, and the 10 CFR Part 37 requirements would apply if this quantity is aggregated in a single location.

To determine whether you have a category 1 quantity for purposes of implementing Part 37 requirements for the transport of such quantities, you would use the same unity rule formula above, but substitute the category 1 threshold value as the divisor for each radionuclide to be shipped. Category 1 thresholds in Appendix A are 100 times the thresholds for category 2 quantities.

The Terabecquerel (TBq) thresholds are the regulatory standard and need to be used in all unity rule calculations. You must therefore convert any Curie (Ci) values in your license for sources and material to TBq as follows:

$$n \text{ (TBq)} = N \text{ (Ci)} \times 0.037 \text{ TBq/Ci.}$$

Below are several examples.

Example 1: The licensee possesses:

5 TBq Co-60 (bulk material)
5 TBq Co-60 (sealed source)
20 TBq Ir-192 (sealed source)

The category 2 threshold for Co-60 is 0.3 TBq and for Ir-192 is 0.8 TBq. Using the sum of fractions formula: $R_1/AR_1 + R_2/AR_2 + R_n/AR_n \geq 1.0$, and dividing the total quantities of Co-60 and Ir-192 by their category 2 threshold quantities, the sum of the fractions is 58 ((5TBq Co-60 + 5TBq Co-60)/0.3 TBq + (20 TBq Ir-192/0.80 TBq) = 58.)

Because this sum is greater than 1, Part 37 requirements apply to this licensee. At a minimum, the licensee must apply the Part 37 requirements to the Co-60 and Ir-192 sources because each source individually is considered a category 2 quantity. Depending on the location of the Co-60 in bulk form, the licensee may need to apply Part 37 requirements if that bulk material is stored with either source, or if all of the bulk material is stored together at one location surrounded by one physical barrier. But if the bulk material is stored in several locations, such that each location contained less than 0.3 TBq and there is a physical barrier between locations, Part 37 requirements would not apply to the bulk material.

Example 2: The licensee possesses:

3 TBq Sr-90 (bulk material)
0.5 TBq Cs-137 (sealed source)
0.1 TBq Am-241 (bulk material)

The category 2 threshold is 10 TBq for Sr-90, 1 TBq for Cs-137, and 0.6 TBq for Am-241. Using the sum of fractions formula: $R_1/AR_1 + R_2/AR_2 + R_n/AR_n \geq 1.0$, and dividing the total quantities of Sr-90 and Cs-137 by their category 2 threshold quantities, the sum of the fractions is 0.97 ((3 TBq Sr-90/10 TBq) + (0.5 TBq Cs-137/1 TBq) + (0.1 TBq Am-241/0.6 TBq) = 0.97.)

Because this sum is less than 1, Part 37 does not apply to this licensee.

Example 3: The licensee possesses:

0.5 TBq Cs-137 (unsealed source)
0.3 TBq Am-241 (sealed source)

The category 2 threshold for Cs-137 is 1 TBq and 0.3 TBq for Am-241. Using the sum of fractions formula: $R_1/AR_1 + R_2/AR_2 + R_n/AR_n \geq 1.0$, and dividing the total quantities of Cs-137 and Am-241 by their category 2 threshold quantities, the sum of the fractions is 1 ((0.5 TBq Cs-137/1 TBq) + (0.3 TBq Am-241/0.6 TBq) = 1.)

Because this sum equals 1, Part 37 requirements may apply. If the two sources are stored together, Part 37 applies. If the licensee stores the sources apart, each protected by at least one independent physical barrier, Part 37 does not apply. See also Q&As for definition of "[Aggregated](#)."

Commission means the Nuclear Regulatory Commission or its duly authorized representatives.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Curie means that amount of radioactive material which disintegrates at the rate of 37 billion atoms per second.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

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

QUESTIONS/ANSWERS:

Q1: What's the difference between diversion and theft?

A1: Both diversion and theft involve the unauthorized movement of radioactive material to an unauthorized destination. When an adversary is actively transporting an offsite shipment away from its intended destination, the two are indistinguishable. The common dictionary meaning of theft is the wrongful "taking and carrying away" or "removing" of property from its owner, implicitly requiring a movement offsite. Also under these definitions, theft implicitly requires continuing possession of the stolen material. By contrast, as defined here, diversion does not require either offsite removal or continuous possession; the diverter could, for example, conceal the diverted material or device onsite and leave it for later misuse by either the diverter or a colluding third party.

Escorted access means 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.

QUESTIONS/ANSWERS:

Q1: Does "accompaniment" mean that the escort must always be physically present when an individual who is not approved for unescorted access is in the security zone?

A1: Generally, yes, although an escort may monitor an unapproved individual remotely (using a closed circuit TV system, for example) as long as the escort maintains continuous direct visual surveillance over the individual at all times. There are some circumstances, such as when a patient undergoes teletherapy, when actual physical accompaniment of such an unapproved individual is not allowed under the as low as reasonable achievable (ALARA) principle, and for which remote surveillance would be the only alternative. Remote visual surveillance should not be so remote, however, as to

interfere with the licensee's ability to detect, assess, and respond immediately to an actual or attempted theft, sabotage, or diversion of radioactive materials.

Q2: Does "direct visual surveillance" mean the same thing as "line-of-sight surveillance?"

A2: No. The term "direct continuous visual surveillance" allows the use of video surveillance. Video surveillance would be appropriate in some, but not all cases. Video surveillance of patients during a treatment, for example, would be appropriate, considering the ALARA complications of having the escort physically present in the treatment room.

Q3: This definition of escorted access requires continuous direct visual surveillance only when an individual not approved for unescorted access is within a security zone. Aren't there circumstances under which this surveillance might be necessary when an unapproved individual is onsite, but outside the security zone?

A3: The licensee is not required to maintain direct visual surveillance outside the security zone, but may choose to escort unapproved individuals in this manner in any area of a facility that the licensee deems appropriate. Direct visual surveillance is required only when an unapproved individual has access to a category 1 or category 2 quantity of radioactive material, and the security zone is effectively the area within which such access is controlled.

Fingerprint orders means the orders issued by the U.S. Nuclear Regulatory Commission or the legally binding requirements issued by Agreement States that require fingerprints and criminal history records checks for individuals with unescorted access to category 1 and category 2 quantities of radioactive material or safeguards information- modified handling.

QUESTIONS/ANSWERS:

Q1: Which particular fingerprint orders referred to in this definition do I need to know about for compliance with this rule?

A1: If you are an existing licensee, you have been issued [NRC orders](#) that require you to take fingerprints and obtain criminal history records checks of employees to determine their trustworthiness and reliability for access to radioactive materials or SGI or SGI-M. The rule's definition here is also intended to include other sources of fingerprinting and criminal history records check requirements, such as license conditions issued by NRC or an Agreement State agency. A license applicant will need to meet the fingerprinting requirements of Part 37.

Government agency means any executive department, commission, independent establishment, corporation, wholly or partly owned by the United States of America which is an instrumentality of the United States, or any board, bureau, division, service, office, officer, authority, administration, or other establishment in the executive branch of the Government.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

License, except where otherwise specified, means a license for byproduct material issued pursuant to the regulations in parts 30 through 36 and 39 of this chapter;

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

License issuing authority means the licensing agency that issued the license, i.e. the U.S. Nuclear Regulatory Commission or the appropriate agency of an Agreement State;

QUESTIONS/ANSWERS:

None. Self-explanatory.

Local law enforcement agency (LLEA) means a public or private organization that has been approved by a federal, state, or local government to carry firearms and make arrests, and 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.

QUESTIONS/ANSWERS:

Q1: Must an LLEA be a government entity?

A1: No. The LLEA may be any security force, including a private one, if it has federal, state, or local government authority to carry firearms and make arrests. University police could be considered an LLEA under the definition, since some university police departments are a fully badged and sworn police force with the authority to make arrests and provide an armed response. A railroad's police force with this authority could also be considered an LLEA.

See also Q&As for § 37.45, LLEA coordination, especially Q&As 3 through 5 for § 37.45(a).

Lost or missing licensed material means licensed material whose location is unknown. It includes material that has been shipped but has not reached its destination and whose location cannot be readily traced in the transportation system.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Mobile device means a piece of equipment containing licensed radioactive material that is either mounted on wheels or casters, or otherwise equipped for moving

without a need for disassembly or dismounting; or designed to be hand carried. Mobile devices do not include stationary equipment installed in a fixed location.

QUESTIONS/ANSWERS:

Q1: The Increased Controls (IC) orders applied additional security requirements to “portable” as well as “mobile” devices. What’s the difference between portable and mobile devices for purposes of compliance with Part 37?

A1: From the standpoint of compliance with § [37.53](#), *Requirements for mobile devices*, there is no difference. The same security requirements apply to both. The definition of “mobile device” for this rule encompasses all devices that can be “hand-carried,” are mounted on wheels/casters, or are otherwise movable by an individual without additional equipment.

Q2: If I have a category 1 or 2 quantity of radioactive material in a 55-gallon drum that isn’t mounted on wheels or casters and can’t be carried by hand, would NRC consider this drum a “mobile device?”

A2: Generally, no, unless the drum were light enough to be turned on its side and rolled to an unauthorized location outside an established security zone. In most cases, a loaded 55-gallon drum would be likely to require a hand truck, forklift, or other equipment to be removed from its authorized place of use or storage. It is a good practice to store the hand truck, forklift, or other equipment for moving the drum in a location away from the storage area.

Q3: If I have a category 1 or 2 quantity of radioactive material in a container that isn’t mounted on wheels or casters and can’t be carried by hand, and I secure it in a pickup truck bed or on a trailer, would NRC consider this source or device “mobile?”

A3: Yes, because the device would be “mounted on wheels” and “equipped for moving without a need for disassembly or dismounting” under this definition. A container or device on a pickup truck bed or on a trailer would also need to meet the requirement of § [37.53\(b\)](#). This subsection provides that unless health and safety requirements for a site prohibit disabling the vehicle, the licensee must “utilize a method to disable the vehicle or trailer when not under direct control and constant surveillance by the licensee.” Licensees subject to this requirement may not rely on the removal of an ignition key to meet the requirement. (See Q&As on § 37.53.)

Movement control center means 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.

QUESTIONS/ANSWERS:

Q1: Must the various functions of the "movement control center" be accomplished by one entity, or may these functions be accomplished by separate departments or personnel?

A1: The movement control center definition does not require that all of the functions be carried out by the same department or personnel. It does require an operations center or base from which all of the functions are handled. To ensure the necessary degree of coordination and effectiveness, it may be more effective if the functions of the movement control center are carried out under the control of a single organization managed by the individual responsible for the timely and effective execution of these functions. The primary purpose of the movement control center is to have staff available that can immediately respond to an emergency and coordinate the required response. As specified by definition, movement control center functions must at a minimum include maintaining current shipment position information, receiving and sending reports, and requesting and coordinating appropriate aid.

No-later-than arrival time means the date and time that the shipping licensee and receiving licensee have established as the time at which an investigation will be initiated if the shipment has not arrived at the receiving facility. The no-later-than-arrival time may not be more than 6 hours after the estimated arrival time for shipments of category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: Does the no-later-than (NLT) arrival time apply to shipments outside the United States?

A1: No. An NLT arrival time must be established only for the domestic portion of a shipment for import or export, that is, shipments with origins and destinations within the U.S. or its territories or possessions. These origins may include locations where imported material is cleared by U.S. customs authorities, and destinations may include terminal facilities for the export of the material.

Q2: The definition of NLT arrival time specifies that the NLT arrival time may not be more than 6 hours after the estimated arrival time for shipments of category 2 quantities of radioactive material. What about category 1 quantities?

A2: The requirement for an NLT arrival time does not apply to shipments of category 1 quantities of radioactive material. For these shipments, each licensee shipping the material must establish a movement control center that must monitor shipments 24 hours a day, 7 days a week, and have the ability to communicate immediately with the appropriate law enforcement agencies in an emergency.

See related Q&As under [§ 37.75](#), *Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material*.

Person means—

(1) Any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, Government agency other than the Commission or the Department of Energy (except that the Department shall be considered a person

within the meaning of the regulations in 10 CFR chapter I to the extent that its facilities and activities are subject to the licensing and related regulatory authority of the Commission under section 202 of the Energy Reorganization Act of 1974 (88 Stat. 1244), the Uranium Mill Tailings Radiation Control Act of 1978 (92 Stat. 3021), the Nuclear Waste Policy Act of 1982 (96 Stat. 2201), and section 3(b)(2) of the Low-Level Radioactive Waste Policy Amendments Act of 1985 (99 Stat. 1842), any State or any political subdivision of or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and
(2) Any legal successor, representative, agent, or agency of the foregoing.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Reviewing official means the individual who shall make the trustworthiness and reliability determination of an individual to determine whether the individual may have, or continue to have, unescorted access to the category 1 or category 2 quantities of radioactive materials that are possessed by the licensee.

QUESTIONS/ANSWERS:

See related Q&As for § 37.23, [Access authorization program requirements](#)

Sabotage means 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.

QUESTIONS/ANSWERS:

Q1: Must I find both “deliberate damage” *and* “malevolent intent” in order to report an incident as sabotage? Can’t I presume malevolent intent if it’s clear that the damage was deliberate?

A1: No, you need not find both deliberate damage and malevolent intent to report suspected sabotage. If you have determined the damage to have been deliberate, you should not hesitate to report it as sabotage or vandalism even if you haven’t yet found convincing evidence that the damage was malevolent. If the damage appears to have been deliberate, and is severe enough to constitute an imminent and substantial danger to an employee or any member of the public, you should report it to the LLEA immediately under [§ 37.57\(a\)](#) regardless of whether the damage might have been malevolent. If you or the employee who discovers the damage has reason to believe it was deliberate, you should also report that it may be malevolent. Also regardless of any apparent malevolence, if the damage is severe enough to constitute an excessive radiation exposure to an employee or any member of the public, you must report it to the NRC or appropriate Agreement State agency immediately under 10 CFR [20.2202](#). Note too that if a quantity of material greater than category 2 has been lost or stolen, you must report it to the NRC or appropriate Agreement State agency immediately under 10 CFR [20.2201](#), regardless of whether or not the removal of the material was malevolent.

Q2: How can I determine for the purposes of this Part that damage to material, a device, or security system component was “deliberate?” How can I determine whether the damage was “with malevolent intent?”

A2: To answer either question, you should consider one or more of the following possible questions about your discovery of the damage:

- Could such severe damage have been accidental -- or could it have been accomplished only by a trained individual who knew or should have known the safety or security consequences and how to avoid them? (If you conclude that the damage was not accidental, you should also consider, at a minimum, the additional questions below.)
- Have there been other suspicious or unexplained instances of damage to material, devices, or security equipment in the past few weeks or months?
- Was the current incident immediately reported by the person who claims to have first discovered it?
- Was that person authorized to be at the site of the damage when it reportedly occurred?
- Was the damage severe enough to indicate that there was intent to degrade or disable the intended function of the damaged device or equipment?
- Does the damage affect safety or security?
- Does the damage appear to have required the efforts of more than one person?
- If you are the first to discover the damage, is there anything in the vicinity or elsewhere on the site to indicate an attempt to conceal the damage?
- Was there collateral damage to physical barriers or monitoring or detection equipment necessary to permit successful forced access to the damaged material, device(s), or security or safety equipment?
- Did this or any other security equipment have to be defeated to gain access to the security zone?
- Is there evidence of forced entry anywhere else on the premises, such as a broken window or jimmied door?
- If the perpetrator(s) were discovered in the act, were they armed? Did they resist or try to escape?
- Did the incident occur at night or during any other interval when the intruder could expect reduced security capabilities at the site?
- Could the perpetrator(s) have attained access to the security zone or security equipment without the help of a knowledgeable insider?

This list of questions is not intended to be exhaustive. There may be other circumstances that prompt other kinds of questions bearing on whether the damage was deliberate or the intent malevolent for the purposes of Part 37.

Safe haven means 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 authorities.

QUESTIONS/ANSWERS:

Q1: Does a safe haven have to be approved by a government entity, such as the state or local police? Do I have to get approval from anyone else, such as the owner or operator of a truck stop?

A1: No. Safe havens need only be identified by the shipping licensee during their preplanning under [§ 37.75\(a\)](#) for the shipment of a category 1 quantity of radioactive material.

Q2: Does “readily recognizable” mean that a truck transport crew has to be able to see a safe haven from the road?

A2: No. Although it would be preferable to choose an easily recognized location, a safe haven may have to be in a forested area, on hilly terrain, or otherwise situated where physical features of the surrounding area may obscure all or part of the site. To be “readily recognizable,” a safe haven need only be in a locale familiar enough to at least one member of the transport crew to enable him or her to know when the transport vehicle needs to turn or exit to reach the site, and know when the transport vehicle has arrived. This individual should also be able to guide local law enforcement or other assistance to the site by phone if necessary.

Q3: Does “readily accessible” mean that the safe haven has to be along the road or right off an exit?

A3: No. Under this definition, a safe haven may be several miles from an exit or turnoff if it meets one of the definition’s other criteria by having security present or providing a site from which, in an emergency, the transport crew can notify and wait for local law enforcement authorities.

Q4: What kind of “security” has to be “present” to satisfy this definition of safe haven? Does this mean that law enforcement agency personnel have to be onsite?

A4: Neither security personnel nor law enforcement authorities need be present at a site for it to serve as a safe haven. Obviously, there are advantages associated with having security present at a site used as a safe haven. However, as noted in the definition, a safe haven may also be a site from which, “in the event of an emergency, the transport crew can notify and wait for the local law enforcement authorities.”

Q5: What does NRC mean when it defines safe haven as a “site?” Does a safe haven have to have a fence or other kind of recognizable property boundaries, and/or be some kind of facility, even if only a parking lot, to meet NRC’s understanding of a “site?”

A5: No. If the site is readily recognizable and readily accessible, it need only meet one of the remaining two criteria in the definition: it must either be where security is present, or where, in the event of an emergency, the transport crew can notify and more safely wait for the local law enforcement authorities.

Q6: So, does this mean that a safe haven can be any place along the side of a road as long as there's an emergency?

A6: A transport crew may well have no choice but to pull to the side of the road in an emergency that makes it unsafe to continue, but this is not the purpose of a safe haven. Nor is it the process by which safe havens must be identified. Under [§ 37.75\(a\)\(2\)](#), safe havens are to be identified *before* an emergency occurs, when the licensee is required to preplan and coordinate shipment information with the governor or the governor's designee of any State through which the shipment will pass. The side of the road may be readily accessible and readily recognizable, but it would not be likely to have security present, and may not even be a place where the transport crew can notify and more safely wait for the local law enforcement authorities in an emergency.

Q7: What conditions enroute would constitute an "emergency" requiring a safe haven under this definition? Would NRC consider only a security incident, such as an armed attack or other malevolent interference with a shipment, to be an "emergency?" Or could an emergency be safety-related, or a mechanical problem requiring a prompt repair?

A7: An emergency could be any of these conditions, and could also include severe weather or the sudden illness or incapacitation of the driver or other member of the transport crew. The key characteristic of an emergency requiring a safe haven under this definition is that the condition must result in an unexpected stoppage of the shipment.

See also pertinent Q&As for § 37.75, Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material.

Security zone means 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.

QUESTIONS/ANSWERS:

Q1: What is the purpose of a security zone?

A1: A security zone is an area, defined by the licensee, that both isolates and controls access to category 1 or category 2 quantities of radioactive material to prevent and detect unauthorized access. The purpose of the zone is to define the area containing the quantities of material that must be protected. A security zone effectively defines where the licensee will apply the isolation and access control measures required by Part 37. All category 1 and category 2 quantities of radioactive material must be used or stored only within a security zone.

Q2: Are the characteristics different for "permanent" and "temporary" security zones?

A2: Both types of security zones must meet the same requirements. See Q&As for §§ 37.47, 37.49, 37.51, and 37.53.

State means a State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

Telemetric position monitoring system means a data transfer system that captures information by instrumentation and/or measuring devices about the location and status of a transport vehicle or package between the departure and destination locations.

QUESTIONS/ANSWERS:

Q1: How does NRC define “departure” and “destination” locations?”

A1: Although it is not defined in the rule, “departure” marks the location where the carrier accepts the consignment of radioactive material for shipment and begins movement of the loaded transport vehicle. The location of departure is the site, usually but not always controlled by the shipping licensee, from which the movement of the loaded transport vehicle begins. “Destination” denotes the location where the receiving licensee accepts the shipment from the carrier and unloads or authorizes the unloading from the carrier’s transport vehicle of the radioactive material specified in the accepted shipment documents.

Trustworthiness and reliability are 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 upon the results from a background investigation.

QUESTIONS/ANSWERS:

Q1: How can I or anybody really know whether an individual is “dependable” in judgment, character, and performance? What does NRC mean by “dependable?”

A1: A judgment of any individual’s dependability is inherently qualitative and not readily amenable to objective measurement or evaluation. Each individual has a temperament, personal history, and other characteristics that require a licensee’s fairest subjective judgment about that individual’s dependability. But the scope of this judgment is limited. For the purposes of this definition, the kind of dependability required is whether the individual can be trusted and relied upon to comply with the licensee’s security requirements, sound an alarm whenever appropriate, and do no willful harm

when he or she is permitted solitary access to any location with an aggregated category 2 or greater quantity of radioactive materials. In addition, under [§ 37.23\(e\)\(1\)](#), the judgment must be based on information produced from a background investigation that satisfies the requirements of [§ 37.25](#).

It is also worth noting that the basis for a judgment about an individual's dependability is limited to the information available at the time. However, if at any time between your initial investigation and the 10-year reinvestigation you receive information that would call that individual's dependability for the purposes of this Part into question, you should not hesitate to re-evaluate the basis for your earlier judgment. Section 37.23(e)(4) specifically provides that a reviewing official "may terminate or administratively withdraw an individual's unescorted access authorization based on information obtained after the background investigation has been completed and the individual granted unescorted access authorization."

Q2: What would constitute an "unreasonable risk" to the public health and safety or security for purposes of Part 37?

A2: An "unreasonable risk" in this context is a risk that granting the subject individual unescorted access to a category 2 or greater quantity of radioactive material would result in its theft, sabotage, or diversion for a malevolent act that affects the public health and safety, and the environment.

See also Q&As on §§ 37.21, 37.23, 37.25, 37.27, and 37.29.

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

QUESTIONS/ANSWERS:

Q1: Is a patient who is alone inside the boundaries of a security zone for teletherapy, but monitored remotely, considered to have unescorted access?

A1: Not if the remote monitoring permits direct and continuous surveillance and an immediate detection, assessment, and response to any unauthorized activity. Patients undergoing radiotherapy would generally be considered "accompanied" if they are under continuous visual surveillance remotely, but nearby. They also are typically in rooms with radiation alarms, closely monitored visually from an adjacent room, and under direct visual surveillance to permit the licensee to effectively detect, assess, and respond immediately to an actual or attempted theft, sabotage, or diversion.

Q2: When must a person who is alone inside the boundaries of a security zone, but monitored remotely, be considered "solitary?"

A2: To be considered "solitary" under this definition, the individual must be both: unaccompanied by an approved individual while inside the boundaries of a security zone; and not under continuous direct visual surveillance at all times. (See definition of [Escorted access](#)) Licensees are required to ensure that all individuals who meet these two conditions for solitary access are approved individuals.

An unapproved individual solely under direct visual surveillance by an approved individual at a central monitoring station remote from the subject security zone should generally not be considered “accompanied” under the definition of escorted access, and should, therefore, be considered sufficiently solitary to require escorting or closer surveillance. Remote visual surveillance should not be so remote as to interfere with the licensee’s ability to detect, assess, and respond immediately to an actual or attempted theft, sabotage, or diversion of radioactive materials. Depending on the configuration of a site’s walls and doors, continuous surveillance from an adjoining room, for example, could be considered “accompaniment” if the approved individual, continuously monitoring the unapproved individual, could immediately warn that individual, or summon timely assistance nearby, to prevent or stop an unauthorized act. By this same operational criterion, however, continuous visual surveillance from another floor or a separate nearby building should not generally be considered “accompaniment,” especially if there are no other licensee personnel near enough to the unapproved individual to make a timely intervention. For the same reason, remote surveillance from another facility offsite should not be considered “accompaniment” for purposes of escorted access under similar operating conditions.

United States, when used in a geographical sense, includes Puerto Rico and all territories and possessions of the United States.

QUESTIONS/ANSWERS:

This definition is not specific to Part 37.

§ 37.7 Communications

Except where otherwise specified or covered under the regional licensing program as provided in § 30.6(b), all communications and reports concerning the regulations in this Part may be sent as follows:

§ 37.7(a)

By mail addressed to: ATTN: Document Control Desk; Director, Office of Nuclear Reactor Regulation; Director, Office of New Reactors; Director, Office of Nuclear Material Safety and Safeguards; Director, Office of Federal and State Materials and Environmental Management Programs; or Director, Division of Security Policy, Office of Nuclear Security and Incident Response, as appropriate, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001;

§ 37.7(b)

By hand delivery to the NRC's offices at 11555 Rockville Pike, Rockville, Maryland 20852;

§ 37.7(c)

Where practicable, by electronic submission, for example, Electronic Information Exchange, or CD-ROM. Electronic submissions must be made in a manner that enables the NRC to receive, read, authenticate, distribute, and archive the submission, and process and retrieve it a single page at a time. Detailed guidance on making electronic submissions can be obtained by visiting the NRC's Website at <http://www.nrc.gov/site-help/e-submittals.html>, by e-mail to MSHD.Resource@nrc.gov; or by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001. The guidance discusses, among other topics, the formats the NRC can accept, the use of electronic signatures, and the treatment of nonpublic information.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

None for this section.

§ 37.9 Interpretations.

Except as specifically authorized by the Commission in writing, no interpretations of the meaning of the regulations in this part by any officer or employee of the Commission other than a written interpretation by the General Counsel will be recognized as binding upon the Commission.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

Q1: Does § 37.9 mean I don't have to comply with an NRC regulatory requirement unless and until its meaning has been interpreted in writing by the NRC General Counsel?

A1: No. You must comply with all applicable regulatory requirements of Part 37. This provision binds the Commission to a particular interpretation of its regulations only if the interpretation is written by the NRC General Counsel or specifically authorized by the Commission in writing. This provision is intended to bind NRC when the meaning of an NRC requirement is subject to differing and disputed interpretations. Having such a binding interpretation is not a precondition for NRC or Agreement State enforcement of requirements with meanings that are plain or otherwise generally accepted. If you have a question about the intended meaning of any requirement, and your question is not clearly addressed in this guidance, please make your question known to NRC at your earliest convenience. You may do this by contacting your nearest NRC regional office listed in paragraph (b)(2) of [10 CFR 30.6](#)

§ 37.11 Specific exemptions

§ 37.11(a)

The Commission may, upon application of any interested person or upon its own initiative, grant such exemptions from the requirements of the regulations in this part as it determines are authorized by law and will not endanger life or property or the common defense and security, and are otherwise in the public interest.

EXPLANATION:

A licensee may ask the NRC for an exemption from a requirement in Part 37 or the NRC can unilaterally decide to exempt a licensee from a requirement. The NRC can grant an exemption provided that it is authorized by law and will not endanger life or property or the common defense and security, and are otherwise in the public interest.

QUESTIONS/ANSWERS:

Q1: If a licensee wants to request an exemption from any requirement of the regulations, what does the licensee need to submit?

A1: A licensee can request an exemption from Part 37 requirements. The licensee should submit an amendment request identifying the regulatory requirement for which the exemption is sought. The amendment request should explain why the licensee is requesting an exemption from the regulatory requirement and how any proposed alternatives will meet that regulatory requirement.

The NRC will evaluate the request and determine if an exemption is appropriate. The NRC will only grant exemptions that it determines are authorized by law and will not endanger life or property or the common defense and security, and are otherwise in the public interest.

It is the licensees' responsibility to provide sufficient justification in support of its exemption request to enable the NRC to make its determination

NRC cannot grant exemptions from requirements mandated by law. For example, the NRC cannot provide an exemption from the fingerprinting and criminal history records check for unescorted access to category 1 and category 2 quantities of radioactive material or access to SGI or SGI-M, because fingerprinting and criminal history records checks are specifically required by § 149 of the Atomic Energy Act ([AEA](#)), as amended by § 652 of the EAct.

§ 37.11 Specific exemptions (cont'd)

§ 37.11(b)

Any licensee's NRC-licensed activities are exempt from the requirements of subparts B and C of this part to the extent that its activities are included in a security plan required by part 73 of this chapter.

EXPLANATION:

NRC licensees may protect the radioactive material covered by Part 37 under a security plan developed under Part 73.

QUESTIONS/ANSWERS:

Q1: If a contract radiographer licensee with material under a Part 37 security plan performs work with that material at a temporary job site located at a reactor or fuel cycle licensee that has a security plan approved under Part 73, which plan would apply?

A1: The materials licensee's Part 37 security plan would apply for the protection of the material. The materials licensee is responsible for meeting the requirements of Part 37 and the licensee's own security plan at a temporary job site, even if the temporary job site is at a licensed reactor or fuel cycle facility.

In addition to the requirements of the materials licensee's security plan, however, the fuel cycle or reactor licensee may also impose other requirements to meet its security plan. For example, a contract radiographer licensee who brings a source onto a reactor site to conduct radiography activities may be subject to such additional reactor security requirements as personal and vehicle searches, access control to vital areas, and training.

Q2: If a Part 50 reactor licensee or a Part 70 fuel cycle facility is also licensed under its respective license to possess an individual source, such as a radiography camera that is at or above the category 2 threshold, would Part 37 requirements apply for the security of the source?

A2: The answer depends on the circumstances. If the licensee protects the source under its approved Part 73 security plan for the reactor area, the licensee would be exempt from the security provisions of Part 37. If the source is in an area not covered by the Part 73 security plan, the Part 37 provisions would apply. Similarly for a Part 70 licensee, if the licensee protects the source under its Part 73 security plan for the fuel facility, the licensee would be exempt from the Part 37 requirements. To ensure that all affected radioactive materials are covered by a security plan, the reactor or fuel cycle facility licensee should document which materials are to be covered under Part 37 and which under Part 73.

Q3: Are activation products contained in, or part of, the reactor structure subject to Part 37?

A3: No. Activation products contained in the structure (such as the stainless steel lining of a reactor vessel, stainless steel bolts, or the reactor hull) would not be subject to Part 37 as long as these materials remain an integral component of a reactor. Upon decommissioning of the reactor, however, waste generated from decommissioning may be subject to Part 37 if the waste meets or exceeds a category 2 threshold. Shipments of decommissioned reactor components, for example, would be subject to Subpart D if their total activity met or exceeded a category 2 threshold and they weighed less than 2000 kilograms (kg) (4409 lbs). See §37.11(c) below.

§ 37.11 Specific exemptions (cont'd)

§ 37.11(c)

A licensee that possesses radioactive waste that contains category 1 or category 2 quantities of radioactive material is exempt from the requirements of subpart B, C, and D of this part. Except that any radioactive waste that contains discrete sources, ion-exchange resins, or activated material that weighs less than 2,000 kg (4,409 lbs) is not exempt from the requirements of this part. The licensee shall implement the following requirements to secure the radioactive waste:

§ 37.11(c)(1)

Use continuous physical barriers that allow access to the radioactive waste only through established access control points;

§ 37.11(c)(2)

Use a locked door or gate with monitored alarm at the access control point;

§ 37.11(c)(3)

Assess and respond to each actual or attempted unauthorized access to determine whether an actual or attempted theft, sabotage, or diversion occurred; and

§ 37.11(c)(4)

Immediately notify the LLEA and request an armed response from the LLEA upon determination that there was an actual or attempted theft, sabotage or diversion of the radioactive waste that contains category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section exempts radioactive wastes that contain category 2 quantities or greater of radioactive material from the security requirements contained in Subparts B, C, and D of Part 37. Instead, the radioactive waste is subject to the security requirements contained in § 37.11(c)(1) – (c)(4). However, if the waste contains discrete sources, ion-exchange resins, or activated material weighing less than 2,000 kg, the requirements contained in Subparts B, C, and D apply.

QUESTIONS/ANSWERS:

Q1: What radioactive material does NRC consider “waste” for purposes of Part 37?

A1: As defined in [10 CFR 20.1003](#), “waste” means “those low-level radioactive wastes containing source, special nuclear, or byproduct material that are acceptable for disposal in a land disposal facility. For the purposes of this definition, “low-level radioactive waste,” as defined in the Low-Level Radioactive Waste Policy Amendments Act of 1985 ([NUREG-0980](#), Vol. 1, p. 3-3) means “radioactive material that ...is not classified as high-level radioactive waste, transuranic waste, spent nuclear fuel, or byproduct material as defined in section 11e.(2) of the Atomic Energy Act of 1954 ... [i.e., uranium mill tailings.]”... .”

Q2: What types of radioactive wastes are exempt?

A2: Radioactive waste with diffuse category 1 or category 2 quantities – as opposed to discrete sources – is exempt only from the requirements of Subparts B, C, and D of Part 37. These wastes are subject to the requirements in § 37.11(c)(1) – (c)(4) in Subpart A of Part 37. Radioactive waste that contains items such as contaminated clothing, gloves, soil, or low specific activity waste would be exempt from the requirements of Subparts B, C, and D. Radioactive waste that contains discrete sources, ion exchange resins, and activated material that weighs less than 2,000 kg are subject to the requirements of Subparts B, C, and D of Part 37

Q3: When are activated material and component parts considered to be waste? If the walls (concrete, steel, etc.) become activated during use, does Part 37 apply?

A3: Walls and component parts that become activated throughout their life are not considered to be waste until they are no longer useful for their intended purpose. Part 37 does not apply to activated material in walls and components during the operating life of a reactor, hot cell, or accelerator. Once the licensee has begun decommissioning and is dismantling the facility, the rubble and removed components would be considered waste and Part 37 would then apply.

Q4: Does the 2,000 kg limit apply to the discrete sources and ion exchange resins or just the activated material?

A4: This weight limit only applies to activated materials and does not apply to discrete sources and ion exchange resins.

Q5: What is meant by discrete sources? Would a waste drum that contained multiple category 3 sources that add up to a category 2 quantity of radioactive material be exempt?

A5: Consistent with 10 CFR 30.4 a discrete source means a radionuclide that has been processed so that its concentration within a material has been purposely increased for use for commercial, medical, or research activities. Waste that has been made radioactive incidentally by a process is not considered a discrete source. The drum would not be exempt since, in this example, it contains discrete sources. The drum, containing aggregated sources, would need to be protected under Part 37.

§ 37.13 Information collection requirements: OMB approval

§ 37.13(a)

The Nuclear Regulatory Commission has submitted the information collection requirements contained in this part to the Office of Management and Budget (OMB) for approval as required by the Paperwork Reduction Act (44 U.S.C. 3501 et seq.). The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has approved the information collection requirements contained in this part under control number 3150-xxxx.

§ 37.13(b)

The approved information collection requirements contained in this part appear in §§ 37.21, 37.23, 37.25, 37.27, 37.29, 37.31, 37.33, 37.41, 37.43, 37.45, 37.49, 37.55, 37.57, 37.71, 37.75, 37.77, 37.79, and 37.81.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

None for this section. Self explanatory.

Subpart B – Background Investigations and Access Authorization Program

§ 37.21 Personnel access authorization requirements for category 1 or category 2 quantities of radioactive material.

§ 37.23 Access authorization program requirements.

§ 37.25 Background investigations.

§ 37.27 Requirements for criminal history records checks of individuals granted unescorted access to category 1 or category 2 quantities of radioactive material.

§ 37.29 Relief from fingerprinting, identification, and criminal history records checks and other elements of background investigations for designated categories of individuals permitted unescorted access to certain radioactive materials or other property.

§ 37.31 Protection of information.

§ 37.33 Access authorization program review.

§ 37.21 Personnel access authorization requirements for category 1 or category 2 quantities of radioactive material

§ 37.21(a) General.

§ 37.21(a)(1)

Each licensee that possesses an aggregated quantity of radioactive material at or above the category 2 threshold shall establish, implement, and maintain its access authorization program in accordance with the requirements of this subpart.

§ 37.21(a)(2)

An applicant for a new license and each licensee that would become newly subject to the requirements of this subpart upon application for modification of its license shall implement the requirements of this subpart, as appropriate, before taking possession of an aggregated category 1 or category 2 quantity of radioactive material.

§ 37.21(a)(3)

Any licensee that has not previously implemented the Security Orders or been subject to the provisions of subpart B shall implement the provisions of subpart B before aggregating radioactive material to a quantity that equals or exceeds the category 2 threshold.

EXPLANATION:

These provisions require licensees to have an access authorization program. New license applicants and licensees newly subject to Part 37 must implement this program

before taking possession of aggregated category 1 or category 2 quantities of radioactive material. A licensee that has not previously implemented NRC Security Orders or been subject to the provisions of subpart B must implement these provisions before aggregating radioactive material to a category 2 or greater quantity.

QUESTIONS/ANSWERS:

Q1: Who is required to have an access authorization program?

A1: Any licensee that possesses an aggregated category 1 or category 2 quantity of radioactive material at a facility must have an access authorization program under § 37.21(a). For first-time license applicants or those seeking a license amendment to authorize possession of an aggregated category 2 or greater quantity of radioactive material, this means that the access authorization program must be in place before the licensee may possess the aggregated material. It also means that if a licensee must implement a security plan under Subpart C or implement the provisions of Subpart D of Part 37 for such aggregated quantities, the licensee will need to have an access authorization program as well.

Q2: I do not currently possess a category 1 or category 2 quantity of radioactive material, but my license authorizes me to possess this quantity. Do I need to implement an access authorization program?

A2: No. If you do not actually possess a category 1 or category 2 quantity of radioactive material, you do not have to implement an access authorization program. However, you do need to implement the program before you take possession of that quantity and aggregate the material at or above a category 2 threshold.

Q3: I am already authorized to possess, at several separate locations, radioactive material that adds up to more than a category 2 quantity, and I now need to aggregate this material at a single location. Will I need to implement an access authorization program?

A3: Yes, if you plan to aggregate the material to a category 2 or greater quantity, you will need to develop and implement an access authorization program before you aggregate the material. You will need to conduct a background investigation, including fingerprinting, for anyone who will have unescorted access to the aggregated category 2 or greater quantity of radioactive material. These individuals will need to be approved for access before the material is delivered for aggregated storage at the single location. You should also notify the appropriate NRC Regional Office that you will be implementing an access authorization program for the first time.

Q4: May I obtain an exemption from the access authorization program requirements if I implement alternative physical or administrative controls and training?

A4: You may apply for an exemption from an access authorization program requirement, but the Commission's discretion to grant an exemption from the access authorization requirements of Subpart B is constrained by statute and a formal determination by the Commission. Under Section 149 of the [AEA](#), NRC must fingerprint "any individual" granted unescorted access to radioactive material subject to NRC regulation that the Commission determines to be "of such significance to the public

health and safety or the common defense and security as to warrant fingerprinting and background checks.” The Commission has determined that unescorted access to material in category 2 or greater quantities requires fingerprinting and background investigations. The Commission will not grant an exemption for this statutory requirement.

Part 37 requirements are designed to provide defense-in-depth for the security of aggregated quantities of radioactive material. No single measure can provide the same level of protection as all security measures integrated into a compliant program. Therefore, if you will be aggregating radioactive material into a category 2 quantity or greater, you must implement each applicable Part 37 requirement unless you can justify the need for an exemption and obtain NRC approval.

Q5: Will I be subject to Subpart B and need to have an access authorization program if I apply to amend my license to increase its possession limits to a category 2 or greater quantity?

A5: If you plan to possess a category 2 or greater quantity of radioactive material that will be aggregated at one location, under § 37.21(a)(2) you must implement an access authorization program before obtaining the material. If you plan to possess the material in less than category 2 quantities at several locations, however, you need not establish or implement an access authorization program before obtaining the radioactive material.

§ 37.21 Personnel access authorization requirements for category 1 or category 2 quantities of radioactive material (cont'd)

§ 37.21(b) General performance objective.

The licensee's access authorization program must ensure that the individuals specified in paragraph (c)(1) of this section are trustworthy and reliable.

EXPLANATION:

This provision establishes the general performance objective of the access authorization program.

QUESTIONS/ANSWERS:

Q1: What is the objective of the access authorization program?

A1: The main objective of the access authorization program is to ensure that individuals who have unescorted access to a category 1 or category 2 quantity of radioactive material are trustworthy and reliable and do not constitute an unreasonable risk to the public health and safety or security of the material.

Q2: How can I protect against an insider threat?

A2: Part 37 requires that unescorted access to category 1 or category 2 quantities of radioactive material be limited to approved individuals. Under [§ 37.25](#) and [§ 37.27](#), an approved individual must be determined to be trustworthy and reliable through a background investigation that includes fingerprinting and a Federal Bureau of Investigation (FBI) criminal history records check. In addition, under [§ 37.43\(c\)](#), the licensee must also provide training to its staff. This training should, among other things, enhance your employees' and contractors' awareness of the requirements in [§ 37.57\(b\)](#) and [§ 37.81\(c\)](#) to assess and report as appropriate "any suspicious activity related to possible theft, sabotage, or diversion" of category 1 or category 2 quantities of radioactive material. Such 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.

In addition, the rule establishes similar, but separate controls on access to materials and access to information in security plans and procedures. Thus, a licensee may grant an approved individual unescorted access to the radioactive material, while limiting or restricting that individual's access to such things as security system codes, monitoring system configurations, alarm system capabilities, and other information about the physical protection of the material. As with access to material, access to such information must be limited to individuals with a need to know who have been determined trustworthy and reliable. These complementary but independent sets of restrictions may not prevent a determined insider, but they will reduce the risk of an individual with malicious intent gaining or enabling others to gain access to the radioactive material.

§ 37.21 Personnel access authorization requirements for category 1 or category 2 quantities of radioactive material (cont'd)

§ 37.21(c) Applicability.

§ 37.21(c)(1)

Licensees shall subject the following individuals to an access authorization program:

§ 37.21(c)(1)(i)

Any individual whose assigned duties require unescorted access to category 1 or category 2 quantities of radioactive material or to any device that contains the radioactive material; and

§ 37.21(c)(1)(ii)

Reviewing officials.

§ 37.21(c)(2)

Licensees need not subject the categories of individuals listed in § 37.29(a)(1) through (13) to the investigation elements of the access authorization program.

§ 37.21(c)(3)

Licensees shall approve for unescorted access to category 1 or category 2 quantities of radioactive material only those individuals with job duties that require unescorted access to category 1 or category 2 quantities of radioactive material.

§ 37.21(c)(4)

Licensees may include individuals needing access to safeguards information-modified handling under part 73 in the access authorization program under subpart B.

EXPLANATION:

These provisions establish who is subject to the access authorization program.

QUESTIONS/ANSWERS:

Q1: Who is subject to the licensee's access authorization program?

A1: Individuals subject to a licensee's access authorization program include reviewing officials and anyone allowed unescorted access to a category 1 or category 2 quantity of radioactive material. Unescorted access is defined as solitary access to category 1 or category 2 quantities of radioactive material or devices containing this material. The term applies to anyone who is unaccompanied while in a security zone by an approved individual who maintains continuous direct visual surveillance at all times. (See Q&As for definitions of "[unescorted access](#)" and "[escorted access](#)" in § 37.5.) This would include an unaccompanied contract carrier or other contract service provider.

You may accept the background investigation conducted by other licensees, such as service providers, if you receive appropriate documentation. You still need to make the

determination that the individual requires unescorted access at your facility and that you accept the documentation from the other licensee. You will need to verify basic identification information before allowing the individual to have unescorted access and the individual must complete the training required by 37.23(a)(2).

For road shipments of category 1 quantities of radioactive material under § 37.79(a)(1) of Subpart D, the access authorization program must also include: vehicle drivers and accompanying individuals. Movement control center personnel; and any individual whose assigned duties provide access to shipment information on category 1 quantities of radioactive material, are subject to access authorization requirements under 10 CFR §§ 73.21 and 73.23 for access to SGI. These individuals may be included in the licensee's Part 37 access authorization program, but are not required to be.

Q2: Why do these individuals need to be subject to the access authorization program?

A2: Individuals who have unescorted access to a category 1 or category 2 quantity of radioactive material could pose a threat to the public health and safety or security, because they could divert or steal risk-significant quantities of radioactive material, or aid others in the commission of such acts.

Q3: Am I required to subject all my employees to the access authorization program?

A3: No. If an unapproved individual has a job-related need to enter your security zone(s), you always have the option to escort that individual and not make a trustworthiness and reliability determination with respect to that individual. Each escort, however, and any other individual with the need for unescorted access, will need to undergo fingerprinting and a background investigation under Part 37 or a comparable access authorization program that meets the requirements of Part 37.

Q4: You note above that unescorted access is defined under § 37.5 as "solitary" access. If an unapproved individual is alone inside the boundaries of a security zone, but monitored remotely, must he or she be considered "solitary" for purposes of the access authorization requirements of Subpart B?

A4: No. To be considered "solitary" under the definition of unescorted access under § 37.5, the person must be unaccompanied by an approved individual while inside the boundaries of a security zone, and not be under continuous direct visual surveillance at all times. Remote visual surveillance can be considered an acceptable form of accompaniment if it is continuous and direct at all times, but it should not be so remote as to interfere with the licensee's ability to detect, assess, and respond immediately to an actual or attempted theft, sabotage, or diversion of radioactive material. Depending on the configuration of a site's walls and doors, continuous surveillance from an adjoining room, for example, could be considered "accompaniment" if the approved individual continuously monitoring the unapproved individual could immediately warn that individual, or summon timely assistance nearby, to mitigate the potential consequences of an unauthorized act. By this same operational criterion, however, continuous visual surveillance from another floor or a separate nearby building should not generally be considered "accompaniment," especially if there are no other licensee personnel near enough to the unapproved individual to make a timely intervention. For the same reason, remote surveillance from another facility offsite should not be

considered “accompaniment” for purposes of escorted access under similar operating conditions.

Q5: May other individuals (e.g., contract physicians, physicists, laboratory staff, house-keeping or security staff, or other staff) not actually using the device or material be authorized unescorted access to a device or radioactive material in a category 2 or greater quantity?

A5: Yes. Other personnel (both licensee and non-licensee) may have unescorted access to the security zone where the device or radioactive material is used or stored if the licensee has determined that they need to have such access and have been approved after undergoing a background investigation that meets the requirements of Subpart B.

Q6: Do other individuals such as contract physicians, physicists, housekeeping, etc need to be fingerprinted even though they don't work directly with the radioactive material?

A6: Yes, unless these individuals' access to the security zone is always escorted. Under § 37.21(c), however, all personnel (both licensee and non-licensee) must be fingerprinted and undergo a background investigation if they have job duties that require unescorted access to a security zone where materials are being used or stored.

Q7: If the aggregated radioactive material is in a secured area within a room, is a trustworthiness and reliability (T&R) determination still required for people who need access to that room?

A7: The answer to this question depends on how the licensee defines the security zone. If the room itself is established as the security zone, an individual with a need to work in that room must be determined to be trustworthy and reliable unless he or she is escorted at all times when in the room. If the licensee establishes the security zone as a smaller secured area within the room, however, the individual would not have to be determined to be trustworthy and reliable to access the part of the room outside the perimeter of the security zone.

Q8: During a source disconnect, would an individual coming in to provide source retrieval services be subject to the access authorization program? If this service individual works for another company, and the company has performed a background investigation on the individual, may I accept that as adequate for my company?

A8: Yes, to both questions, unless you escort those individuals. Individuals without a trustworthiness and reliability determination, but with a need for access must be escorted during source retrieval operations. Alternatively, you may accept a service provider licensee's background investigation if it implements Part 37 requirements. The service provider must, however, provide you a written verification of its employee's trustworthiness and reliability under [§ 37.29\(a\)\(13\)](#). The written verification from the service provider licensee must include the name of each employee who will be providing the service, and a statement to the effect that the employee has been determined to be trustworthy and reliable in accordance with the requirements in Part 37. You must verify the identity of the employee and document your determination basis.

Q9: Would individuals transporting radioactive material be subject to the background investigation requirements?

A9: Yes, for shipments of both category 1 and category 2 quantities, if the licensee itself is transporting the material, these individuals would be subject to the access authorization program because they would have access to the material during shipment. For road shipments of category 1 quantities of radioactive material, fingerprinting and background investigations would be required under § 37.21(c)(1)(i) for all vehicle drivers and accompanying individuals, whether licensee or contractor employees, because their assigned job duties effectively give them unescorted access to this material.

Fingerprinting and background checks would also be required for movement control center personnel, and any individual whose assigned duties provide access to category 1 shipment information that is safeguards information requiring - modified handling (SGI-M).

For road shipments of category 2 quantities of radioactive material, however, commercial drivers and package handlers have been relieved from the background investigation elements of the access authorization program under [§ 37.29\(a\)](#)(10) and (11), respectively. These individuals are subject to DOT security requirements.

Q10: In our operation, practically everyone knows at least something about expected category 1 shipments. Is a T&R determination required for everyone within the operation?

A10: No, but under [10 CFR 73.23\(b\)\(2\)](#), you do need to make a T&R determination on every individual who is granted access to SGI-M.

Under [10 CFR 73.23\(a\)\(2\)](#), SGI-M specifically includes shipping information on category 1 quantities of radioactive material. Types of shipment information in §§ 37.75 - 37.81 of Part 37 that could be considered SGI-M under 10 CFR 73.23(a)(2) would include, among other things, information on: physical security plans and procedures, immobilization devices, and escort requirements that are more detailed than NRC regulations; scheduling and itinerary information; arrangements with and capabilities of local police response forces; locations of safe havens; and details of alarm and communication systems, communication procedures, and duress codes. The performance requirements for handling SGI-M are set forth in [10 CFR 73.21](#), and specific types of information to be protected as SGI-M are itemized in 10 CFR 73.23(a).

Q11: Is the reviewing official subject to the access authorization program?

A11: Yes. The reviewing official must undergo fingerprinting and a background investigation. See the Q&As on § 37.23(b) for additional information on reviewing officials.

Q12: May additional employees (e.g., new hires or existing employees changing positions within the company) who did *not* have unescorted access under the fingerprinting orders be granted unescorted access to a category 1 or category 2 quantity of radioactive material without undergoing fingerprinting and a background investigation?

A12: No. Before being granted unescorted access to material, all employees the licensee identifies as requiring unescorted access must undergo fingerprinting and the background investigation and be determined to be trustworthy and reliable. The licensee may escort these individuals until a background investigation has been completed.

Q13: May a reviewing official who authorizes access to radioactive materials also approve individuals for access to SGI?

A13: Yes. Part 73 requires that a reviewing official conduct the background check review but does not specify who that individual must be, nor any qualifications for the position. A licensee may choose to use the same individual for both SGI access under Part 73 and unescorted access to materials under Part 37.

Q14: May service providers not associated with a Manufacturing and Distribution (M&D) license be provided unescorted access to a category 1 or category 2 quantity of radioactive material at a customer facility?

A14: Yes. Service provider licensees may make a trustworthiness and reliability determination for individuals who provide service at their customer's facilities. Service provider employees who have not been determined to be trustworthy and reliable must be escorted by an employee of the customer who is authorized to have unescorted access to the radioactive material or device containing it. See Q&As on § 37.[29\(13\)](#).

Q15: Our industry is subject to three different Federal background check programs: Bureau of Alcohol, Tobacco, Firearms, and Explosives, the DOT, and the NRC. All three Federal agencies have different requirements, which can be very cumbersome, confusing and costly. Must I establish yet another background investigation program simply to comply with Part 37?

A15: The need for a separate background investigation program for Part 37 will depend on the specific requirements of the other applicable federal agency background investigation program(s). If you have a background investigation program for other activities at a site, and that program also complies with the requirements of Part 37, you do not need to create a separate program for the radioactive material subject to Part 37. You will, however, need to document how specific elements of existing programs are used to implement each Part 37 requirement and why you expect that these elements will demonstrate compliance with each requirement.

Q16: Do individuals on an oil rig who actually manipulate the drilling tools have to be approved individuals for access control purposes under Part 37 if they are not employed by the licensee?

A16: No, as long as there is an approved individual escorting these individuals or exercising direct control of the devices with radioactive material.

§ 37.23 Access authorization program requirements

§ 37.23(a) Granting unescorted access authorization.

§ 37.23(a)(1)

Licensees shall implement the requirements of this subpart for granting initial or reinstated unescorted access authorization.

§ 37.23(a)(2)

Individuals who have been determined to be trustworthy and reliable shall also complete the security training required by § 37.43(c) before being allowed unescorted access to category 1 or category 2 quantities of radioactive material.

EXPLANATION:

Each licensee must implement the requirements of Part 37 Subpart B before granting an individual unescorted access to category 1 or category 2 quantities of radioactive material. An individual must also complete security training before exercising the unescorted access.

QUESTIONS/ANSWERS:

Q1: What additional NRC requirements must be met before allowing an individual unescorted access to a category 1 or category 2 quantity of radioactive material?

A1: In addition to the background investigation and determination of trustworthiness and reliability, the individual must complete the security training required by [§ 37.43\(c\)](#) before being allowed unescorted access to the material. This is essential for the individual to have an adequate understanding of his or her responsibilities. There may also be other applicable health and safety requirements that the individual will have to meet before being allowed unescorted access or using the material.

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(b) Reviewing officials.

§ 37.23(b)(1)

Reviewing officials are the only individuals who may make trustworthiness and reliability determinations that allow individuals to have unescorted access to category 1 or category 2 quantities of radioactive materials possessed by the licensee.

§ 37.23(b)(2)

Each licensee shall name one or more individuals to be reviewing officials. After completing the background investigation on the reviewing official, the licensee shall provide under oath or affirmation, a certification that the reviewing official is deemed trustworthy and reliable by the licensee. The fingerprints of the named reviewing official must be taken by a law enforcement agency, Federal or State agencies that provide finger printing services to the public, or commercial fingerprinting services authorized by a State to take fingerprints. The licensee shall recertify that the reviewing official is deemed trustworthy and reliable every 10 years in accordance with § 37.25(b).

EXPLANATION:

Only ROs may make T&R determinations authorizing individuals to have unescorted access. Reviewing officials must themselves undergo background investigations, and the licensee must certify by oath or affirmation that the RO is trustworthy and reliable.

QUESTIONS/ANSWERS:

Q1: What is the role of the reviewing official?

A1: The RO makes the T&R determinations for the licensee and determines who may be granted unescorted access authorization. Note that the Increased Control Fingerprinting Orders referred to a trustworthiness and reliability official or T&R Official as the individual who made determinations on an employee's trustworthiness and reliability. Unlike the RO, the T&R Official did not have to be fingerprinted and subject to a background investigation. This rule closes that potential security gap by requiring a T&R determination for each RO.

Q2: Who can be a reviewing official?

A2: The licensee decides who is named as an RO. The reviewing official may be the radiation safety officer (RSO), someone from the Human Resources (HR) Department, or any other individual. In order to review the FBI criminal history records, the RO must be a licensee employee not a contractor. Also, the RO must be authorized for unescorted access to category 1 or category 2 quantities of radioactive material or access to SGI or SGI-M, but the RO does not have to be allowed to actually have access to the material.

Q3: May the HR Department be designated to perform the background investigations and be the repository for T&R determination records? If we have a process in place, may we continue to use that process? Does the RSO have to be involved?

A3: The review and/or record storage may be delegated to a licensee's HR or any other appropriate department depending on its mission and available resources. Additionally, a licensee may use the information previously obtained through the hiring process or another background investigation process to support a T&R determination without having to re-verify the information. The individual responsible for T&R determinations must also undergo fingerprinting and an FBI criminal history check, however, and the licensee must document the basis for concluding that its ROs are trustworthy and reliable.

The RSO does not have to be involved in T&R determinations, but because safety and security often go hand-in-hand, the RSO will likely need to be integrally involved in any implementation decisions.

Q4: Must individuals whose sole job duties are to determine eligibility for employment (e.g., HR specialists) undergo a background investigation and be determined to be trustworthy and reliable?

A4: No. Only the RO must undergo a background investigation and be determined trustworthy and reliable, because an untrustworthy RO could approve access by other untrustworthy individuals as part of a conspiracy to steal, sabotage, or divert radioactive material. The T&R determination may, however, use relevant information obtained and evaluated by human resource personnel when determining whether to hire an individual. If the T&R determination is not made by the HR staff, and the licensee is only relying on the HR staff to obtain information from the background check (e.g., employment history, education, and personal references), the HR staff does not have to undergo a background investigation.

Q5: How do I name an individual to be a reviewing official?

A5: You need to submit the individual's name and fingerprints to the NRC. The fingerprints of the individual(s) being considered for reviewing official need to be taken by either a law enforcement agency, a Federal or State agency that provides fingerprinting services to the public, or a commercial fingerprinting service authorized by a State to take fingerprints. After completing the background investigation on the candidate RO and determining that he or she is trustworthy and reliable, you must provide under oath or affirmation a certification that you deem the reviewing official to be trustworthy and reliable. In accordance with § 37.25(b), you must also re-certify that the reviewing official is trustworthy and reliable every 10 years after his or her selection. Additional guidance for evaluating an individual's trustworthiness and reliability for allowing unescorted access is provided as [Annex A](#) at the end of the Q&As for this Subpart.

Q6: If a licensee already has a T&R official or RO to comply with an NRC security order, may this individual continue to serve as the RO under Part 37?

A6: If the T&R official or RO required by an NRC security order has undergone fingerprinting and a background investigation, he or she may continue to serve as the RO without further action. If the individual serving as the T&R official has not undergone fingerprinting and a background investigation, these steps must be completed before he or she can make any additional T&R determinations.

Q7: Section 37.23(b)(2) requires that the fingerprints of the RO be taken by a law enforcement agency, a Federal or State agency that provides fingerprinting services to the public, or a commercial fingerprinting service authorized by a State to take fingerprints. This makes the licensee incur additional cost to travel to an authorized agency and fees to have the authorized agency take fingerprints. Why doesn't the rule allow the RO to be fingerprinted by the licensee's personnel?

A7: Because the RO has greater responsibility in the access authorization program, and will be making the determinations to allow access, the NRC determined it necessary for the reviewing official's fingerprints to be taken by an independent entity to ensure that the identification provided matches the person being fingerprinted. This ensures the correct identification of the individual submitting the fingerprints. Without this requirement, the reviewing official could substitute as his or her own fingerprints of another individual who is known not to have a criminal history or terrorist ties.

Q8: How do I know that a new applicant for RO duties isn't someone who's been denied unescorted access in some other state and has just come to me to get approval? Will NRC or some other organization keep a registry of such applicants?

A8: If you do an adequate employment history check, and learn that the applicant worked for other licensees, you may be able to forestall this problem by specifically asking one or more of his or her most recent employers. If none of these previous employers is willing to provide information on previous denials of access authorization, you may try to get information from friends, relatives, or other sources independent of the applicant's references under § 37.25(a)(6). You may also ask the applicant in a personal interview and look for non-verbal cues that may indicate that he or she is lying or withholding relevant information.

The NRC does not have a system to track individuals that have been granted unescorted access or those that have been denied.

Q9: What if a licensee's reinvestigation of its RO, or new information from any source at any time between reinvestigations, requires the licensee to revoke the RO's access authorization? Do all of his or her T&R determinations on other individuals since the previous investigation need to be re-done?

A9: The answer to this question will depend on the kind of new information the licensee obtains about the RO. A discovery that the individual is on a no-fly list for suspected collaboration with a known criminal or terrorist organization, for example, should warrant a review of all his or her past T&R determinations, or at least those dating from about the time he or she was first put on such a list. The licensee is responsible for ensuring that only trustworthy and reliable individuals are authorized to have access to radioactive materials. The licensee's assessment of the extent of its potential security liability should include, but may not be limited to, such factors as: the number of employees to whom the RO has authorized unescorted access since his or

her last background check; the licensee's knowledge of the kinds and frequency of contact, social, financial, familial, or romantic, that the RO has had with any of these employees; and the timing of their access authorization approvals in relation to the timing of the event(s) that raise doubts in your mind about the former RO's trustworthiness or reliability.

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(b) Reviewing officials.

§ 37.23(b)(3)

Reviewing officials must be permitted to have unescorted access to category 1 or category 2 quantities of radioactive materials or access to safeguards information-modified handling, if the licensee possesses safeguards information or safeguards information-modified handling.

§ 37.23(b)(4)

Reviewing officials cannot approve other individuals to act as reviewing officials.

§ 37.23(b)(5)

A reviewing official does not need to undergo a new background investigation before being named by the licensee as the reviewing official if:

§ 37.23(b)(5)(i)

The individual has undergone a background investigation that included fingerprinting and a FBI criminal history records check and has been determined to be trustworthy and reliable by the licensee; or

§ 37.23(b)(5)(ii)

The individual is subject to a category listed in § 37.29(a).

EXPLANATION:

Reviewing officials must be permitted unescorted access to category 1 or category 2 radioactive materials, or SGI or SGI-M if the licensee possesses this information. Reviewing officials may not approve other individuals to act as reviewing officials. A reviewing official does not need to undergo a new background investigation if he or she has already been determined trustworthy and reliable after a background investigation that included fingerprinting and a criminal history records check.

QUESTIONS/ANSWERS:

Q1: When may a RO make T&R determinations to permit unescorted access by employees?

A1: The RO may make T&R determinations for any employee who requires unescorted access only after the licensee has completed the required fingerprinting, FBI criminal history records check, and background investigation of the RO and certified to the NRC, under oath or affirmation, that she or he is trustworthy and reliable.

Q2: May I appoint multiple ROs?

A2: Yes, but each must undergo fingerprinting, a background investigation, and an FBI criminal history records check, and you must certify under oath or affirmation that each RO is trustworthy and reliable. In order to review FBI criminal history records, each RO must be a licensee employee, not a contractor.

Q3: Section 37.23(b)(4) prohibits a reviewing official from approving other individuals to act as reviewing officials. May the incumbent RO do anything related to a licensee's nomination of another reviewing official, or is the incumbent barred from providing any support?

A3: An approved RO may conduct the other aspects of the background investigation ([§ 37.25\(a\)\(2\) – \(a\)\(7\)](#)) for an individual who is to be nominated by the licensee as a reviewing official.

Q4: May a State official exempted under [§ 37.29\(a\)\(6\)](#) or [§ 37.29\(a\)\(7\)](#) serve as a reviewing official?

A4: Yes. An official qualifying for relief from fingerprinting and other background investigation requirements under this subsection may serve as a reviewing official, as would an individual covered by any of the other categories of relief. Such a scenario is not likely to arise, however, unless the official serves a state entity licensed by its Agreement State regulatory agency.

Q5: Why must ROs be permitted unescorted access to category 1 or category 2 quantities of radioactive materials or access to SGI?

A5: It is important that individuals making the final determination of trustworthiness and reliability for others be trustworthy and reliable themselves. This means that ROs must undergo the same background investigation as individuals granted unescorted access, including fingerprinting and the FBI criminal records check. If the RO is not fingerprinted, a potentially exploitable vulnerability could be created in the security program. The NRC's AEA authority to collect fingerprints only applies to individuals who have unescorted access to radioactive material or access to SGI. The reviewing official must therefore be permitted access to radioactive material or SGI for the NRC to be authorized to require the collection of his or her fingerprints for submittal to the FBI for processing. The RO will not need to actually use the unescorted access, however, if the licensee determines that the RO has no need for it to perform a job duty.

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(c) Informed consent.

§ 37.23(c)(1)

Licensees may not initiate a background investigation without the informed and signed consent of the subject individual. This consent must include authorization to share personal information with other individuals or organizations as necessary to complete the background investigation. Before a final adverse determination, the licensee shall provide the individual with an opportunity to correct any inaccurate or incomplete information that is developed during the background investigation. Licensees do not need to obtain signed consent from those individuals that meet the requirements of § 37.25(b). A signed consent must be obtained prior to any reinvestigation.

§ 37.23(c)(2)

The subject individual may withdraw his or her consent at any time. Licensees shall inform the individual that:

§ 37.23(c)(2)(i)

If an individual withdraws his or her consent, the licensee may not initiate any elements of the background investigation that were not in progress at the time the individual withdrew his or her consent; and

§ 37.23(c)(2)(ii)

The withdrawal of consent for the background investigation is sufficient cause for denial or termination of unescorted access authorization.

EXPLANATION:

Licensees may not begin a background investigation without the informed and signed consent of the subject individual. The subsection also requires a licensee to inform the subject individual of his or her right to correct inaccurate or incomplete information, and have an opportunity to correct it, before the licensee makes an adverse T&R determination. If an individual withdraws consent to a background investigation, the licensee may not begin any new element of that investigation.

QUESTIONS/ANSWERS:

Q1: What is informed consent?

A1: Informed consent is the individual's authorization that allows the licensee to conduct the background investigation to determine whether the individual is trustworthy and reliable. The licensee needs to explain to the individual that a background investigation is being conducted, and explain the potential consequences if the individual does not agree to the background investigation. 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 include authorization to share personal information with other individuals or organizations as necessary to complete the background investigation. A template for a

possible consent form that a licensee can adapt for its use is provided as [Annex B](#) at the end of the Subpart B section.

Q2: For individuals who have already been granted unescorted access under the various orders, does a licensee need to go back and obtain informed consent?

A2: No, unless these individuals have not already undergone a background investigation that included fingerprinting and an FBI criminal history records check. The licensee must obtain an informed consent before starting any new background investigation, and before a reinvestigation of any currently approved individual.

Q3: How do I obtain informed consent from an individual?

A3: You should first explain the informed consent process to the individual either orally or in writing. The easiest way to obtain the informed consent is to have a form with the necessary information that the individual could read and then sign and date. A template for a possible consent form is provided as [Annex B](#).

Q4: What should I do if an individual withdraws his or her consent and I'm in the middle of his or her background investigation?

A4: If an individual withdraws his or her consent, you're required under § 37.23(c)(2)(ii) to inform the individual that withdrawal of consent for the background investigation is sufficient cause for denial or termination of unescorted access authorization. You may finish work on any elements of the background investigation you had undertaken before the consent was withdrawn, but under § 37.23(c)(2)(i) you may not initiate any additional elements that were not already in process.

Q5: If an individual withdraws his or her consent and I terminate the background investigation, may the individual be granted unescorted access to the material?

A5: No. If an individual withdraws consent for the background investigation and that investigation is, therefore, never completed, the licensee would not have a basis for granting that individual unescorted access.

Q6: May an individual who initially withdraws permission for a background investigation, but later gives permission, be granted unescorted access?

A6: Yes. If the completed background investigation supports the determination, the individual may be granted unescorted access. The fact that permission was initially withdrawn would not in itself be sufficient grounds for denial.

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(d) Personal history disclosure.

Any individual who is applying for unescorted access authorization shall disclose the personal history information that is required by the licensee's access authorization program for the reviewing official to make a determination of the individual's trustworthiness and reliability. Refusal to provide, or the falsification of, any personal history information required by this subpart is sufficient cause for denial or termination of unescorted access.

EXPLANATION:

These provisions establish that individuals applying for unescorted access authorization must disclose their personal history information.

QUESTIONS/ANSWERS:

Q1: What is a personal history disclosure?

A1: The personal history disclosure is the information required to be provided by the individual seeking unescorted access to category 1 or category 2 quantities of radioactive material. It is the type of information typically collected on an employment application. The information should include items such as employment history, education, references, and any arrest record. It may also include, but is not required to include, information related to finances such as bankruptcies. This information provides the RO with a starting point for the background investigation.

Q2: The information sounds like information provided for employment. May I use an employment application to gather the information?

A2: The information to be provided under a personal history disclosure is similar to information obtained by many companies in an application for employment. If the employment application contains adequate information, it may be used for this purpose.

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(e) Determination basis.

§ 37.23(e)(1)

The reviewing official shall determine whether to permit, deny, unfavorably terminate, maintain, or administratively withdraw an individual's unescorted access authorization based on an evaluation of all of the information collected to meet the requirements of this subpart.

§ 37.23(e)(2)

The reviewing official may not permit any individual to have unescorted access until the reviewing official has evaluated all of the information collected to meet the requirements of this subpart and determined that the individual is trustworthy and reliable. The reviewing official may deny unescorted access to any individual based on information obtained at any time during the background investigation.

§ 37.23(e)(3)

The licensee shall document the basis for concluding whether or not there is reasonable assurance that an individual is trustworthy and reliable.

§ 37.23(e)(4)

The reviewing official may terminate or administratively withdraw an individual's unescorted access authorization based on information obtained after the background investigation has been completed and the individual granted unescorted access authorization.

§ 37.23(e)(5)

Licensees shall maintain a list of persons currently approved for unescorted access authorization. When a licensee determines that a person no longer requires unescorted access or meets the access authorization requirement, the licensee shall remove the person from the approved list as soon as possible, but no later than 7 working days, and take prompt measures to ensure that the individual is unable to have unescorted access to the material.

EXPLANATION:

These provisions establish requirements for reviewing officials to grant, deny, or withdraw an individual's unescorted access authorization. Licensees are required to document the reason that an individual is determined to be trustworthy and reliable, and to maintain a list of individuals approved for unescorted access.

QUESTIONS/ANSWERS:

Q1: What information should the reviewing official use to determine that an individual is trustworthy and reliable?

A1: Under § 37.23(e)(2), the reviewing official must use all of the information gathered during the background investigation to make a determination that an individual is trustworthy and reliable. It is expected that licensees will use their best efforts to

obtain this information. Information previously obtained during the hiring process may be used to support the T&R determination without having to re-verify that information.

The reviewing official may deny unescorted access to any individual based on any information obtained at any time during the background investigation that calls into question the individuals' trustworthiness and reliability. Under [§ 37.27\(b\)](#), however, the licensee may not base a final determination to deny an individual unescorted access to category 1 or category 2 quantities of radioactive material solely on the basis of information received from the FBI involving: (1) an arrest more than 1 year old for which there is no information of the disposition of the case; or (2) an arrest that resulted in dismissal of the charge or an acquittal. If there is no record on the disposition of the case, it may be that information on a dismissal or acquittal was not recorded. Some indicators that licensees should consider as potential trustworthiness and reliability concerns can be found in [Annex A](#).

Q2: How will we obtain all the information we need to complete a background investigation before granting unescorted access to an individual without a previous employment record (e.g., a recent high school or college graduate)?

A2: For new hires without an employment history, you will need to rely more on other aspects of the background investigation such as references. A lack of employment history need not be a negative consideration in determining whether an individual is deemed to be trustworthy and reliable and given unescorted access to category 1 or category 2 quantities of radioactive material. The individual may be escorted until the background investigation has been completed and the individual has been determined to be trustworthy and reliable for unescorted access.

Q3: Are managers subject to the same background investigations?

A3: Yes. If a manager has unescorted access to the radioactive material, he or she is subject to the same background investigation requirements.

Q4: What criteria do I use to determine trustworthiness and reliability?

A4: The NRC has not developed a set of criteria for determining trustworthiness and reliability because no such list is likely to cover all licensees' needs, and each licensee is in the best position to weigh the many considerations that must support such determinations. Therefore, it is your responsibility to make T&R determinations for all employees granted unescorted access. The background investigations under [§ 37.25](#) are designed to identify past actions that might call into question an individual's trustworthiness and reliability. Some indicators that licensees should consider as potential concerns can be found in [Annex A](#). Although you should review this Annex in its entirety, some of the indicators are provided here for your convenience:

- Impaired performance attributable to psychological or other disorders.
- Conduct that warrants referral for criminal investigation or results in arrest or conviction.
- Indication of deceitful or delinquent behavior.
- Attempted or threatened destruction of property or life.
- Suicidal tendencies or attempted suicide.
- Illegal drug use or the abuse of legal drugs.

- Alcohol abuse disorders
- Recurring financial irresponsibility.
- Irresponsibility performing assigned duties.
- Inability to deal with stress, or having 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, or repeated absenteeism.
- Significant behavioral changes, moodiness or depression.

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

Q5: Are you requiring licensees to determine if employees are telling the truth?

A5: No. Under § 37.23(e)(1), licensees are required only to evaluate all of the information collected to meet the requirements of this subpart, and document under § 37.23(e)(3) the basis for concluding whether or not there is reasonable assurance that an individual is trustworthy and reliable.

Q6: If someone has a drug or alcohol problem, does that automatically make him or her unreliable?

A6: No. A drug or alcohol problem does not in itself make an individual unreliable, especially if the individual has acknowledged the problem and is undergoing treatment.

Q7: How should the T&R determination for my employees be documented?

A7: Under § 37.23(e)(3), the documentation must include the individual employee's or applicant's name and the basis for concluding whether there is reasonable assurance that he or she is trustworthy and reliable. The elements you are required to consider in making your determination are set forth in [§ 37.25](#). Because the basis for your determination is also the result of a process, a good documentation practice would include the criteria, procedures, and records you used to support your determination, the date of this determination, and the name and signature of the person responsible for making it. Where you have been unable to obtain adequate information for an element, such as a character and reputation determination, you should make this clear and describe the efforts you made to gather the needed information.

The type of documentation may include fax, voice mail, or e-mail records, letters, photos, film, audio or video tape, notes to a file, or anything else you used to support your determination. The form of the documentation may be an original or copy, on paper, electronic, or other media, as long as the record is legible for the required period and can be accessed. To discourage unauthorized alterations, electronic copies should if possible be read-only, such as those in portable document format (pdf).

Q8: If I can't obtain all of the information required in § 37.25, may I still grant the individual unescorted access?

A8: Yes. If you conclude that the individual should still be authorized for unescorted access based on other background investigation information, you may grant the individual unescorted access. Under § 37.23(e), you must document the basis for your decision to grant unescorted access. If a previous employer, educational institution, or any other entity with which the individual claims to have been engaged fails to provide information at least 10 business days after your request, or indicates an inability or unwillingness to provide information, or if you are unable to reach the entity, under § 37.25(a)(7), you must document that and attempt to obtain the information from an alternate source.

You also have the option of escorting the individual and not making a T&R determination.

Q9: If I've determined someone to be trustworthy and reliable, and that individual later takes the material for malevolent use, what actions are expected of me? What liability do I assume because of my T&R determination?

A9: If there was nothing in the background investigation that would have caused you to deny access, and you did everything that was required, you would not be in violation of the access authorization requirements. You are required to provide reasonable assurance that persons granted access are trustworthy and reliable. If you fail to provide that assurance, you will be in violation of the Part 37 requirements, and enforcement action will be considered. But providing assurance means that you have taken reasonable efforts as required by Part 37 to ascertain trustworthiness and reliability, and you have documented those actions. As long as you can show that you have made a reasonable good-faith effort, NRC will not second-guess your decision.

Q10: Does the denial of unescorted access create legal liability for the licensee?

A10: Although you should check the requirements of applicable state laws, the NRC does not consider a denial of unescorted access authorization to be a denial of employment. The applicant may still work in areas of the facility outside of security zones, or perform escorted work within the facility. A denial only prevents the employee from having unescorted access to a category 1 or category 2 quantity of material.

Q11: How can we address the unique challenges related to establishing trustworthiness and reliability for foreign nationals?

A11: Determining the trustworthiness and reliability of foreign nationals, including students, does pose special challenges. An evaluation of academic and other references (e.g., transcripts, college applications, financial aid applications, etc.), may form part of the basis for a T&R determination. A visa does not, in and of itself, provide an adequate basis for determining that the individual is trustworthy and reliable.

Background investigations are required to verify and develop information that supports the basis for the T&R determination. Under § 37.25(a)(6) licensees must obtain independent corroborating information to the extent possible. The Part 37 requirements incorporate the phrase "to the extent possible" to communicate the expectation that licensees will use their best efforts to obtain the information required. If obtaining such corroborative information becomes impossible, however, and you conclude that the

individual should still be authorized for unescorted access based on other background investigation information, you should be prepared to document your efforts to obtain the necessary information.

Q12: If I decide that one of my employees previously granted unescorted access to radioactive material should no longer have unescorted access, what actions can I take?

A12: You should immediately revoke the individual's unescorted access. You are ultimately responsible for determining the best method to revoke an employee's unescorted access to radioactive material. Any change in access status should be documented with supporting information.

Q13: Does my list of individuals who have been granted unescorted access need to include all employees and contractors who have been denied unescorted access?

A13: No. The list only needs to include those individuals to whom you have decided to grant unescorted access. The list is not intended to include unapproved individuals whom you must escort.

Q14: Are there any other sources of information I should check before making a final determination on an individual?

A14: Yes, you should check the NRC's list of escalated enforcement actions issued to individuals. The list includes individuals who are prohibited from working with radioactive materials. This listing can be found on the NRC's website at: <http://www.nrc.gov/reading-rm/doc-collections/enforcement/actions/individuals/>.

Q15: How quickly must I remove an individual from my list of those approved for unescorted access after I've determined that he or she no longer requires it?

A15: Under § 37.23(e)(5), you must remove that individual from your approved list as soon as possible, but no later than 7 working days after you've determined that he or she no longer requires unescorted access to the radioactive material subject to this Part. Under this same subsection, you must also take prompt measures to ensure that he or she is no longer able to have unescorted access.

§ 37.23 Access authorization program requirements

§ 37.23(f) Procedures.

Licensees shall develop, implement, and maintain written procedures for implementing the access authorization program. The procedures must include provisions for the notification of individuals who are denied unescorted access. The procedures must include provisions for the review, at the request of the affected individual, of a denial or termination of unescorted access authorization. The procedures must contain a provision to ensure that the individual is informed of the grounds for the denial or termination of unescorted access authorization and allow the individual an opportunity to provide additional relevant information.

EXPLANATION:

These provisions establish requirements for written procedures for implementing the access authorization program.

QUESTIONS/ANSWERS:

Q1: Am I as a licensee required to have procedures for conducting background investigations?

A1: Although § 37.23(f) does not specifically require procedures for conducting background investigations, it does require you to develop, implement, and maintain written procedures for implementing the access authorization program as a whole. The NRC expects that you would have procedures for conducting background investigations as an important component of your procedures for your access authorization program. Under § 37.23(f), your procedures must enable applicants to review the outcome of your T&R determination, for example, and under § 37.23(e), your determination must be based on information produced from a background investigation. Your procedures under this subsection must also address the notification of individuals denied authorization for unescorted access, must ensure that they are informed of the grounds for your denial or termination of unescorted access authorization, and must provide such individuals an opportunity upon request to review your denial or termination and provide additional relevant information. Thus, it would be good practice to ensure that your procedures address your expectations for the performance and documentation of background investigations.

Q2: What procedures would you suggest for making T&R determinations?

A2: The NRC does not suggest specific procedures for making T&R determinations. However, in general licensees should consider developing procedures that address, among other things: how to conduct a background investigation, how to make and document a determination basis, the criteria for when the licensee would accept another company's findings and what information the licensee needs to verify; how to reinstate an individual, how to maintain the list of individuals approved for unescorted access; and how to withdraw an individual's approved unescorted access. Procedures may differ in kind, sequence, structure, and level of detail as long as they produce the kinds of information and documentation required by [§§ 37.25](#) and [37.27](#).

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(g) Right to correct and complete information.

§ 37.23(g)(1)

Prior to any final adverse determination, licensees shall provide each individual subject to this subpart with the right to complete, correct, and explain information obtained as a result of the licensee's background investigation. Confirmation of receipt by the individual of this notification must be maintained by the licensee for a period of 1 year from the date of the notification.

§ 37.23(g)(2)

If after reviewing his or her criminal history record an individual believes that it is incorrect or incomplete in any respect and wishes to change, correct, update, or explain anything in the record, the individual may initiate challenge procedures. These procedures include direct application by the individual challenging the record to the law enforcement agency that contributed the questioned information or a direct challenge as to the accuracy or completeness of any entry on the criminal history record to the Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306 as set forth in 28 CFR 16.30 through 16.34. In the latter case, the Federal Bureau of Investigation (FBI) will forward the challenge to the agency that submitted the data, and will request that the agency verify or correct the challenged entry. Upon receipt of an official communication directly from the agency that contributed the original information, the FBI Identification Division makes any changes necessary in accordance with the information supplied by that agency. Licensees must provide at least 10 days for an individual to initiate action to challenge the results of an FBI criminal history records check after the record being made available for his or her review. The licensee may make a final adverse determination based upon the criminal history records only after receipt of the FBI's confirmation or correction of the record.

EXPLANATION:

These provisions require licensees to give individuals the right to complete, correct and explain the information gathered for the licensee's T&R determination before the licensee makes an adverse determination. Licensees must also give these individuals the right to challenge that information before the licensee makes an adverse T&R determination.

QUESTIONS/ANSWERS:

Q1: Why must I provide an applicant for unescorted access authorization the right to "complete, correct, and explain" the information I obtained during a background investigation before I make a final adverse determination (i.e. deny unescorted access)?

A1: An individual is given the right to review the record prior to any adverse determination because the information you're relying on to make that determination must

be complete, correct, and fully explained. You do not want to make an adverse decision based on possibly incomplete or inaccurate information. Misinformation could be the result of a recordkeeping error, identity theft, or misidentification of another individual with the same or similar name. An individual may also have been charged with an offense of some type, but found innocent or had the charges dropped, and the record might never have been updated to reflect this additional information. The individual might also be able to provide mitigating information that could be relevant to your decision.

Q2: May any of the background investigation information be challenged?

A2: Yes, the individual may request clarification of any information he or she believes is incorrect. For some kinds of information, the individual may simply provide the licensee what he or she believes to be the correct information. The licensee may then consider the new information in its T&R determination process. The licensee should, however, verify the corrected information if possible.

Q3: What is the process for challenging criminal history records?

A3: If the individual believes that his or her criminal history records are incorrect or incomplete in any respect, he or she may initiate challenge procedures. These procedures would include direct application by the individual to the law enforcement agency that contributed the questioned information. An individual may also challenge the accuracy or completeness of any entry on the criminal history record by contacting the FBI at:

Federal Bureau of Investigation,
Criminal Justice Information Services (CJIS) Division,
ATTN: SCU, Mod. D-2,
1000 Custer Hollow Road,
Clarksburg, WV 26306

Instructions for a challenge to the FBI are set forth in [28 CFR 16.30](#). The FBI will forward the challenge to the agency that submitted the data, and will request that the agency verify or correct the challenged entry. Upon receipt of an official communication directly from the agency that contributed the original information, the FBI's Identification Division makes any necessary changes to the individual's criminal history record.

The licensee may not make a final adverse determination based solely on the criminal history records until the licensee receives the FBI's confirmation or correction of the record.

Q4: How long must I allow for an individual to challenge my findings before I make a final determination to grant or deny authorization for unescorted access?

A4: Under § 37.23(g)(2), you must provide at least 10 days for an individual to initiate action to challenge the results of an FBI criminal history records check, although you may allow more time. You may use your judgment for other elements of the background investigation. The implementation procedures for your access authorization program should specify your timeframes for these challenges. In any case, you may not make a

final adverse determination based on the criminal history records until you have received the FBI's confirmation or correction of the record(s) that the individual has challenged.

§ 37.23 Access authorization program requirements (cont'd)

§ 37.23(h) Records.

§ 37.23(h)(1)

The licensee shall retain documentation regarding the trustworthiness and reliability of individual employees for 3 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

§ 37.23(h)(2)

The licensee shall retain a copy of the current access authorization program procedures as a record for 3 years after the procedure is no longer needed. If any portion of the procedure is superseded, the licensee shall retain the superseded material for 3 years after the record is superseded.

§ 37.23(h)(3)

The licensee shall retain the list of persons approved for unescorted access authorization for 3 years after the list is superseded or replaced.

EXPLANATION:

These provisions establish recordkeeping requirements for licensee access authorization programs.

QUESTIONS/ANSWERS:

Q1: What access authorization records am I required to retain?

A1: The NRC considers "documentation regarding the trustworthiness and reliability of individual employees" under § 37.23(h)(1) to include all fingerprint and criminal history records received from the FBI, or a copy if the individual's file has been transferred, and all records from the other background investigation requirements under § 37.25(a)(2) through (a)(7). You are also required under § 37.29(a)(12) to retain any written confirmations received from entities concerning a federal security clearance, any written confirmations received concerning a favorably adjudicated criminal history records check under § 37.29(b), and under § 37.29(a)(13), any written verifications received from service providers. You must also retain a record of your determination bases (reasons for granting unescorted access or denying it) under § 37.23(e)(3). The determination documentation must include the individual's name, and should include: the criteria, procedures, and supporting documentation you used in the process of making the determination for each individual; the date of the determination; and the name and signature of the reviewing official responsible for making it. You are also required to retain copies of the implementation procedures. (See also Q&As on § 37.23(e).)

Q2: What form of documentation do I need to keep for the access authorization program? Must I convert my paper documents to a digital format?

A2: No. You may choose to scan paper and other documents into digital format for your own convenience and economy of storage space, but this is not required. The form of the documentation may be an original or copy, on paper, electronic, or other media,

as long as the record is legible for the required period and can be accessed. To discourage unauthorized alterations, electronic copies should if possible be read-only, such as those in portable document format (pdf).

Q3: What procedures do I need to keep for the access authorization program?

A3: Under § 37.23(h)(2), you need to retain copies of all the procedures required to implement the access authorization program. This may include procedures for obtaining written consent, conducting the investigation and reinvestigation, correcting the record, challenging a determination to deny authorization for unescorted access, and documenting the final determination.

Q4: Do I need to keep any information relating to the lists of individuals approved for unescorted access other than the lists themselves?

A4: No. You are required under § 37.23(h)(3) only to have a copy of the list of individuals who have current unescorted access to the material. When a list is updated, the previous list must be kept as a record for 3 years. No other list-related records need be retained, although you will need to retain background investigation and determination basis related records for each individual on the list.

Q5: Must I also keep a list of individuals who have been denied access?

A5: No. The fact that someone is not included on the access list means that they shouldn't be granted unescorted access to the material, and a list of individuals who have been denied access is not needed.

Q6: How long must the records be maintained?

A6: Background investigation records must be maintained for 3 years after the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material. Under § 37.23(e)(3), these records must also include those that provided the basis for the licensee's determination on whether or not an individual is trustworthy and reliable for unescorted access authorization. The list of individuals approved for unescorted access authorization must be maintained for 3 years after the list is superseded or replaced. Procedures must be retained under § 37.23(h)(3) for 3 years after the procedure has been replaced with a new or revised version.

Q7: If a facility closes and the license is terminated does the licensee need to keep records for an additional 3 years?

A7: No. Once the Commission terminates a license for any reason, the licensee is no longer required under [§ 37.103](#) to maintain its records for the access authorization program, and they may be destroyed. (See also [§ 37.31](#) for requirements on the protection of personal information.)

§ 37.25 Background investigations

§ 37.25(a) Initial Investigation.

Before allowing an individual unescorted access to category 1 or category 2 quantities of radioactive material or to the devices that contain the material, licensees shall complete a background investigation of the individual seeking unescorted access authorization. The scope of the investigation must encompass at least the 7 years preceding the date of the background investigation or since the individual's eighteenth birthday, whichever is shorter. The background investigation must include at a minimum:

EXPLANATION:

These provisions establish the requirement to conduct a background investigation for individuals needing unescorted access to category 1 and category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: How far back in time must I look into an individual's historical information as part of the background investigation?

A1: The scope of the investigation must encompass at least the 7 years preceding the date of the background investigation or since the individual's eighteenth birthday, whichever is shorter. To the extent possible, you should look into their history as far back as is necessary to satisfy yourself that sufficient information is available to meet your criteria for determining trustworthiness and reliability.

Q2: What are the components of a background investigation?

A2: A background investigation includes several components: fingerprinting and an FBI identification and criminal history records check; verifications of the individual's true identity; a review of information obtained about the individual's employment history and education; and a character and reputation determination.

Q3: Why are background investigations and T&R determinations necessary?

A3: The background investigation is a tool to obtain information necessary to make decisions about whether an individual is trustworthy and reliable and may be permitted unescorted access to a category 2 or greater quantity of radioactive material. It is essential to ensure that an individual seeking unescorted access to radioactive material is dependable in judgment, character, and performance, such that unescorted access by that individual to category 1 or category 2 quantities of radioactive material does not constitute an unreasonable risk to the public health and safety or security.

A trustworthiness and reliability determination provides the licensee decision that there is reasonable assurance that the individual allowed unescorted access will not use the material for malicious purposes. This requirement goes beyond access control for

radiation protection purposes, and further limits access to only those individuals who have a legitimate need to access the licensed material or device.

Q4: Are these background investigation requirements equivalent to those used in nuclear power plants?

A4: No. Nuclear power plants have additional requirements such as a credit history check, a psychological assessment, and a behavioral observation program to determine an employee's trustworthiness and reliability (See 10 CFR [73.56](#) and [73.57](#)).

Q5: How does a background investigation assure trustworthiness and reliability?

A5: No background check can provide total assurance that a person granted unescorted access will not use the material for malicious purposes, but the required investigation does provide information to determine with reasonable assurance that the individual is who he or she purports to be. It also provides the licensee information about whether the individual's character, reputation, and behavior might be adverse to the safe and secure operation of the licensee's facility. A background investigation can provide the licensee a reasonable basis to determine that allowing an individual to have unescorted access to the licensed material would not constitute an unreasonable risk of a malevolent use of radioactive materials.

§ 37.25 Background investigations (cont'd)

§ 37.25(a)(1)

Fingerprinting and an FBI identification and criminal history records check in accordance with § 37.27;

EXPLANATION:

This provision requires the background investigation to include fingerprinting and an FBI identification and criminal history records check.

QUESTIONS/ANSWERS:

Q1: Why is the NRC requiring fingerprinting and a criminal history records check for individuals to have unescorted access to category 1 or category 2 quantities of radioactive material?

A1: Section 149 of the [AEA](#) requires fingerprinting and an FBI identification and criminal history records check for “any individual who is permitted unescorted access to radioactive materials or other property subject to regulation by the Commission that the Commission determines to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks.” The Commission determined that category 1 and category 2 quantities of radioactive material are of significance to the public health and safety or the common defense and security. Therefore, individuals who have access to category 1 or category 2 quantities of radioactive material must be fingerprinted.

Fingerprinting an individual for an FBI criminal history records check is an important element of the background investigation. It can provide comprehensive information regarding an individual's recorded criminal activities within the U.S. and its territories, and the individual's known affiliations with violent gangs or terrorist organizations. It is one element of the determination of trustworthiness and reliability. See Q&As for [§ 37.27](#) for more detail.

Q2: Why hasn't the NRC established criteria for making a consistent determination on the finding of the fingerprint reports? Won't this lack of criteria result in inconsistent approval or denial of unescorted access authorizations for people who are trustworthy and reliable?

A2: The NRC took a number of considerations into account when it decided not to provide specific criteria for making decisions about ROs and authorizing unescorted access. Since the individual circumstances of each applicant may vary significantly, each licensee needs the flexibility to establish its own program. Also, because the information obtained from employment history and other background checks may vary widely, and licensees may not be able to obtain sufficient information to determine compliance with all criteria, the licensee is unlikely to avoid having to apply its subjective judgment about an applicant in any case. Moreover, a single set of criteria for application to all cases may not be fair to some individuals who may otherwise be well-qualified. A criterion prohibiting the selection of a candidate with any criminal record less

than 10 years old, for example, might disadvantage otherwise well-qualified candidates, whom a licensee might prefer after taking the candidate's professional qualifications, employment history, character references, and other, more recent information into account. Because the individual circumstances of each individual may vary significantly, each licensee needs the flexibility to establish its own program, using its own criteria.

Although a licensee is allowed to apply criteria that may be inconsistent with those of other licensees, this does not necessarily result in unfairness. One size does not fit all. Some licensees may be more comfortable with someone who has a criminal record, for example, while other licensees may decide that with an ample availability of other qualified applicants, an applicant with such a record may be employable, but should not be allowed unescorted access to the licensee's radioactive material. A criminal record does not by itself mean that an individual is not trustworthy and reliable. The individual may have acknowledged his or her mistake and now be a model citizen. Also, a licensee may always allow an individual unescorted access, but implement additional measures to oversee that individual.

The licensee is in the best position to decide what best fits its needs. Because each licensee will be deciding whether to trust an individual with its assets, licensees have the greatest stake in making a well-informed decision on the person best qualified to fill such a sensitive position. Thus, licensees should be allowed to develop their own criteria for these decisions.

Q3: May I use a contractor to process FBI criminal history record information (CHRI) to meet this requirement?

A3: No. In response to an NRC request for clarification concerning the use of contractors or other third parties for processing CHRI, the FBI analyzed the Commission's AEA authority in 1997 and concluded that the use of private contractors by the NRC and its licensees to receive and process FBI CHRI is prohibited.

§ 37.25 Background investigations (cont'd)

§ 37.25(a)(2) Verification of true identity.

Licensees shall verify the true identity of the individual who is applying for unescorted access authorization to ensure that the applicant is who he or she claims to be. A licensee shall review official identification documents (e.g., driver's license; passport; government identification; certificate of birth issued by the state, province, or country of birth) and compare the documents to personal information data provided by the individual to identify any discrepancy in the information. Licensees shall document the type, expiration, and identification number of the identification document, or maintain a photocopy of identifying documents on file in accordance with § 37.31. Licensees shall certify in writing that the identification was properly reviewed, and shall maintain the certification and all related documents for review upon inspection;

EXPLANATION:

This provision requires background investigations to include verification of the individual's true identity.

QUESTIONS/ANSWERS:

Q1: How does a licensee verify true identity?

A1: To verify the identity of an applicant for access authorization under this subsection, the employer must examine "official identification documents" to determine whether they reasonably appear to be genuine and relate to the individual. The documents should be compared to information provided by the applicant. The document information and the certification of review should be maintained as a record. You are not required to determine that the identification is authentic.

Q2: What documents may be used to verify identity?

A2: You may use identity documents issued by a State or local government or by the Federal government, provided they contain a photograph and information such as name, date of birth, gender, height, eye color, and address. These documents include passports, drivers' licenses, and ID cards issued by government entities. You may use one or more of the documentation types required by the U.S. Citizenship and Immigration Service's (CIS's) I-9 form used to apply for eligibility for employment. The I-9 form contains a list of acceptable documentation types, and is available at no cost at:

<http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnnextoid=31b3ab0a43b5d010VgnVCM10000048f3d6a1RCRD&vgnnextchannel=db029c7755cb9010VgnVCM10000045f3d6a1RCRD>

For the complete list of allowable documents, see p. 5 of the I-9 form. Note that Items B 10-12 generally are not acceptable, unless you believe you need to authorize unescorted access for a minor. These types of documentation (e.g., nursery school

records, report cards, and hospital records) are available only to an applicant under the age of 18 using the I-9 form who is unable to provide one of the other documents listed on this form.

§ 37.25 Background investigations (cont'd)

§ 37.25(a)(3) Employment history verification.

Licensees shall complete an employment history verification, including military history. Licensees shall verify the individual's employment with each previous employer for the most recent 7 years before the date of application;

§ 37.25(a)(4) Verification of education.

Licensees shall verify that the individual participated in the education process during the claimed period;

EXPLANATION:

These provisions require verification of employment history and education as part of the background investigation.

QUESTIONS/ANSWERS:

Q1: Is NRC defining 7 years of employment as “uninterrupted” service, or may there be breaks in service?

A1: There may be breaks in service, but under this subsection, a licensee must go back a minimum of 7 years unless the individual is younger than 25. (For an individual younger than 25, the licensee need only go back to the individual's 18th birthday.) If the individual has gaps in his or her employment record, the licensee should attempt to determine why there are gaps.

Q2: What kind of employment evaluation needs to be conducted if the employee has been with the licensee 7 years or more? Does the education verification need to be performed for a long-term employee?

A2: The licensee may use its own records of employment for an individual employed with the company more than 7 years; there is no need to check any previous employers. The education verification also does not need to be performed, if it occurred more than 7 years ago. If the education verification was performed as a part of the hiring process, this check does not need to be repeated.

Q3: What if a former employer refuses to provide the information I request?

A3: For interviews with past employers, the NRC understands that simple verbal confirmations of past employment and timeframe may be all the information a former employer is willing to provide on an individual. Although a simple confirmation of the nature and timeframe of past employment would not by itself suffice to permit a licensee to find an individual trustworthy and reliable, it would constitute independent corroboration of the accuracy of the individual's information about that period of his or her employment.

§ 37.25 Background investigations (cont'd)

§ 37.25(a)(5) Character and reputation determination.

Licensees shall complete reference checks to determine the character and reputation of the individual who has applied for unescorted access authorization. Unless other references are not available, reference checks may not be conducted 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 any individual who resides in the individual's permanent household. Reference checks under this subpart must be limited to whether the individual has been and continues to be trustworthy and reliable;

EXPLANATION:

This provision requires the background investigation to include a determination of an applicant's character and reputation.

QUESTIONS/ANSWERS:

Q1: What constitutes a character and reputation determination?

A1: This is similar to a reference check for employment. In conducting the reference checks, some things to consider asking are:

- Would you rehire the individual?
- Would you trust the individual with company assets?
- Do 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 reliability?

A licensee may 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, provided that the information is clearly pertinent to the subject individual's likely conduct or behavior if he or she were granted unescorted access to any quantity of radioactive material subject to this Part. In addition to records of any arrest or conviction as an adult or juvenile felon, examples of considerations pertinent to an individual's trustworthiness and reliability may include, but need not be limited to: evidence of false or deceitful statements; loss of a license to drive; repeated high-speed traffic or other violations indicating a reckless disregard for the safety or security of others; a recent bankruptcy, foreclosure, repossession, or garnishment of income; repeated non-payment of alimony, child support, or lawfully incurred financial obligations for periods of months; repeated instances of personal harassment; or conduct or behavior that would violate any of the licensee's corporate or professional codes of ethics or workplace conduct.

Q2: What criteria do I use to evaluate an applicant's character and reputation?

A2: The NRC has not developed a set of criteria for evaluating character and reputation because no such list is likely to cover all individual's circumstances or all licensees' needs. Each licensee is in the best position to weigh the many considerations that must support such evaluations. In addition to the considerations listed in Q&A 1 above, some indicators of character and reputation that licensees should consider for what may be trustworthiness and reliability concerns can also be found in [Annex A](#).

Q3: Reference checks under this subpart "must be limited to whether the individual has been and continues to be trustworthy and reliable." What kinds of information are *not* to be considered relevant to an individual's trustworthiness or reliability?

A3: The "not relevant" category includes information about ethnicity, religious affiliation, ideology or political affiliation, sexual orientation, or membership in any organization that does not advocate, perpetrate, or otherwise support violence against persons, damage to property, or criminal activities including hate crimes. Otherwise, information about any action, behavior, or conduct that is dishonest, deceitful, a conflict of interest or otherwise unethical, or a violation of any law may be considered relevant to an individual's trustworthiness or reliability.

Q4: This subsection provides that unless other references are not available, reference checks "may not be conducted 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 any individual who resides in the individual's permanent household." Does this mean that a licensee may not interview or seek information from any member of a subject individual's family in the course of making a determination about that individual's character or reputation?

A4: No. A licensee may contact family members as a reference check if no other references are available.

§ 37.25 Background investigations (cont'd)

§ 37.25(a)(6)

The licensee shall also, to the extent possible, obtain independent information to corroborate that provided by the individual (e.g., seek references not supplied by the individual); and

§ 37.25(a)(7)

If a previous employer, educational institution, or any other entity with which the individual claims to have been engaged fails to provide information or indicates an inability or unwillingness to provide information within a time frame deemed appropriate by the licensee but at least after 10 business days of the request or if the licensee is unable to reach the entity, the licensee shall document the refusal, unwillingness, or inability in the record of investigation; and attempt to obtain the information from an alternate source.

EXPLANATION:

These provisions require licensees to obtain to the extent possible background investigation information independent from that provided by the individual. Licensees must also document the refusal, unwillingness, or inability of a source to provide information.

QUESTIONS/ANSWERS:

Q1: What type of information is considered independent information to corroborate that provided by the individual?

A1: Independent information may be obtained through interviews with anybody who knows or previously knew the individual—such as teachers, friends, coworkers, neighbors, local members of a church, mosque, synagogue, club, or civic association of which the applicant is a member, or family members. Although information obtained from independent sources may not by itself suffice to permit a licensee to find an individual trustworthy and reliable, it would constitute independent corroboration of the accuracy of the individual's information about that period of his or her life. It may also provide information that could support a decision not to authorize unescorted access.

Q2: What should I do if an individual or entity contacted as part of a background investigation refuses to respond?

A2: If a previous employer, educational institution, or any other entity fails to provide information or indicates an inability or unwillingness to provide information in a timely manner, you are required under § 37.25(a)(7) to document the refusal, unwillingness, or inability to respond in the record of investigation. You must then attempt to obtain confirmation of the applicant's employment or education history or other personal associations from at least one alternate source.

Past employers are often hesitant to say anything about a past employee for fear of being held liable. If you receive any input from a former employer or other reference (even if he or she refuses to comment), you should document the conversation and take

notes about what the former employer or reference said. If attempts to contact the reference fail after several tries, you should make a note of that as well.

A licensee may ask the individual for the name of another co-worker or a second-line supervisor who may be willing to provide confirmation of employment.

Q3: Won't documenting my attempts to obtain information from uncooperative references and alternate sources of information under § 37.25(a)(7) be excessive and time consuming?

A3: Not necessarily. Documentation may consist of an e-mail from such a reference or alternate source, or a note to a file about an interview or phone conversation.

Q4: May I consider credit history as another source of "independent information" in evaluation of an applicant's background?

A4: Yes, although you will need to comply with applicable state laws or local ordinances that prohibit employment discrimination based on credit history. Nothing in the NRC regulations prohibits a licensee from conducting additional types of checks, and you may always use measures beyond the regulatory minimum required by the access authorization program.

§ 37.25 Background investigations (cont'd)

§ 37.25(b) Grandfathering.

§ 37.25(b)(1)

Individuals who have been determined to be trustworthy and reliable for unescorted access to category 1 or category 2 quantities of radioactive material under the Fingerprint Orders may continue to have unescorted access to category 1 and category 2 quantities of radioactive material without further investigation. These individuals shall be subject to the reinvestigation requirement.

§ 37.25(b)(2)

Individuals who have been determined to be trustworthy and reliable under the provisions of part 73 of this chapter or the security orders for access to safeguards information, safeguards information-modified handling, or risk-significant material may have unescorted access to category 1 and category 2 quantities of radioactive material without further investigation. The licensee shall document that the individual was determined to be trustworthy and reliable under the provisions of part 73 of this chapter or a security order. Security order in this context refers to any order that was issued by the NRC that required fingerprints and an FBI criminal history records check for access to safeguards information, safeguards information-modified handling, or risk significant material such as special nuclear material or large quantities of uranium hexafluoride. These individuals shall be subject to the reinvestigation requirement.

EXPLANATION:

These provisions relieve from further investigation individuals who have been determined trustworthy and reliable under comparable NRC-required background investigations.

QUESTIONS/ANSWERS:

Q1: If I have approved an individual for unescorted access under a previously-issued NRC security order, do I need to conduct a new background investigation?

A1: No. Nor do you need to conduct a new background investigation for employees who were granted unescorted access to category 1 or category 2 quantities of radioactive material or access to SGI under legally binding requirements issued by an Agreement State or the NRC. These previously approved individuals are considered to be grandfathered and do not need a new background investigation to meet the new requirements. The individuals will need to undergo a reinvestigation 10 years after the initial determination, however, and that background investigation will need to meet Part 37 requirements for the reinvestigation.

Q2: Do you have grandfather provisions for those who are long-term employees regarding trustworthiness and reliability?

A2: No. Long-term employees are not automatically grandfathered, unless they have previously undergone a background investigation as discussed in Q&A 1 above, or they fall under one of the categories of individuals granted relief from elements of the background investigation. See Q&As on [§ 37.29](#) for additional information on who may be relieved from fingerprinting.

Q3: I have an access authorization covered by Part 73. Do I need to reinvestigate individuals before I allow them to have unescorted access to category 2 or greater quantities of my material?

A3: No. If you have a Part 73 access authorization program, you may grandfather an individual under [§ 37.25\(b\)\(2\)](#) if you document that he or she was determined to be trustworthy and reliable under Part 73 or an NRC security order requiring fingerprints and an FBI criminal history records check for access to SGI, SGI-M, or such risk significant material as special nuclear material or large quantities of uranium hexafluoride.

§ 37.25 Background investigations (cont'd).

§ 37.25(c) Reinvestigations.

Licenseses shall conduct a reinvestigation every 10 years for any individual with unescorted access to category 1 or category 2 quantities of radioactive material. The reinvestigation shall consist of fingerprinting and an FBI identification and criminal history records check in accordance with § 37.27. The reinvestigations must be completed within 10 years of the date on which these elements were last completed.

EXPLANATION:

This provision requires background reinvestigations every 10 years.

QUESTIONS/ANSWERS:

Q1: Why is a reinvestigation required every 10 years?

A1: A reinvestigation every 10 years is necessary because an individual's criminal history may change over time in a manner that can adversely affect his or her trustworthiness and reliability. The 10-year clock begins on the day an individual was given unescorted access to the radioactive material.

Q2: What elements are included in the reinvestigation?

A2: The reinvestigation is not a complete check. It is limited to fingerprinting and the FBI criminal history records check, and need not include identification through employment verification or the character and reputation determination. If the reinvestigation finds new information about a potentially adverse change in the individual's criminal records, however, the licensee may need to gather information from additional sources to consider whether to revise its previous determination about the individual's character and reputation.

Q3: Must I do a reinvestigation of an individual who qualified under § 37.29 for relief from fingerprinting and background investigations, such as an individual approved under another federal security review program?

A3: The relief provided by [§ 37.29](#) does apply to the reinvestigation, but you will need to check and document that the individual still meets the relief category. If the affected individual has an approval that is still valid under another federal security review program, you do not need to conduct a reinvestigation. Under § 37.29(a)(12), however, the individual approved under the other federal security review program must make available the appropriate documentation that he or she has an active Federal security clearance, and you must receive written confirmation from the agency/employer that granted the Federal security clearance or reviewed the criminal history records check.

§ 37.27 Requirements for criminal history records checks of individuals granted unescorted access to category 1 or category 2 quantities of radioactive material

§ 37.27(a) General performance objective and requirements.

§ 37.27(a)(1)

Except for those individuals listed in § 37.29 and those individuals grandfathered under § 37.25(b), each licensee subject to the provisions of this subpart shall fingerprint each individual who is to be permitted unescorted access to category 1 or category 2 quantities of radioactive material. Licensees shall transmit all collected fingerprints to the Commission for transmission to the FBI. The licensee shall use the information received from the FBI as part of the required background investigation to determine whether to grant or deny further unescorted access to category 1 or category 2 quantities of radioactive materials for that individual.

EXPLANATION:

These provisions require licensees to fingerprint individuals to be permitted unescorted access and submit the fingerprints to the NRC for transmission to the FBI.

QUESTIONS/ANSWERS:

Q1: May I work directly with the FBI without having to process the fingerprints through the NRC?

A1: No. The NRC does not have the authority to allow licensees to submit fingerprints directly to the FBI instead of submitting them through the NRC. Section 149 of the AEA requires that "fingerprints obtained by an individual or entity as required [in this section] be submitted to the Attorney General of the United States through the Commission for identification and a criminal history records check." The NRC recognizes that some licensees may work directly with the FBI to process fingerprints to meet other requirements for criminal history checks. To meet the requirements of Part 37, however, the licensee will still have to process fingerprints through the NRC to the FBI, unless the individual is covered under by a relief category in § 37.29.

§ 37.27(a) General performance objective and requirements (cont'd).

§ 37.27(a)(2)

The licensee shall notify each affected individual that his or her fingerprints will be used to secure a review of his or her criminal history record, and shall inform him or her of the procedures for revising the record or adding explanations to the record.

§ 37.27(a)(3)

Fingerprinting is not required if a licensee is reinstating an individual's unescorted access authorization to category 1 or category 2 quantities of radioactive materials if:

§ 37.27(a)(3)(i)

The individual returns to the same facility that granted unescorted access authorization within 365 days of the termination of his or her unescorted access authorization; and

§ 37.27(a)(3)(ii)

The previous access was terminated under favorable conditions.

§ 37.27(a)(4)

Fingerprints do not need to be taken if an individual who is an employee of a licensee, contractor, manufacturer, or supplier has been granted unescorted access to category 1 or category 2 quantities of radioactive material, access to safeguards information, or safeguards information-modified handling by another licensee, based upon a background investigation conducted under this subpart, the Fingerprint Orders, or part 73 of this chapter. An existing criminal history records check file may be transferred to the licensee asked to grant unescorted access in accordance with the provisions of § 37.31(c).

§ 37.27(a)(5)

Licensees shall use the information obtained as part of a criminal history records check solely for the purpose of determining an individual's suitability for unescorted access authorization to category 1 or category 2 quantities of radioactive materials, access to safeguards information, or safeguards information-modified handling.

EXPLANATION:

These provisions establish requirements for reinstatement of unescorted access authorizations, and for the use of information from previous background investigations.

QUESTIONS/ANSWERS:

Q1: Am I obligated to tell an individual why he or she is being fingerprinted?

A1: Yes. Under § 37.27(a)(2), you must inform the individual that his or her fingerprints will be used to conduct a criminal history records check.

Q2: How should I inform the individual?

A2: You may inform the individual orally or in writing. However, you are required to obtain signed consent to conduct the background investigation. See also Q&As on [§ 37.23\(c\)](#).

Q3: If an employee who has unescorted access quits and then returns, does the licensee need to fingerprint the individual again?

A3: If the employee has been gone for 365 days or less, left under favorable conditions, and had previously undergone fingerprinting and an FBI criminal history records check, the individual will not need to be fingerprinted again. If the individual's unescorted access had been terminated for cause, however, the individual will need to be fingerprinted again.

Q4: Do I need to obtain fingerprints of service provider licensees and other individuals who have been granted unescorted access by the service provider or other licensee?

A4: No. You do not need to obtain fingerprints of individuals employed by a service provider licensee if that licensee meets the requirements of Part 37. Employees of these service provider licensees working at a customer's facility need not go through the customer's process for determining trustworthiness and reliability for granting unescorted access. Rather, because the service provider licensee has already made its own determination of trustworthiness and reliability for its employees, the service provider licensee may provide its customers with certification of an individual's trustworthiness and reliability for being granted unescorted access. The service provider licensee's program must meet the requirements of Subpart B of Part 37, however. The licensee will still need to determine that the individual should be granted unescorted access and document your basis. The licensee is not required to accept the service provider's certification and can choose to escort the individual(s).

Q5: May I use information obtained as part of a criminal history records check for other purposes?

A5: No. You may use the information obtained under this Part only to determine suitability for either access to SGI or unescorted access to a category 1 or category 2 quantity of radioactive material.

§ 37.27(b) Prohibitions.

§ 37.27(b)(1)

Licensees may not base a final determination to deny an individual unescorted access authorization to category 1 or category 2 quantities of radioactive material solely on the basis of information received from the FBI involving:

§ 37.27(b)(1)(i)

An arrest more than 1 year old for which there is no information of the disposition of the case; or

§ 37.27(b)(1)(ii)

An arrest that resulted in dismissal of the charge or an acquittal.

§ 37.27(b)(2)

Licensees may not use information received from a criminal history records check obtained under this subpart in a manner that would infringe upon the rights of any individual under the First Amendment to the Constitution of the United States, nor shall licensees use the information in any way that would discriminate among individuals on the basis of race, religion, national origin, gender, or age.

EXPLANATION:

These provisions prohibit the use of certain background investigation information.

QUESTIONS/ANSWERS:

Q1: Why can't I deny an individual unescorted access authorization based solely on FBI information about an arrest that resulted in a dismissal or acquittal, or an arrest more than 1 year old for which there is no information on the disposition of the case?

A1: This misuse of such information would be a violation of NRC regulations and federal law. Section 149(c)(2)(C) of the [AEA](#) requires that Commission regulations for the use of FBI criminal history records check information "ensure that no final determination may be made solely on the basis of information provided under this section involving ...an arrest more than 1 year old for which there is no information of the disposition of the case; or ... an arrest that resulted in dismissal of the charge or an acquittal." Taking such action on an incomplete record might unfairly penalize the individual. It is possible that the charges have been dropped, or the individual found innocent and the record never updated to reflect the additional information.

§ 37.27(c) Procedures for processing of fingerprint checks.

§ 37.27(c)(1)

For the purpose of complying with this subpart, licensees shall use an appropriate method listed in § 37.7 to submit to the U.S. Nuclear Regulatory Commission, Director, Division of Facilities and Security, 11545 Rockville Pike, ATTN: Criminal History Program/Mail Stop TWB-05 B32M, Rockville, MD 20852, one completed, legible standard fingerprint card (Form FD-258, ORIMDNRCOOOZ), electronic fingerprint scan or, where practicable, other fingerprint record for each individual requiring unescorted access to category 1 or category 2 quantities of radioactive material. Copies of these forms may be obtained by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, by calling (630) 829-9565, or by e-mail to FORMS.Resource@nrc.gov. Guidance on submitting electronic fingerprints can be found at <http://www.nrc.gov/site-help/e-submittals.html>, by calling (630) 829-9565, or by e-mail to FORMS.Resource@nrc.gov. Guidance on submitting electronic fingerprints can be found at <http://www.nrc.gov/site-help/e-submittals.html>.

§ 37.27(c)(2)

Fees for the processing of fingerprint checks are due upon application. Licensees shall submit payment with the application for the processing of fingerprints through corporate check, certified check, cashier's check, money order, or electronic payment, made payable to "U.S. NRC." (For guidance on making electronic payments, contact the Security Branch, Division of Facilities and Security at (301) 492-3531.) Combined payment for multiple applications is acceptable. The Commission publishes the amount of the fingerprint check application fee on the NRC public Web site. (To find the current fee amount, go to the Electronic Submittals page at <http://www.nrc.gov/site-help/e-submittals.html> and see the link for the Criminal History Program under Electronic Submission Systems.)

§ 37.27(c)(3)

The Commission will forward to the submitting licensee all data received from the FBI as a result of the licensee's application(s) for criminal history records checks.

EXPLANATION:

These provisions establish procedures for processing fingerprint checks.

QUESTIONS/ANSWERS:

Q1: Where do I submit the fingerprints for processing?

A1: Under the AEA, you are required to submit the fingerprints to the NRC, which forwards the fingerprints to the FBI for processing. If an individual comes under one of the relief categories specified in § 37.29, you will not need to submit the individual's fingerprints to the NRC. A completed fingerprint card (form FD-258) should be sent to:

U.S. Nuclear Regulatory Commission

Director, Division of Facilities and Security
11545 Rockville Pike
Attn: Criminal History Program/Mail Stop – TWB-05B32M
Rockville, MD 20852

Q2: How can I obtain more fingerprint cards?

A2: You can request more fingerprint cards (form FD-258) by writing to the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555, by calling (630) 829-9565, or by e-mail to forms.resource@nrc.gov.

Q3: What information do I need to include on the fingerprint card?

A3: Licensees need to include the following information on each fingerprint card:

- a. Last name, first name, middle name
- b. Signature of person being fingerprinted
- c. Residence of person being fingerprinted (e.g., nearest town, state or territory, and zip code.)
- d. Date
- e. Signature of official taking the fingerprints
- f. Address of employer taking fingerprints
- g. Reason for being fingerprinted (e.g., Part 37 regulatory requirement)
- h. Aliases
- i. Citizenship
- j. Social security number and any of the other corresponding numbers requested on the card if applicable (SSN only; no passport or other ID numbers. If the individual does not have an SSN, leave this box blank.)
- k. Date of birth
- l. Place of birth
- m. Sex
- n. Race (e.g., A – Asian or Pacific Islander, B – Black, H – Hispanic/Latino, I – American Indian or Alaskan Native, W – White)
- o. Height
- p. Weight
- q. Eye color (BLK – Black, BLU – Blue, BRO – Brown, GRY – Gray, GRN – Green, HAZ – Hazel, MAR – Maroon, MUL – Multicolored, PNK – Pink)
- r. Hair color (BAL – Bald, BLK – Black, BLN – Blond, BLU – Blue, BRO – Brown, GRY – Gray or Partially, GRN – Green, ONG – Orange, PNK – Pink, PLE – Purple, RED – Red or Auburn, SDY – Sandy, XXX – Unknown, WHI – White)

NRC Licensees should use their NRC docket number in the field "YOUR NO. OCA." Agreement State licensees should use their two letter State abbreviation followed by a dash and the licensee's license number. For new license applications, an Agreement State may not be able to provide a license number prior to license issuance. In this situation, the Agreement State should create a unique identification number for the applicant for the purpose of completing the fingerprinting card (e.g. CA-123456). The number must be unique for each applicant and not repeated once used. Incomplete fingerprint cards will not be processed and will be returned to the licensee.

Q4: May I use fingerprint cards I obtain from my LLEA?

A4: No. Cards from other sources cannot be used because of past problems with some of the cards.

Q5: Who may fingerprint my employees?

A5: You should have their fingerprints taken by an authorized official, such as a representative from a LLEA. An official authorized, for this purpose could also be available through private entities, contractors, or an established on-site fingerprinting program. Note, however, that under § 37.23(b)(2), the fingerprints of the nominated reviewing official must be taken by a law enforcement agency, a Federal or State agency that provides finger printing services to the public, or a commercial fingerprinting service authorized by a State to take fingerprints.

With the exception of the RO, there is no limitation on who may take the fingerprints. If you have fingerprints taken at a facility other than that of a recognized Federal, State, or local law enforcement agency, however, you should ensure that the prints are taken legibly and match the identity of the individual named on the fingerprint card. In these cases, the individual taking fingerprints should at a minimum:

1. Be trained to take fingerprints. (Training to take fingerprints is offered through the FBI, or may be available from local law enforcement agencies and some professional associations.);
2. Verify the identity of the individual being fingerprinted by checking a government-issued picture identification (*e.g. a passport or driver's license*) and verify that the name on the card matches the government-issued identification; and
3. Sign the block on the fingerprint card labeled "SIGNATURE OF OFFICIAL TAKING THE FINGERPRINTS."

Q6: Is there a fee associated with NRC's processing of the fingerprints?

A6: Since December 1, 2009, the fee to process each fingerprint card has been \$26.00. The fee does change on occasion, however, so you should check before submitting your fee payment. The NRC publishes the amount of the fingerprint check application fee on the NRC public web site. (To find the current fee amount, go to the Electronic Submittals page at <http://www.nrc.gov/site-help/e-submittals.html> and select the link for the Criminal History Program.) Additional fees may be charged by the entity taking the fingerprints.

Fees for the processing of fingerprint checks are due upon application. Under § 37.27(c) (2), licensees must submit payment with the application for the processing of fingerprints through corporate check, certified check, cashier's check, money order, or electronic payment, made payable to "U.S. NRC." (For guidance on making electronic payments, contact the Facilities Security Branch, Division of Facilities and Security at (301) 492-3531). Combined payment for multiple applications is acceptable.

Q7: May the NRC waive the fee for processing the fingerprints?

A7: No. The NRC by law may not waive or reduce the fee for processing the fingerprints. Subparagraph a.(3) of Section 149 of the AEA explicitly requires that the costs of an identification or records check be paid by the individual or entity required to conduct the fingerprinting.

Q8: What method of payment does the NRC accept?

A8: NRC's preferred method of payment is electronic payment through Pay.gov at <http://www.pay.gov>. Payments through Pay.gov can be made directly from the Licensee's credit or debit card. Licensees will need to establish a password and user ID before they can access Pay.gov. To establish an account, licensee requests must be sent to paygo@nrc.gov. The request must include the licensee's name, address, point of contact, e-mail address, and phone number. The NRC will forward each request to Pay.gov and someone from Pay.gov will contact the licensee with all of the necessary account information.

Licensees using Pay.gov must make payments for processing before submitting applications for fingerprint checks to the NRC. Combined payment for multiple applications is acceptable. Licensees must include the Pay.gov payment receipt(s) along with the application(s).

For additional guidance on making electronic payments, contact the Facilities Security Branch, Division of Facilities and Security, at (301)492-3531. The NRC also accepts checks, cashier checks, or money orders made out to the U.S. Nuclear Regulatory Commission along with the submission of fingerprint cards. Fingerprint cards along with Pay.gov receipt, check, cashier check or money order should be sent to:

Division of Facilities and Security
Mail Stop TWB-05 B32M
Attn: Criminal History Program
U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD. 20852-2738

Q9: When making a payment to the NRC through Pay.gov for processing of fingerprints, Pay.gov requires a TCN. What is a TCN, and what information should go in this field?

A9: TCN stands for "Transaction Control Number." It is a tool for licensees to track their submissions and may include as much identifying information as would be useful for that purpose. For instance, licensees may include the names of one or more individuals for whom payment is being made, the licensee's name, and the date of submittal. Since that field is on the pay.gov form, the field may be used for individuals' names or any other identifying information.

Q10: May I submit my fingerprint cards electronically to the NRC?

A10: Yes. Some licensees may choose to make arrangements to submit fingerprints electronically to the NRC, but for many licensees, the cost of electronic fingerprinting equipment may be prohibitive. To establish an electronic fingerprinting program with the NRC, please contact NRC's Facility Security Branch at 301-492-3531. Please note that

under § 37.7, electronic submissions must be made in a manner that enables the NRC to receive, read, authenticate the sender, and forward the submission to the U.S. Attorney General for FBI processing. Any fingerprint equipment to be used for the purposes of complying with the fingerprinting requirements will need to be certified by the FBI for quality and performance standards. The NRC and FBI systems are capable of receiving Electronic Fingerprint Transmission Specifications (EFTS) fingerprints, either Type 4 (rolled prints) or Type 14 (flat prints). A sample listing of FBI-certified fingerprint equipment is available at: <https://www.fbibiospecs.org/iafis/>.

Q11: What happens to the fingerprint cards after the NRC receives them from the licensee?

A11: The NRC scans the fingerprint cards to transmit to the FBI electronically. The cards are retained and secured for approximately a month, and destroyed thereafter in accordance with federal guidelines.

Q12: Why might a fingerprint card be unclassifiable?

A12: Fingerprints may be unclassifiable for a number of reasons, including:

1. Incomplete impressions (fingers not completely rolled from one side of the nail to the other).
2. Left and right hands reversed on the fingerprint card.
3. The same hand or finger printed twice on the card.
3. Fingerprints are not clear and distinct (e.g., smudged, uneven, or too dark or light).
4. Fingers on the card are missing or partially missing without an explanation.

To avoid rejection of fingerprints by the FBI as "unclassifiable," the individual taking the prints should ensure that they are of good quality and do not include any of these deficiencies, and should also follow the instructions on the back of the fingerprint card. Fingerprint cards with incomplete or missing information will be returned to the licensee to provide complete information, resulting in a delay in processing.

The FBI has provided guidance on the taking of fingerprints for submission to the FBI at <http://www.fbi.gov/hq/cjisd/takingfps.html>. This guidance also discusses special situations, such as fingerprinting an individual with abnormalities of the fingers, thumbs or hands, and the appropriate way to identify such situations on the fingerprint card. The guidance also includes a checklist to verify that the fingerprint impressions meet the FBI's requirements.

Q13: What are the next steps in the process if the FBI rejects a Form FD-258 (fingerprint card) because the fingerprints are not classifiable? What options are available to licensees if, after multiple attempts, an individual's fingerprints cannot be classified based on conditions other than poor quality?

A13: If the initial fingerprint submission is returned by the FBI because the fingerprint impressions cannot be classified, the fingerprints may be retaken and resubmitted (i.e., new Form-258 or electronic submission) for a second attempt. The licensee will not be charged for the resubmission if the licensee provides a copy of the FBI TCN or the FBI response indicating the fingerprints could not be classified. If the FBI is unable to

classify the second submission of fingerprints, the licensee may submit additional fingerprint impressions for the individual, as follows:

1. The third fingerprint card submission will require payment of an additional \$26 processing fee.
2. If the third submission is also returned as unclassifiable, the licensee may submit a fourth set of fingerprints. An additional fee is not required because the fee for the third submission includes one resubmission. As with the second submission, the FBI response or TCN should be included, or the submission may be treated as a new request and an additional fee may be charged. Please note that a licensee may opt to take and submit the third and fourth sets of fingerprints together to avoid a potential delay in the response. If the third set is returned as unclassifiable, the NRC will automatically resubmit the fourth set.
3. If the fourth submission is returned as unclassifiable, the licensee should submit six (6) additional fingerprint cards for the individual. All six cards will be forwarded to the FBI, who will take what they believe to be the best quality prints from each card to make a complete set of fingerprints. An additional \$26 processing fee is required and covers the processing of all six fingerprint cards, but does not include an additional resubmission.
4. If the FBI is unable to obtain classifiable fingerprints from the six cards, **based on conditions other than poor quality** (e.g., medical conditions or physical anomalies that prevent the taking of readable prints), then the NRC will automatically request a check based on a name search for the individual, and will forward the results to the licensee.
5. No further submissions will be required, and the licensee may consider the results of the name search-FBI identification and criminal history records check as a component in determining trustworthiness and reliability.

The NRC will consider licensee requests for deviation from the above process for good cause (e.g., a demonstrated history of difficulty providing classifiable fingerprints during other fingerprinting programs or a documented medical condition or physical anomaly that can prevent the taking of readable prints). Licensees may submit a request for consideration of alternatives, and provide the basis for the need for an alternative process to NRC's Facilities Security Branch in the Division of Facilities and Security (requests may be made by phone at 301-492-3531 or mailed to:

Office of Administration
Division of Facilities and Security
Mail Stop TWB-05 B32M
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0012

Please note that requests for an alternative to the above process will not affect a licensee's responsibility to fingerprint individuals for unescorted access or to comply with the trustworthiness and reliability requirements.

Licensees should be aware that Steps 3 and 4 above do not occur often, and should take notice that Step 4 may occur *only* in instances where the FBI has determined that the fingerprints cannot be classified based on conditions other than poor quality. Failure to provide quality fingerprint impressions may result in the disqualification of the individual from further consideration for unescorted access

§ 37.29 Relief from fingerprinting, identification, and criminal history records checks and other elements of background investigations for designated categories of individuals permitted unescorted access to certain radioactive materials

§ 37.29(a)

Fingerprinting, and the identification and criminal history records checks required by section 149 of the Atomic Energy Act of 1954, as amended, and other elements of the background investigation are not required for the following individuals prior to granting unescorted access to category 1 or category 2 quantities of radioactive materials:

§ 37.29(a)(1)

An employee of the Commission or of the Executive Branch of the U.S. Government who has undergone fingerprinting for a prior U.S. Government criminal history records check;

§ 37.29(a)(2)

A Member of Congress;

§ 37.29(a)(3)

An employee of a member of Congress or Congressional committee who has undergone fingerprinting for a prior U.S. Government criminal history records check;

§ 37.29(a)(4)

The Governor of a State or his or her designated State employee representative;

§ 37.29(a)(5)

Federal, State, or local law enforcement personnel;

§ 37.29(a)(6)

State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives;

§ 37.29(a)(7)

Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i. of the Atomic Energy Act;

§ 37.29(a)(8)

Representatives of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who have been certified by the NRC;

§ 37.29(a)(9)

Emergency response personnel who are responding to an emergency;

§ 37.29(a)(10)

Commercial vehicle drivers for road shipments of category 2 quantities of radioactive material;

§ 37.29(a)(11)

Package handlers at transportation facilities such as freight terminals and railroad yards;

§ 37.29(a)(12)

Any individual who has an active Federal security clearance, provided that he or she makes available the appropriate documentation. Written confirmation from the agency/employer that granted the Federal security clearance or reviewed the criminal history records check must be provided to the licensee. The licensee shall retain this documentation for a period of 3 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material; and

§ 37.29(a)(13)

Any individual employed by a service provider licensee for which the service provider licensee has conducted the background investigation for the individual and approved the individual for unescorted access to category 1 or category 2 quantities of radioactive material. Written verification from the service provider must be provided to the licensee. The licensee shall retain the documentation for a period of 3 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section identifies the categories of individuals who may be relieved from the background investigation elements. In addition, it establishes the conditions under which a licensee may accept a federal agency security clearance or the T&R determination of a service provider licensee.

QUESTIONS/ANSWERS:

Q1: What is the basis for relieving individuals from fingerprinting and criminal history records check requirements?

A1: Under section 149.b. of Chapter 12 of the [AEA](#), the NRC may by rule relieve individuals from the fingerprinting, identification, and criminal history records check

requirements if it finds that such action is “consistent with its obligations to promote the common defense and security and to protect the health and safety of the public.”

Q2: How may I determine if an individual has undergone a previous background investigation and falls under one of the categories listed in § 37.29?

A2: For some categories of individuals, it will be obvious. A police officer, NRC employee, or State employee, for example, will have identification of some sort that identifies the individual and his or her employer, so that no further checking will be necessary. For those categories of individuals where it is not obvious, either the individual or the individual’s employer will need to provide documentation.

Q3: What type of documentation is necessary?

A3: Under § 37.29(a)(12)), documentation must consist of written confirmation from the agency or employer that granted a Federal security clearance or reviewed the criminal history records check. Documentation may be a confirmation letter that the named individual has a security clearance meeting the requirements of Subpart B and issued on a specified date. Documentation may also consist of a copy of the background investigation determination itself if the agency or employer provides it.

To show that the service provider’s employee has undergone a background check under § 37.29(a)(13), equivalent to that required under § 37.25, the service provider licensee must provide the service recipient licensee a written communication that includes the name and identifying information of the employee who will be providing the service, and an affirmation that this employee has been determined to be trustworthy and reliable in accordance with the requirements in 10 CFR 37.25(a)(1) through (a)(7). To comply with these requirements, the service provider’s background investigation must include: fingerprinting and an FBI identification and criminal history records check; verifications of the individual’s true identity, employment history, and education; and a character and reputation determination.

Q4: How long must I keep documentation records?

A4: You must keep the records under § 37.23(h)(1) for at least 3 years after the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material, or, under § 37.103, until your license is terminated, whichever comes first.

Q5: May emergency first responders, such as police and fire department personnel, be deemed trustworthy and reliable without a background check?

A5: Yes. NRC, state radiation-protection agency, and local law enforcement officials are relieved from the background investigation elements for purposes of this requirement. In the event of an emergency, such as a fire or explosion, firefighters may be granted unescorted access for the purposes of controlling the emergency situation. Firemen are not provided relief from the background investigation for routine inspections that the fire department may conduct.

Q6: May properly qualified security equipment vendors and/or service providers be considered trustworthy and reliable and granted unescorted access to the radioactive material or devices containing the radioactive material?

A6: Yes, provided that the vendor/service provider meets the requirements of Part 37. Employees of the vendor/service provider licensees need not go through the customer's process for determining their trustworthiness and reliability for unescorted access at a customer's facility. Rather, if the vendor/service provider licensee has made its own determination of trustworthiness and reliability for its personnel, this licensee may provide its customers a certification of each employee's trustworthiness and reliability for being granted unescorted access. The vendor/service provider's program must, however, meet the requirements of Subpart B of Part 37.

Q7: What does NRC mean by "commercial driver" in § 37.29(a)(10)?

A7: A commercial driver is someone who drives commercial vehicles for a living. For example, someone driving for Fed Ex or UPS (United Parcel Service) is considered a commercial driver. The NRC will rely on DOT and Transportation Security Administration (TSA) programs for background investigations of these personnel. Note that this relief is only provided for individuals transporting category 2 quantities of radioactive material. A commercial driver transporting a category 1 quantity will need to undergo a background investigation. An individual who works for the licensee and drives a company truck between radiography jobs will not be considered to be a commercial driver and will need to undergo a background investigation before having unescorted access to a category 1 or category 2 quantity of radioactive material.

Q8: Why are commercial drivers and package handlers relieved from undergoing background checks under Part 37?

A8: These individuals are typically outside the control of the licensee and the licensee would have no way of knowing or influencing who those individuals might be. The NRC will rely on the U.S. DOT and TSA programs for background investigations of these individuals. While the background investigation may not be identical to those required under Part 37, the NRC believes that the potential risk that a commercial driver or package handler might pose due to any difference in the background investigation is acceptably small.

Q9: If an individual falls under one of the categories listed for relief in § 37.29, am I required to grant the individual unescorted access to the material?

A9: No. Part 37 does not require that unescorted access to any radioactive materials or other property subject to regulation by the NRC be granted to any individual. You will still need to decide whether to grant or deny an individual unescorted access independently of whether he or she qualifies for relief from fingerprinting and other background investigation elements under one of the categories in § 37.29. This section simply makes clear that a licensee may permit unescorted access to certain categories of individuals without performing a background investigation if these officials are otherwise qualified for access and have a demonstrated need for it. Any training required under § 37.43(c) will need to be conducted before such individuals may be granted unescorted access, however.

Q10: Would State Radiation Control Program Directors or their designated State employee representatives be exempt from background checks under Part 37 even if their need for unescorted access is not security-related, such as in a safety inspection?

A10: Yes. These officials are relieved from the background investigation elements under § 37.29(a)(6).

Q11: Am I required to allow an NRC or Agreement State inspector unescorted access?

A11: No. The requirement under [§ 37.105](#), for example, to provide inspectors access to your facilities and records does not require you to provide unescorted access. You may always escort the inspector(s) when they are in a security zone or inspecting protected information.

§ 37.29 Relief from fingerprinting, identification, and criminal history records checks (cont'd)

§ 37.29(b)

Fingerprinting, and the identification and criminal history records checks required by section 149 of the Atomic Energy Act of 1954, as amended, are not required for an individual who has had a favorably adjudicated U.S. Government criminal history records check within the last 5 years, under a comparable U.S. Government program involving fingerprinting and an FBI identification and criminal history records check provided that he or she makes available the appropriate documentation. Written confirmation from the agency/employer that reviewed the criminal history records check must be provided to the licensee. The licensee shall retain this documentation for a period of 3 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material. These programs include, but are not limited to:

§ 37.29(b)(1)

National Agency Check;

§ 37.29(b)(2)

Transportation Worker Identification Credentials (TWIC) under 49 CFR 1572;

§ 37.29(b)(3)

Bureau of Alcohol, Tobacco, Firearms, and Explosives background check and clearances under 27 CFR 555;

§ 37.29(b)(4)

Health and Human Services security risk assessments for possession and use of select agents and toxins under 42 CFR 73;

§ 37.29(b)(5)

Hazardous Material security threat assessment for hazardous material endorsement to commercial drivers license under 49 CFR 1572; and

§ 37.29(b)(6)

Customs and Border Protection's Free and Secure Trade (FAST) Program.

EXPLANATION:

Individuals with a favorably-adjudicated U.S. Government criminal history records check under a comparable federal program within the last 5 years may be relieved from the Part 37 fingerprinting and FBI criminal history records check. The other elements of the required background investigation must be conducted.

QUESTIONS/ANSWERS:

Q1: What does it mean for an individual to have a “favorably adjudicated” U.S. Government criminal history records check?

A1: You may consider an individual's criminal history records check to have been “favorably adjudicated” if the individual is authorized under the applicable program to conduct the activity for which the check was made. As noted in § 37.29(b), the adjudication must have been conducted within the last 5 years, under a comparable U.S. Government program involving fingerprinting and an FBI identification and criminal history records check such as those programs listed.

Q2: What does NRC consider a comparable U.S. Government program?

A2: A comparable U.S. Government program is one that requires an individual to submit fingerprints for an FBI criminal history records check. In most cases the Government agency would issue an approval that could include an identification card or a specific approval to work in certain areas. Comparable U.S. Government programs include:

- National Agency Check (NAC)
- Transportation Worker Identification Credentials (TWIC)
- Bureau of Alcohol, Tobacco, Firearms, and Explosives background check and clearances under 27 CFR 555;
- Health and Human Services security risk assessments for possession and use of select agents and toxins under 42 CFR 73;
- Hazardous Material security threat assessment for hazardous material endorsement to commercial drivers license under 49 CFR 1572; and
- Customs and Border Protection’s Free and Secure Trade (FAST) Program

Q3: What documentation must I have in order to accept the individual's claim that he or she has been favorably adjudicated?

A3: Under § 37.29(b), the individual must make available documentation that his or her adjudication is currently valid, and you must receive written confirmation from the agency/employer that reviewed the criminal history records check.

Q4: May I grant unescorted access to category 2 or greater quantities of radioactive materials to an individual relieved from fingerprinting and criminal history investigation without any other checks?

A4: No. You are still required to fulfill the requirements of § 37.25(a)(2) through (a) (6) for other elements of the background investigation. These elements include verification of true identity, verification of employment and education, a character and

reputation determination, and an acquisition and, to the extent possible, an evaluation of information obtained from sources independent of those provided by the individual. After completing these checks, you may then grant unescorted access, if the individual's job duties require it.

Q5: When an individual has been favorably adjudicated under a “comparable U.S. Government program” under § 37.29(b), does this mean comparable to one of the programs listed under § 37.29(b)(1) through (b)(6) above, or comparable to the background investigation requirements of Part 37?

A5: To be “comparable” for the purposes of § 37.29(b), the e program must include fingerprinting and an FBI criminal history records check.

Q6: Do I need to obtain a signed consent from an individual who has undergone a fingerprinting and a criminal history records check under a comparable federal program?

A6: Yes, you will need a signed consent from an employee who has undergone fingerprinting and a criminal history records check under a comparable federal program because you will still need to conduct the other elements of the background investigation required by § 37.25. These other elements include verification of the individual's true identity and employment and education history, and an evaluation of his or her character and reputation.

Q7: Must I do a reinvestigation of an individual who qualified for relief from fingerprinting and background investigations, such as an individual approved under another federal security review program under § 37.29(b)?

A7: The relief provided by § 37.29 does apply to the reinvestigation, but you will need to check and document that the individual still meets the relief category. If the affected individual has an approval that is still valid under another federal security review program, you do not need to conduct a reinvestigation.

§ 37.31 Protection of information

§ 37.31(a)

Each licensee who obtains background information on an individual under this subpart shall establish and maintain a system of files and written procedures for protection of the record and the personal information from unauthorized disclosure.

EXPLANATION:

Licensees must establish and maintain a filing system and written procedures to protect from unauthorized disclosure records and personal information produced from background investigations under Part 37.

QUESTIONS/ANSWERS:

Q1: Are licensees required to protect information obtained during a background investigation?

A1: Yes. The collected information will likely contain personally identifiable information (PII), and should be provided only to authorized individuals. Under § 149(c) (2)(D) of the AEA, as amended, the Commission is required to 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.” Accordingly, under § 37.31(a), the licensee is required to establish and maintain a system of files and procedures to protect the information from disclosure to any unauthorized person. It is a good practice to store background investigation documentation in a locked drawer or file cabinet.

Q2: What does NRC consider to be “unauthorized disclosure?”

A2: NRC considers “disclosure” to be the providing, either deliberately or inadvertently, of any information obtained in a background investigation in accordance with this subpart by any means, including electronic means such as fax, voice mail, or e-mail. Such disclosure is “unauthorized” if the recipient of the information is not the subject individual, the individual’s representative, an authorized representative of the NRC or an Agreement State agency, or a reviewing official. (See § 37.31(b).)

Q3: If I need to prepare an information protection program for my employees’ background investigation information, and I want someone other than the RO or other physical security staff (e.g., an information technology specialist) to prepare the program, do I have to conduct a full background investigation on that individual, even if he or she does not require access to radioactive material to perform a job duty?

A3: No, an individual preparing an information protection program for the access authorization program is not required to undergo a background investigation.

Q4: Should my procedures for information protection address the destruction of records?

A4: This section does not explicitly require that your information protection procedures address the destruction of records, but this would be a good practice, especially for PII. PII is information that can be used, by itself or in combination with other information, to distinguish or trace an individual's identity. It includes such information as an individual's Social Security number, date and place of birth, mother's maiden name, biometric records, and records of his or her education, financial transactions, and employment or medical history. To prevent an unauthorized individual from gaining access to records containing PII, they should be destroyed, by shredding, burning, pulping, degaussing, or a similarly irreversible method. For more information and guidance on protecting PII, a 2007 [Office of Management and Budget \(OMB\) memorandum](#) to federal agencies may be useful. You should also check for applicable state or local government requirements for PII protection and destruction.

§ 37.31 Protection of information (cont'd)

§ 37.31(b)

The licensee may not disclose the record or personal information collected and maintained to persons other than the subject individual, his or her representative, or to those who have a need to have access to the information in performing assigned duties in the process of granting or denying unescorted access to category 1 or category 2 quantities of radioactive material, safeguards information, or safeguards information-modified handling. No individual authorized to have access to the information may disseminate the information to any other individual who does not have a need to know.

EXPLANATION:

This provision restricts the disclosure or re-dissemination of personal information collected under Part 37 background investigations.

QUESTIONS/ANSWERS:

Q1: Under what circumstances may I disclose the personal information obtained during a background investigation?

A1: You may disclose the information to the subject individual, his or her representative, a duly authorized representative of NRC or an Agreement State agency, or an individual with a need for access to the information to perform an assigned duty supporting a decision on unescorted access to SGI, SGI-M, or to a quantity of radioactive material subject to Part 37. If you have a question whether an individual has a need to know the information, you should verify the need before providing the information. You may want to contact your supervisor to see if the request is legitimate. It is good practice to ask the requestor to put the request in writing, specify the nature of the information requested, and document the requestor's need to know. State, local, or federal law may also require disclosure for such purposes as criminal investigations.

Q2: How do I determine that another person requesting access to these records or personal information has a need to know?

A2: If it is not the individual or an NRC or Agreement State inspector, you should inquire why the individual needs the information. You may contact the individual's supervisor to verify the need for the information. If the individual is from another company, you will need to find out why he or she is requesting the information. You will want to make sure that the request is legitimate and determine whether your company will comply with the request. You are not required to share information with other licensees.

Q3: Do I need to document a need to know?

A3: There is no specific requirement in Part 37 to document a need to know, but you should consider this a prudent practice to enable you to demonstrate compliance with

the requirement not to disseminate the information to any other individual who does not have a need to know.

§§ 37.31 Protection of information (cont'd)

37.31(c)

The personal information obtained on an individual from a background investigation may be provided to another licensee:

37.31(c)(1)

Upon the individual's written request to the licensee holding the data to disseminate the information contained in his or her file; and

37.31(c)(2)

The recipient licensee verifies information such as name, date of birth, social security number, gender, and other applicable physical characteristics.

EXPLANATION:

These provisions establish conditions under which personal information obtained on an individual from a background investigation may be provided to another licensee.

QUESTIONS/ANSWERS:

Q1: May one licensee transfer personal information it obtained during an investigation to another licensee?

A1: Yes, if the subject individual makes a written request to the licensee to transfer the information contained in his or her file.

Q2: If I receive background investigation information from another licensee, may I rely on that information, or must I re-verify it?

A2: Unless the information is older than the 10-year reinvestigation period, yes, you may rely on the information without re-verification. Under § 37.23(e)(3), however, you must document the basis for concluding that each individual with unescorted access to category 2 or greater quantities of radioactive material is trustworthy and reliable. You are required to verify such information as the name, date of birth, social security number, gender, and other physical characteristics of the subject individual to ensure that he or she is the person whose file has been transferred. You want to be sure that the information transferred is for the correct individual. You may ask the originating licensee to provide information about distinguishing characteristics so that you can verify the individual. Such characteristics could include estimated height, birthmarks, scars, tattoos, missing or partially missing fingers or fingernails, and, if permissible under applicable laws and regulations, race and ethnicity.

Q3: Must I re-disseminate an employee's background investigation information if he or she requests it?

A3: No. Part 37 contains no such requirement. Sharing with another licensee the information you developed is entirely at your discretion.

§ 37.31 Protection of information (cont'd)

§ 37.31(d)

The licensee shall make background investigation records obtained under this subpart available for examination by an authorized representative of the NRC to determine compliance with the regulations and laws.

§ 37.31(e)

The licensee shall retain all fingerprint and criminal history records (including data indicating no record) received from the FBI, or a copy of these records if the individual's file has been transferred, on an individual for 3 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

EXPLANATION:

Licensees must make background investigation records available for NRC examination to determine compliance. Licensees must also retain all fingerprint and criminal history information received from the FBI on an individual for 3 years from the date the individual no longer requires unescorted access.

QUESTIONS/ANSWERS:

Q1: Does the NRC have a right to review the background investigation records?

A1: Yes. To determine compliance with applicable laws and regulations, an inspector or other authorized representative of the NRC may examine the background investigation records, and § 37.31(d) requires the licensee to make them available for examination.

Q2: What background investigation records do I need to maintain for NRC inspection under § 37.31(d)?

A2: This subsection requires you to make available for NRC examination "background investigation records obtained under this subpart." This would include, among other things, all records required to be maintained under § 37.23(e) concerning your basis for concluding whether or not there is "reasonable assurance that an individual is trustworthy and reliable." In addition, more generally, [§ 37.23\(h\)\(1\)](#) requires you to retain for 3 years "documentation regarding the trustworthiness and reliability of individual employees." The NRC considers this documentation to include, in addition to the fingerprint and criminal history records covered under § 37.27(e) above, all background investigation records you are required to obtain under § 37.25(a)(2) through (a)(6).

You are also required to retain: under [§ 37.29\(b\)](#), any written confirmations received concerning a favorably adjudicated criminal history records check; under § 37.29(a)(12), any written confirmations you received from U.S. government entities concerning a federal security clearance; and under § 37.29(a)(13), any written verifications received from service providers.

Q3: What fingerprint and criminal history records do I need to maintain?

A3: Under § 37.31(e), you must retain all fingerprint and criminal history records (including data indicating no record) received from the FBI or a copy of these records if the individual's file has been transferred.

Q4: How long do I need to keep background investigation and fingerprint and criminal history records on an individual?

A4: Under § 37.31(e), if the individual's fingerprint and criminal history file has been received from another party, you must retain a copy of these records for 3 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material. Under § 37.23(h)(1), you must retain records on your determination of an individual's trustworthiness and reliability, including background investigation records, for 3 years from the date the individual no longer requires unescorted access. If your license is terminated before either of these retention periods elapses, however, under [§ 37.103](#) you need only retain these records until your license has been terminated.

Q5: According to § 37.23(h) I need to keep records for 3 years. Since these records will contain information that needs to be protected how do I properly dispose of them?

A5: The background investigation records will likely contain personal information that will be considered personally identifiable information (PII). Records containing PII should be destroyed, not just tossed in the trash, to prevent an unauthorized individual from gaining access to that information.

§ 37.33 Access authorization program review

§ 37.33(a)

Each licensee shall be responsible for the continuing effectiveness of the access authorization program. Each licensee shall ensure that access authorization programs are reviewed to confirm compliance with the requirements of this subpart and that comprehensive actions are taken to correct any noncompliance that is identified. The review program shall evaluate all program performance objectives and requirements. Each licensee shall periodically (at least annually) review the access program content and implementation.

§ 37.33(b)

The results of the reviews, along with any recommendations, must be documented. Each review report must identify conditions that are adverse to the proper performance of the access authorization program, the cause of the condition(s), and, when appropriate, recommend corrective actions, and corrective actions taken. The licensee shall review the findings and take any additional corrective actions necessary to preclude repetition of the condition, including reassessment of the deficient areas where indicated.

§ 37.33(c)

Review records must be maintained for 3 years.

EXPLANATION:

Licensees must review and assess the effectiveness of their access authorization programs, take appropriate corrective actions, and maintain the records for 3 years.

QUESTIONS/ANSWERS:

Q1: How should I evaluate the “effectiveness” of my access authorization program to comply with NRC requirements for program reviews?

A1: You should consider several things when evaluating the continued effectiveness of your program. Specifically, you should consider your ability to demonstrate compliance with all the applicable requirements of this subpart and to take comprehensive and effective actions to correct identified noncompliances. Most importantly, however, you should keep in mind that continuing effectiveness is not a static condition. Continuing improvements are an essential part of an effective program. To minimize the potential for overlooking an adverse condition, your program reviews should address each applicable requirement of this subpart. They should identify adverse conditions, noncompliances, and root causes, and should provide corrective actions. You should also follow up on the implementation of these actions and reassess their affect on the program. The hallmark of an effective program is not the absence of recorded adverse conditions or noncompliances; it is documented evidence that the licensee has made diligent efforts to find these problems and is continuing to reassess the effectiveness of its actions to prevent problems from reoccurring. Ultimately, the

most important indicator of an effective program is that the licensee is consistently able to identify and successfully address existing and emerging deficiencies.

Q2: How do I ensure that I will meet the requirement to review the access authorization program “at least annually?”

A2: Recognizing that some demands on licensees’ time and resources are beyond their control, the NRC will consider you to be conducting a program review “at least annually” if you conduct it each year at about the same time of year, not to exceed 12 months.

Q3: Must I engage an outside contractor to conduct access authorization program reviews? If not, how may I ensure that the review isn’t conducted by the same people carrying out the activities being reviewed?

A3: Although hiring an independent party to conduct access authorization program reviews would be one way to demonstrate compliance, the regulation does not require it. Although self assessments do have value and would meet the requirement, you should try to avoid the situation where individuals are reviewing their own work. If you have a large enough staff, one way to avoid self-review would be to establish a review team of approved individuals led by an individual, such as the security official or RSO, who works outside the management chain of your access authorization staff. If you have separate programs at more than one location with a different reviewing official at each location, another way to run a more arm’s length review would be to have the review team at one location review the program implemented by the staff of a different facility. Licensees may also choose to set up a review team through an industry association, with participants from several independent member organizations to conduct program reviews.

Q4: Do I need to report to NRC any noncompliance identified during an access authorization program review?

A4: No, unless the noncompliance was required to be reported to the NRC under a specific requirement.

Q5: What would NRC consider a “condition adverse to the proper performance of the access authorization program?”

A5: NRC will consider an adverse condition to be anything that, if not corrected, could impair the effectiveness of the licensee’s access authorization program or its continuing compliance with the requirements of this subpart. An example of an adverse condition might be a delay in the re-evaluation of an employee’s trustworthiness and reliability after receiving information about a felony arrest. Another example might be a failure to determine beforehand under § 37.31(b) the need to know of an unfamiliar individual making an initial request for the re-dissemination of personal information about an employee. An adequate program review should never be limited to looking only for existing or imminent noncompliances. It should assess or reassess all conditions that may call into question the continuing effectiveness of the licensee’s access authorization program.

Q6: Section 37.33(b) requires the report resulting from a program review to recommend corrective actions “when appropriate.” When should I recommend corrective actions?

A6: At a minimum, a program review report should recommend one or more corrective actions for each noncompliance or condition “adverse to the proper performance of the access authorization program” identified as a result of the review.

Q7: What should I consider as “review documentation” for the purposes of this subsection?

A7: You should retain the annual review report itself and any attachments or enclosures related to that report. Related records should include: the membership and leadership of the review team if applicable; a description of the management approval process for the annual report, if applicable; root cause analyses for identified non-compliances or adverse conditions; recommended corrective actions; evaluations of the effectiveness of past corrective actions; and other documents that were considered in the review. A good review documentation practice is to include minority views on issues in the report on which there has been significant professional disagreement. NRC does not expect you to retain rough drafts of your annual access authorization program reviews, or meeting records, or the notes of each member of a review team.

Q8: How long should I maintain records of the program review?

A8: Records must be maintained for 3 years under § 37.33(c).

Q9: Do I need to keep a paper copy of the program review or may I keep an electronic copy?

A9: You may keep either a paper copy or an electronic copy as long as the record is legible for the required period and can be accessed. To discourage unauthorized alteration, it is good practice to make electronic copies read-only if possible, such as by applying a portable document format (pdf).

Annex A

Additional Guidance for Evaluating an Individual's Trustworthiness and Reliability for Allowing Unescorted Access to Certain Radioactive Material

Each licensee is responsible for determining whether to grant an individual unescorted access to certain radioactive materials. The licensee shall allow only individuals approved and documented by the licensee as trustworthy and reliable to have unescorted access to a category 2 or greater quantity of radioactive material and devices containing that quantity. The T&R determination is made by the licensee's reviewing official (RO), based on the information collected during the background investigation. The RO must document the determination basis. Note that the guidance can also be used when information is received after an individual has been approved for unescorted access.

Unescorted access determinations require an evaluation of a person's trustworthiness and reliability. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise about whether that person can be relied on and trusted to exercise the responsibility necessary for working with risk-significant radioactive materials. The purpose of the T&R determination requirement is to provide reasonable assurance that those individuals are trustworthy and reliable, and do not constitute an unreasonable risk to the public health and safety, including the potential to commit or aid theft or radiological sabotage. In evaluating the relevance of an individual's conduct, the RO should consider such factors as:

1. The nature, extent, and seriousness of the conduct;
2. The circumstances surrounding the conduct, including evidence as to whether it was deliberate;
3. The frequency and recency of the conduct;
4. The individual's age and maturity at the time of the conduct;
5. The extent to which participation in the conduct was voluntary;
6. The presence or absence of rehabilitation and other permanent behavioral changes;
7. The motivation for the conduct;
8. The potential for pressure, coercion, exploitation, or duress as a result of the conduct; and
9. The likelihood of continuation or recurrence.

Each case must be judged on its own merits, and the final determination remains the responsibility of the licensee. In every case, the RO must evaluate trustworthiness and reliability based on an accumulation of information that supports a positive finding, prior to granting unescorted access. Items to consider include:

1. Whether the information collected is consistent and adequate.
2. Whether the applicant's true identity can be reasonably verified by comparing applicant-provided identification and personal history data with pertinent information from the background investigation and other data sources.
3. 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 to the NRC, the licensee will receive an FBI identification and criminal history record since the individual's eighteenth birthday. The licensee's RO should evaluate that information using the guidance below.

The licensee's RO is required to evaluate all available information in making a T&R determination for unescorted access to radioactive materials, including the criminal history records information pertaining to the individual. The FBI identification and criminal history records check is used to determine whether the individual has a record of criminal activity that indicates that the individual should not have unescorted access to radioactive materials subject to the requirements of Part 37. Each T&R determination for unescorted access to radioactive materials, which must include a review of criminal history information, must be documented to include the basis for the decision made.

Licensees must not make a final determination solely on the basis of criminal history check information involving an arrest more than 1 year old for which there is no information on the disposition of the case, or an arrest that resulted in dismissal or acquittal of the charge.

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 unreliability or untrustworthiness of the employee. The licensee will have to judge the nature and recency of the criminal activity. The licensee may authorize individuals with criminal records for 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. Each review of criminal history and other background checks information must be documented to include the decision-making basis. When evaluating the results of the criminal history records check, the licensee should consider, at a minimum, whether the subject individual:

1. Committed, attempted to commit, aided, or abetted another who committed or attempted to commit any act of sabotage, espionage, treason, sedition, or terrorism.
2. Publicly or privately advocated actions that may be inimical 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.
3. Knowingly established or continued a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, or revolutionary, or 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.)
4. Joined or engaged in any activity knowingly in sympathy with or in support of any foreign or domestic organization, association, movement, group, or

combination of persons which advocates or practices 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 which advocates 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.)

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

6. Has been convicted of a crime(s) which, in the reviewing official's opinion, indicate poor judgment, unreliability, or untrustworthiness.

Licensees may also consider how recently such indicators occurred and other extenuating or mitigating factors in their determinations. Section 149.c.(2)(B) of the AEA requires that the information obtained as a result of fingerprinting be used solely for the purposes of making a determination as to 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. 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.

All information collected is to be considered in making a trustworthiness or reliability determination for unescorted access. Potentially disqualifying information obtained from confidential or unnamed sources must be substantiated and documented, and should not be used as the sole basis to deny access authorization unless 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. It is the licensee's responsibility to make the trustworthiness and reliability determination for an employee seeking unescorted access. The T&R determination is designed to identify past actions pertinent to whether there is reasonable assurance of an individual's future reliability. In addition to the criminal history records check, licensees may want to consider whether the subject individual has exhibited:

1. Impaired performance attributable to psychological or other disorders;
2. Conduct that warrants referral for criminal investigation or results in an arrest or conviction;
3. An indication of deceitful or delinquent behavior;
4. Attempted or threatened destruction of property or life;
5. Suicidal tendencies or has attempted suicide;
6. Illegal drug use or the abuse of legal drugs;
7. Alcohol abuse disorders;
8. Recurring financial irresponsibility;
9. Irresponsibility performing assigned duties;
10. Inability to deal with stress, or having the appearance of being under unusual stress;

11. Failure to comply with work directives;
12. Hostility or aggression toward fellow workers or authority;
13. Uncontrolled anger, violation of safety or security procedures, or repeated absenteeism; or
14. 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.

I understand that photocopies of this authorization and consent document with my signature are valid, and that this authorization will remain in effect so long as I am authorized to obtain unescorted access to the radioactive material subject to 10 CFR 37.

Signature (In ink)		Full Name (Type or print legibly)		Date signed
Other names used			Date of birth	Social Security Number
Current street address and Apt. #	City and country	State	Zip code	Home telephone

Subpart C – Physical Protection Requirements During Use

- 37.41 Security program.
- 37.43 General security program requirements.
- 37.45 LLEA coordination and notification.
- 37.47 Security zones.
- 37.49 Monitoring, detection, and assessment.
- 37.51 Maintenance and testing
- 37.53 Requirements for mobile devices.
- 37.55 Security program review.
- 37.57 Reporting of events.

§ 37.41 Security program

§ 37.41(a) Applicability.

§ 37.41(a)(1)

Each licensee that possesses an aggregated category 1 or category 2 quantity of radioactive material shall establish, implement, and maintain a security program in accordance with the requirements of this subpart.

EXPLANATION:

Each licensee that possesses an aggregated quantity of category 1 or category 2 quantities of radioactive material must have a security program.

QUESTIONS/ANSWERS:

Q1: What is the purpose of a security program?

A1: The purpose of a security program under Part 37 is to plan and document how the licensee will protect category 1 and 2 quantities of radioactive material. The program specifies how features such as training, access controls, detection and assessment methods, and response capabilities will function together to mitigate the potential detrimental consequences to public health and safety and the environment.

Q2: What does it mean to have an “aggregated” quantity of radioactive material?

A2: The NRC considers radioactive material to be “aggregated” if someone could gain access to a category 2 or greater quantity by breaching a single physical barrier. “Aggregated” has the same meaning as “collocated” in the guidance for the Increased

Controls orders. Part 37 uses the term “aggregated” instead of “collocated” to avoid the confusion that could arise when several separate non-aggregated quantities of radioactive material are located at the same site or inside the same facility.

Q3: Does Part 37 apply if I have two or more sources at the same location that, when added together, meet or exceed a category 2 threshold quantity?

A3: Part 37 applies if there is no additional physical barrier between the sources or devices, so that an intruder would have to defeat only one barrier to gain access to a category 2 or greater quantity of radioactive material. With only one common barrier, the sources or devices are considered aggregated and you will have to develop and implement a security program. An example would be a high dose after-loader with a back up source. If the two sources were stored in the same area behind a single barrier, they would be aggregated and Part 37 would apply. Using this same example of a high-dose after-loader and backup source, Part 37 would not apply if the backup source is stored in a separate locked room or in a locked container that could not be removed, such as a safe. These would be considered additional barriers, and the after-loader and backup source would no longer meet the definition of “aggregated” because they would no longer be isolated by a single physical barrier.

Q4: How do I determine whether I possess a category 1 or category 2 quantity of radioactive material?

A4: Use the sum-of-the-fractions method, also known as the unity rule, to determine whether you possess a category 1 or category 2 quantity of radioactive material. You may need to implement Part 37 requirements even if you do not possess any single source or single radionuclide in excess of a category 2 threshold. For combinations of materials (including sealed sources, unsealed sources, and bulk material) and radionuclides, a licensee must include multiple sources (including bulk material) of the same radionuclide and multiple sources (including bulk material) of different radionuclides to determine if the requirements apply. For the purposes of this calculation, licensees are required to consider all of the radioactive material the license possesses at the location in question.

To determine whether you have a category 2 quantity and are required to implement Part 37 requirements, you may use the following formula for the unity rule:

$$R_1/AR_1 + R_2/AR_2 + R_n/AR_n \geq 1.0$$

Where R_1 = total amount of radionuclide 1, AR_1 = category 2 threshold of radionuclide 1, R_2 = total amount of radionuclide 2, AR_2 = category 2 threshold of radionuclide 2, R_n = total amount of radionuclide n, AR_n = category 2 threshold of radionuclide n, etc. ≥ 1.0 .

To determine whether you have a category 1 quantity for purposes of implementing Part 37 requirements, you would use the same unity rule formula above, but substitute the category 1 threshold value as the divisor for each radionuclide. Category 1 thresholds in Appendix A are 100 times the thresholds for category 2 quantities.

The Terabecquerel (TBq) thresholds need to be used in all unity rule calculations because Terabecquerels are the regulatory standard. You must therefore convert any Curie (Ci) values in your license to TBq using the formula:

$$n \text{ (TBq)} = N \text{ (Ci)} \times 0.037 \text{ TBq/Ci.}$$

For illustrative examples of unity rule and T bq conversion calculations, see the Q&As for the definitions of category 1 and category 2 quantities in [§ 37.5](#).

Q5: If I have radioactive materials aggregated to a category 2 or greater quantity, what do I have to do to meet the separate requirements of § 37.41(a)(1) to “establish,” to “implement,” and to “maintain” a security program?

A5: To “establish” the security program, you must develop a written security plan that describes a strategy and a set of technologies and measures that, when implemented with written procedures that are also required, will demonstrate compliance with each of the applicable requirements of Subpart C of this rule. Under § 37.41(c) below, the security program must, as appropriate, include the program features described in §§ [37.43](#), [37.45](#), [37.47](#), [37.49](#), [37.51](#), [37.53](#), and [37.55](#). The specific measures to be implemented under the security program must include, among other things: the establishment of security zones; the design and procurement of a physical protection system for monitoring, detection, assessment, and alarm/communication; the procurement of any needed support services, such as a commercial security service between normal working hours; and coordination with affected LLEAs. The program must also include recordkeeping measures and provide for the operation, testing, and maintenance of equipment and technologies that, functioning as an integrated system with the other measures required under this section, 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.

To “implement” the security program, you must have: trained necessary staff under § 37.43(c) to follow your program’s procedures; installed and be using all the access control measures or systems required under § 37.43(a)(1)(ii); completed initial LLEA coordination efforts under § 37.45; installed in accordance with § 37.47 the physical barriers protecting each security zone; and installed and be using all the monitoring, detection, and alarm/communications systems required under § 37.49. You must also have placed into service all the appropriate other measures, such as those for testing and maintenance under § 37.51, those for mobile devices under § 37.53, those for reporting of events under § 37.55, and those for program reviews under § 37.57, that are required by this Part and that you will be relying on to meet the performance objectives of § 37.41(b).

To “maintain” the security program, you must show that you have implemented and are continuing to: fund the program’s access authorization and control, training, monitoring, detection, assessment, alarm/communication, and LLEA coordination activities; and inspect, test, and repair the equipment installed to keep it functioning properly. You will also need to periodically evaluate and update operating, training, and LLEA coordination procedures, and other measures required by this Part as appropriate to address lessons learned and ensure the continuing compliance of the system you have designed and implemented to meet the performance objectives of § 37.41(b).

Q6: Must I have a security program for temporary job sites?

A6: Yes. If a licensee has a category 1 or category 2 quantity of radioactive material at a temporary job site, the licensee must have a security program that meets the requirements of Part 37. This does not mean that the licensee must develop and implement a security program specifically for each temporary job site, however. It only means that the licensee's security plan under § 37.43(a) must address the security of the licensee's category 1 or category 2 quantities of radioactive material while working at temporary as well as permanent job sites.

Additionally, when transporting radioactive material in such quantities to and from a temporary job site, the licensee must control access, monitor, detect, assess, and respond to an actual or attempted theft, sabotage, or diversion. These measures against unauthorized access must also be applied when the transport vehicle is stopped at a hotel, restaurant, gas station, or other location. (See Q&As on § 37.79(a)(2)).

Q7: If I'm a licensed contract radiographer, and I must leave a radiography camera at another licensee's or customer's facility that provides its own site security, who is responsible for security? When I'm expected to leave a camera on site at an oil refinery, for example, who provides security there, and if the customer provides the security, how can I know whether the security satisfies Part 37?

A7: Licensees that possess radioactive material are responsible for its security and control, and need to meet Part 37 security requirements whether at their own or a customer's facility. If you choose to store one of your devices at a customer's facility, both you and the customer must ensure that applicable Part 37 requirements are met. You will need to evaluate whether your customer's physical protection program will comply with the Part 37 requirements applicable at the agreed storage location, and you and the customer should have a clear understanding of your respective roles and responsibilities and the features of the customer's security and control program that are to be relied on to meet the applicable security requirements for your device. You should assess the customer's security systems and measures against those of your own program for implementing these requirements.

§ 37.41 Security program (cont'd)

§ 37.41(a) Applicability.

§ 37.41(a)(2)

An applicant for a new license and each licensee that would become newly subject to the requirements of this subpart upon application for modification of its license shall implement the requirements of this subpart, as appropriate, before taking possession of an aggregated category 1 or category 2 quantity of radioactive material.

§ 37.41(a)(3)

Any licensee that has not previously implemented the Security Orders or been subject to the provisions of subpart C shall provide written notification to the NRC regional office specified in § 30.6 of this chapter at least 90 days before aggregating radioactive material to a quantity that equals or exceeds the category 2 threshold.

EXPLANATION:

New license applicants and licensees newly subject to Part 37 must implement the requirements of Subpart C before taking possession of an aggregated category 1 or category 2 quantity of radioactive material. A licensee that has not previously implemented the Security Orders or been subject to the provisions of Subpart C must notify the appropriate NRC regional office in writing at least 90 days before aggregating radioactive material to a quantity that equals or exceeds the category 2 threshold.

QUESTIONS/ANSWERS:

Q1: At what point in the process of transferring possession of radioactive material would I be considered to have "taken possession" of a category 1 or category 2 quantity? Have I "taken possession" of a source under Part 37 when the carrier or delivery service crosses my site boundary, for example? When the carrier has brought the source into my facility building? When the source is in a permanent security zone on my site?

A1: The NRC will consider you to have taken possession of a category 1 or category 2 quantity when you have accepted the consignment of the material from the shipper or transferring licensee and assumed physical control of the material. Thus, you would not be deemed to have taken possession when the shipper has crossed your site boundary or brought the source into a building on your facility site, unless you accept the consignment and assume physical control of the material at that point on your premises. At that point, if the acceptance of the consignment caused you to have aggregated radioactive material in a category 2 or greater quantity, then you must be meeting the requirements of Part 37. If you are ordering new byproduct material that would put you over the category 2 limit for an aggregated quantity when it arrives at your facility, you should have established your security program before you order the material, including the access authorization program required by Subpart B.

Q2: Would I be considered to have "taken possession" if the carrier delivers a shipment and then leaves without my having accepted the consignment?

A2: Yes. The licensee would be held accountable if the carrier left a shipment on the doorstep or loading dock. The licensee is responsible for making arrangements for receipt of the shipment. Except in extreme or emergency circumstances, however, this scenario is highly unlikely. The shipping licensee is required under § 37.79(a)(3)(iii) to use a carrier that requires a signature for receipt of category 2 shipments.

Q3: If I am receiving multiple deliveries of radioactive material, when would I be considered to have taken possession of an "aggregated" category 1 or category 2 quantity?

A3: You would be considered to have taken possession of an "aggregated" category 1 or category 2 quantity of radioactive material when and if you place an accumulated quantity at or above the category 2 threshold behind a single physical barrier. If you place one or more of these deliveries in a total quantity less than category 2 behind a separate, independent physical barriers, you are not possessing an "aggregated" quantity of material as defined in Part 37.

§ 37.41 Security program (cont'd)

§ 37.41(b) General performance objective.

Each licensee shall establish, implement, and maintain a security program that is designed to 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.

§ 37.41(c) Program features.

Each licensee's security program must include the program features, as appropriate, described in §§ 37.43, 37.45, 37.47, 37.49, 37.51, 37.53, and 37.55.

EXPLANATION:

This provision establishes the general performance objective of the security program and specifies the features it must include, as appropriate.

QUESTIONS/ANSWERS:

Q1: What does it mean for a licensee's security program to be designed to detect, assess, and respond to an unauthorized access event "without delay?"

A1: You must have a security program that enables you to detect unauthorized access to the security zone when it occurs, to determine whether the unauthorized access was an actual or attempted theft, and to initiate an appropriate response right away. The objectives are to reduce the risk that the material will be stolen and used for an unauthorized purpose, and if it is stolen, to improve the likelihood of timely recovery or mitigate potential consequences.

Q2: What's the difference between "actual" and "attempted" unauthorized access? Wouldn't the same kinds of measures apply to both?

A2: Yes, the same kinds of measures apply to both. Although the measures for immediate detection, assessment, and response to *actual* unauthorized access to radioactive materials will also be required for *attempts* to gain unauthorized access, licensees should also be alert for covert actions in preparation for an attempted theft, sabotage, or diversion. Such covert actions could include the theft and copying of keys to locked rooms or storage containers, for example, or gaining access to security codes for copying onto duplicate key cards. Licensees should, therefore, monitor, assess, and respond to actual or attempted unauthorized access to keys, security cards, codes, or other means that could be used in an attempt to gain unauthorized access to the material in a security zone.

Q3: Can licensees use measures required for radiation safety to comply with Part 37 security requirements too?

A3: Yes. Systems used to control access to high radiation areas as required by 10 CFR Part 20, or equivalent Agreement State regulations, or other detection and access control systems used for radiation protection, may be used or modified for security purposes, provided that the uses or modifications do not compromise the

original safety purpose. Documentation should describe how these systems provide the required intrusion detection.

Q4: What are the principal requirements of a security program?

A4: The licensee must have a security program to continuously monitor and immediately detect unauthorized access to category 1 or category 2 quantities of radioactive material when the unauthorized access occurs. The program must also enable the licensee to determine whether the unauthorized access is an actual or attempted theft, and to initiate an appropriate response without delay. The detection system must be capable of detecting all unauthorized access to the security zone, including breaches of barriers used to isolate and control access to the protected radioactive material. It must also be capable of detecting an unauthorized removal of protected material from security zones. Assessment can be by either automated devices or trained personnel who can initiate the appropriate response. Licensees should consider the possibility of simultaneous alarms at multiple locations. The program's documentation must also describe the processes the licensee will use to assess and respond to unauthorized access.

A licensee's security program must include a written security plan, implementing procedures, training, the use of security zones, the protection of information, requests for coordination with the cognizant LLEA(s), additional security measures for mobile devices if applicable, testing and maintenance of security-related equipment, an annual program review, and incident reporting requirements. Each of these areas is discussed in more detail in the following questions and answers.

§ 37.43 General security program requirements

§ 37.43(a) Security plan.

§ 37.43(a)(1)

Each licensee identified in § 37.41(a) shall develop a written security plan specific to its facilities and operations. The purpose of the security plan is to establish the licensee's overall security strategy to ensure the integrated and effective functioning of the security program required by this subpart. The security plan must at a minimum:

§ 37.43(a)(1)(i)

Describe the measures and strategies used to implement the requirements of this subpart; and

§ 37.43(a)(1)(ii)

Identify the security resources, equipment, and technology used to satisfy the requirements of this subpart

EXPLANATION:

Subject licensees must develop a written security plan with an overall security strategy to ensure the integrated and effective functioning of the security program. The subsection also specifies minimum contents of the security program.

QUESTIONS/ANSWERS:

Q1: Must licensees submit their written security plans to NRC?

A1: No. Part 37 does not require, and the NRC does not want, licensees to submit security plans or implementing procedures to NRC for review or approval. The security plan will be subject to NRC inspection.

Q2: What must a licensee's security plan address?

A2: As noted in 37.43(a)(1), the plan must, among other things, include a description of the measures and strategies to implement the security requirements and identify the resources, equipment, and technology used. To explain the licensee's overall strategy, it would be a good practice for the security plan to describe any site-specific conditions that affect how the licensee will implement the requirements.

Security plans are important for the implementation of a performance-based regulation. 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 facilitate meeting the program review requirements of [§ 37.33](#), the licensee may also consider describing in the security plan a process 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.

One method for developing a security plan would be to structure the plan in accordance with Appendix II of IAEA's Implementing guide, *Security of Radioactive Sources*, IAEA Nuclear Security Series No. 11 (http://www-pub.iaea.org/MTCD/publications/PDF/Pub1387_web.pdf). Although Appendix II of the guide notes that "[t]he level of detail and depth of content [of a licensee's security plan] should be commensurate with the security level of the source(s) covered by the plan," and not all of the recommended measures may apply to a given licensee's situation, the Appendix sets forth the recommended contents of a typical security plan for the radioactive materials subject to Part 37. For easy reference, these contents are set forth below:

- A description of the radioactive material, its categorization, and its use.
- A description of the environment, building and/or facility where the radioactive material is used or stored, and if appropriate a diagram of the facility layout and security system.
- The location of the building or facility relative to areas accessible to the public.
- Local security procedures.
- The objectives of the security plan for the specific building or facility, including:
 - The specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - The kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - The equipment or premises that will be secured.
- The security measures to be used, including:
 - The measures to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - The design features to evaluate the quality of the measures against the assumed threat.
- The administrative measures to be used, including:
 - The security roles and responsibilities of management, staff and others;
 - Routine and non-routine operations, including accounting for the source(s);
 - Maintenance and testing of equipment;
 - Determination of the trustworthiness of personnel;
 - The application of information security;
 - Methods for access authorization;
 - Security-related aspects of the emergency plan, including event reporting;
 - Training;
 - Key control procedures;
 - The procedures to address an increased threat level;

- The process for periodically evaluating the effectiveness of the plan and updating it accordingly.
- Any compensatory measures that may need to be used.
- References to existing regulations or standards.

Q3: Can the security plan and implementing procedures be in the same document?

A3: Yes, but any document or group of documents that contains both the security plan and its implementing procedures must meet the respective requirements in § 37.41(a) and § 37.41(b) for each of these program elements.

Q4: Is a licensee required to develop specific additional contingency plans for situations where a facility or site needs to evacuate staff due to an emergency, natural disaster, or other events where public health and safety are threatened?

A4: Part 37 does not specifically require a licensee to develop any contingency plans as such, but contingency planning is considered a best practice in the development of security plans. NRC encourages contingency planning as consistent with the intent of Part 37 and the security culture it seeks to promote. Because licensees are required to ensure the security and accountability of the radioactive material protected under this Part, they should also consider measures to maintain this security and accountability in the event of an evacuation or other emergency situation. These plans, if developed, should address such things as floods, earthquakes, and tornadoes that have an increased probability of occurring in the area where the facility or site is located.

Q5: Should the radiation safety office or officer be involved in the development or implementation of security plans and procedures?

A5: Although RSOs and their staff may not be the licensee's experts in security, it is a good idea to involve them because they can provide valuable insights for improving the consideration of safety and security risks in a system-integrated way. The radiation safety office or officer can also provide advice and analysis to ensure that security requirements are being implemented in a manner that does not compromise safety.

Q6: Can a licensee with a security plan already in place for the Increased Controls Orders be automatically exempted from requirements to develop and implement a new security plan under Part 37?

A6: No, you are not automatically exempt from the requirements in Part 37 to have a security plan. If you have an existing security plan, you will need to check that it meets all of the requirements for a security plan in Part 37. If it does, you may continue to use your existing plan.

Q7: If I already have a high-level corporate security plan in place that meets the requirements of § 37.43(a), do I still have to develop and implement a separate security plan to demonstrate compliance with Part 37?

A7: No. As long as a pre-existing site or corporate-wide plan meets the requirements of Subpart C as to the content of the security plan, the plan would be acceptable and a new plan would not need to be developed. Each site would need to have a copy of the plan for implementation.

Q8: If I'm a licensee possessing a category 2 or greater quantity of radioactive material, and I hire a service contractor licensed by NRC or another Agreement State, do the requirements of the contractor's security program govern the contractor employee when he or she is on my site, or must the employee comply with the requirements of my security program?

A8: This would depend on the ownership of the material . If you own the radioactive material or devices containing it, as would be the case with a hospital owning a gamma stereotactic radiosurgery device, your contractor would be governed by your security program. If the contractor owns the material or device, such as a radiography camera that the contractor brings to your site, the contractor's security requirements would apply to its use and the control of that device or material.

§ 37.43 General security program requirements (cont'd)

§ 37.43(a) Security plan.

§ 37.43(a)(2)

The security plan must be reviewed and approved by the individual with overall responsibility for the security program.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

Q1: For review and approval of the security plan, who should be considered “the individual with overall responsibility for the security program?”

A1: The licensee can designate the individual. The individual can be the company president, chief executive, the RSO, or any other individual who has been designated as the responsible person for the security program. The individual responsible for the security of all the licensee’s category 1 or category 2 quantities of radioactive material is the appropriate individual to provide written approval of the plan.

§ 37.43 General security program requirements (cont'd)

§ 37.43(a) Security plan.

§ 37.43(a)(3)

A licensee shall revise its security plan as necessary to ensure the effective implementation of Commission requirements. The licensee shall ensure that:

§ 37.43(a)(3)(i)

The revision has been reviewed and approved by the individual with overall responsibility for the security program; and

§ 37.43(a)(3)(ii)

The affected individuals are instructed on the revised plan before the changes are implemented.

EXPLANATION:

A licensee must revise its security plan as needed to ensure effective implementation. Any revision must be reviewed and approved by the individual with overall responsibility for the security program, and affected individuals must be instructed on the revised plan before the licensee implements the changes.

QUESTIONS/ANSWERS:

Q1: How frequently should I revise my security plan?

A1: There is no predetermined frequency for revision of the security plan. You may want to revise yours after the completion of the annual security program review so that any recommendations are addressed in the revised plan. You may need to revise your security plan if you increase the quantity of radioactive material you have aggregated at a given location, if you move the location of a storage area for an aggregated quantity, or if you alter your facility in a way that could affect the security of your licensed radioactive material subject to this Part. You would also need to revise your security plan before you change the measures you rely on to comply with Part 37. If you plan to shift from direct surveillance to an offsite-monitored alarm system, for example, you would need to address that change in revisions to your security plan and procedures.

Q2: Who should approve revisions to the security plan under § 37.43(a)(3)(i)?

A2: The revised security plan must be approved by the individual who has overall responsibility for the security program. As noted in the discussion of § 37.43(a)(2), the approving individual may be the company president, chief executive, the RSO, or any other individual who has been given the responsibility for the security program.

Q3: Section 37.43(a)(3)(ii) requires me to ensure that “affected individuals” are “instructed” on the revised plan before the changes are implemented. How broadly or narrowly should I define “affected individuals?” Do I have to retrain all my employees and any service contractor employees before I can put any change in my security plan into effect?

A3: No, you do not need to retrain all your employees or contractors before implementing a change in your security plan. You only need to retrain those employees whose responsibilities or job duties would be impacted.

Q4: Section 37.43(a)(3)(ii) also requires me to ensure that these affected individuals are “instructed” on the revised plan before the changes are implemented. What must I require of the “affected individuals” to show that they have been sufficiently “instructed?” Must all the affected individuals get a passing score on a proficiency exam or demonstrate the needed new skills before I can put the change into effect?

A4: No, you do not need to require all the affected individuals to pass a proficiency exam or demonstrate mastery of the necessary skills before implementing a change in your security plan. The instruction could, depending on the change, consist of reading new procedures, a briefing on the new item(s), or on-the-job training. As with any training, you need to document that the training occurred. You should consider the scope of the security plan revision in relation to the scope of each individual’s job duties to identify those individuals who may need to show a more measurable level of knowledge or skill to ensure effective or timely implementation of the change in your security plan. A change that would affect the licensee’s policy on employee observation or reporting of suspicious activities may only require a briefing before implementation. A good practice to demonstrate compliance with this instruction requirement would be to require the affected individual(s) to sign a statement that they have read and are familiar with the relevant portion of the security plan and procedures

§ 37.43 General security program requirements (cont'd)

§ 37.43(a) Security plan.

§ 37.43(a)(4)

The licensee shall retain a copy of the current security plan as a record for 3 years after the security plan is no longer required. If any portion of the plan is superseded, the licensee shall retain the superseded material for 3 years after the record is superseded.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

Q1: If I've received a license amendment that reduces my possession limits to quantities below a category 2 threshold, and my pre-license amendment records are inspected a few months or a year later, am I still required to maintain these records for the rest of the 3-year period?

A1: Yes, you are required to retain most records, including those preceding your license amendment, for 3 years, although some records must be maintained until your license is terminated. In the case of the security plan, you must retain the record for 3 years after the plan is no longer needed. You may destroy all Part 37-related records once your license has been terminated.

Q2: What does it mean for the security plan or any portion of it to be "superseded?"

A2: The NRC would consider the security plan to be "superseded" once a revision to the plan has been approved. A plan can be completely revised or partially revised to be considered superseded. The licensee would need to retain a copy of the old security plan for 3 years, or until license termination if that occurs before then.

§ 37.43 General security program requirements (cont'd)

§ 37.43(b) Implementing procedures.

§ 37.43(b)(1)

The licensee shall develop and maintain written procedures that document how the requirements of this subpart and the security plan will be met.

§ 37.43(b)(2)

The implementing procedures and revisions to these procedures must be approved in writing by the individual with overall responsibility for the security program.

§ 37.43(b)(3)

The licensee shall retain a copy of the current procedure as a record for 3 years after the procedure is no longer needed. Superseded portions of the procedure must be retained for 3 years after the record is superseded.

EXPLANATION:

Subject licensees must have written procedures documenting how the security plan and other Subpart C requirements will be implemented. The procedures and future revisions must be approved in writing by the individual with overall responsibility for the program. The licensee must keep a copy of the current procedure as a record for 3 years after the procedure is no longer required. If any portion is superseded, the licensee must keep the superseded material for 3 years.

QUESTIONS/ANSWERS:

Q1: Am I required to develop security procedures if I don't actually possess a category 2 quantity of material?

A1: No. A licensee only needs to develop security procedures if it possesses an aggregated quantity that meets or exceeds the category 2 threshold and must therefore implement a security program. If a licensee plans on obtaining additional radioactive material, or relocating currently possessed radioactive material into an aggregated quantity that meets or exceeds the category 2 threshold, the licensee must establish its security program before obtaining or relocating the material. This would include having the procedures in place.

Q2: What must a licensee's security procedures address?

A2: Generally, the security procedures must address how the licensee will implement the applicable features required under Subpart C. Depending on the licensee and its operating requirements, these features would require the licensee's procedures to address training; establishing and maintaining security zones; monitoring, detection, assessment, and response measure; maintenance and testing measures; the reporting of events; and the periodic review of 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 an LLEA response, to a malevolent intrusion that would require LLEA intervention. These procedures should include, if applicable, provisions for immediate response, for after-hours notification of LLEAs and the licensee individual responsible for security, for handling of both radiation safety and security-related types of emergencies, and for events at temporary job sites.

Procedures should also address the roles of the licensee's staff and, where applicable, its contractors. The licensee's staff and contractors must 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. It is important to note, however, that when developing these security procedures, the licensee must not compromise facility operational safety, occupational safety, fire safety, and emergency planning at the facility.

Q3: Is there flexibility built into the Part 37 implementation process?

A3: Yes. Part 37 is purposely not prescriptive, which allows licensees to tailor programs to their specific facility and operations. Various approaches are available for licensees to meet the objectives of Part 37, and there is no one solution to any material control challenge facing licensees. This guidance document provides examples of how Part 37 requirements may be met. Licensees do not have to implement any of the examples in the guidance; each example describes only one acceptable method to comply with Part 37 requirements.

Q4: Who can approve implementing procedures?

A4: The individual considered to have overall responsibility for the licensee's security program is the individual who must approve any security implementing procedures (see § 37.43(a)(2)).

Q5: What does it mean for the security procedure or any portion of it to be "superseded?"

A5: A procedure is superseded when a new version of the procedure has been issued. A procedure can be completely revised or partially revised to be considered superseded. The licensee would need to retain a copy of the old procedure for 3 years, or until license termination if that occurs before then.

§ 37.43 General security program requirements (cont'd)

§ 37.43(c) Training.

§ 37.43(c)(1)

Each licensee shall conduct training to ensure that those individuals implementing the security program possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively. The training must include instruction in:

§ 37.43(c)(1)(i)

The licensee's security program and procedures to secure category 1 or category 2 quantities of radioactive material, and in the purposes and functions of the security measures employed;

§ 37.43(c)(1)(ii)

The responsibility to report promptly to the licensee any condition that causes or may cause a violation of Commission requirements;

§ 37.43(c)(1)(iii)

The responsibility of the licensee to report promptly to the local law enforcement agency and licensee any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material; and

§ 37.43(c)(1)(iv)

The appropriate response to security alarms.

§ 37.43(c)(2)

In determining those individuals who shall be trained on the security program, the licensee shall consider each individual's assigned activities during authorized use and response to potential situations involving actual or attempted theft, diversion, or sabotage of category 1 or category 2 quantities of radioactive material. The extent of the training must be commensurate with the individual's potential involvement in the security of category 1 or category 2 quantities of radioactive material.

EXPLANATION:

Individuals implementing the security program must be trained. The training must cover the program and its procedures, the purpose and function of the security measures, and the individual's responsibilities. The extent of the training must be commensurate with the individual's potential involvement in radioactive material security.

QUESTIONS/ANSWERS:

Q1: What is the purpose of the training program?

A1: The purpose of the training program is to make sure that those employees responsible for implementing security measures know what is expected of them and know how to do their job.

Q2: What minimum elements must a training program include?

A2: A licensee's training program should be evaluated against this Subpart C's performance objective of ensuring that each individual with responsibility for any aspect of the security program has the requisite knowledge, skills, and abilities to carry out that responsibility effectively. Thus, 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. Examples of appropriate subjects for training would include the controls 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, and ways to confirm quickly and accurately whether an intrusion is likely to be intentional or accidental. An adequate program must also train employees to identify "condition[s] that cause ... or may cause a violation" of Commission requirements. This should include training on identifying and reporting suspicious activities. An adequate program should also cover the operation of primary and backup communication systems for such reporting.

The licensee's staff members must have a clear understanding of their individual responsibilities and constraints in an emergency, and training should provide step-by-step instructions and clear guidelines for what to do and whom to contact. Step-by-step instructions and clear guidelines should also be provided in training 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, you might train most of your employees on escort responsibilities and general alarm response. Those that will be conducting surveillance should be trained on what to look for and how to respond when they see something unusual.

Q3: What "potential situations" involving theft, diversion, or sabotage should a licensee consider when determining who should be trained?

A3: There is no single set of potential security situations that would apply to every licensee's individual security needs. Each licensee's security plan should develop and evaluate a set of site-specific theft, diversion, and sabotage scenarios that could arise from the licensee's particular operating requirements and work site settings with sufficient probability, consequences, or both to make it prudent for the licensee to address. These scenarios should be addressed in the training program. Potential situations must be evaluated for the monitoring, detection, assessment, and response functions needed for a timely and effective response, and scenarios could include events ranging from an inadvertent unauthorized access that would not require an LLEA response, to a malevolent intrusion that would. These procedures should include provisions for immediate response, for after-hours notification of LLEAs and licensee management, and for handling credible radiation safety problems that could result from postulated security emergencies. Where applicable, the licensee should also develop training requirements for security events at temporary job sites.

Q4: The rule requires the extent of the licensee's security training for affected individuals to be "commensurate with the individual's potential involvement" in the subject material's security. Should all individuals with a valid reason to be on-site be considered to have "potential involvement" in a security emergency, and therefore require training?

A4: No. Although it is good practice to provide some basic training to all employees (so that they know how to respond to an alarm, for example), only those individuals with security responsibilities are required to be trained. If an employee does not have unescorted access to the radioactive material, does not have access to any security information, and has no security duties, he or she may not need to receive any security training beyond the basics of safely responding to alarms. Nor do all individuals need to receive the same level of training.

Q5: How should a licensee demonstrate that the individuals responsible for implementing the security plan have acquired the necessary "knowledge, skills, and abilities" to carry out their assigned duties and responsibilities "effectively?"

A5: Although testing is not required, one measure of the likelihood that a trainee will be able to carry out assigned security responsibilities is evidence that the trainee took and passed a reasonable test of the knowledge, skill, or ability objectives of the training.

Another measure of the likelihood that an employee or contractor will be able to carry out assigned security responsibilities is evidence that he or she has successfully participated in a drill or exercise designed to test the integrated functionality of the entire security system, including monitoring, detection, assessment, and response. Using such system-wide drills or table top exercises, and notifying affected LLEAs of opportunities to participate in such training, can be an especially effective way for some licensees to train their personnel.

Depending on the frequency and relative complexity of an individual's assigned duties, however, adequate training can also be demonstrated through the daily or weekly conduct of his or her job. This could be especially true for some elements of refresher training. If the individual is a security guard who makes regular checks on designated work locations, for example, or who must report the operating status of security equipment at specified intervals, the employee's routine fulfillment of these job duties may be sufficient evidence that he or she needs no further training in these duties, at least until new equipment, new technologies, or new procedures necessitate new training.

§ 37.43 General security program requirements (cont'd)

§ 37.43(c) Training. (cont'd)

§ 37.43(c)(3)

Refresher training must be provided at a frequency not to exceed 12 months and when significant changes have been made to the security program. This training must include:

§ 37.43(c)(3)(i)

Review of the training requirements of paragraph (c) of this section, and any changes made to the security program since the last training;

§ 37.43(c)(3)(ii)

Reports on any relevant security issues, problems, and lessons learned;

§ 37.43(c)(3)(iii)

Relevant results of NRC inspections; and

§ 37.43(c)(3)(iv)

Relevant results of the licensee's program review and testing and maintenance.

§ 37.43(c)(4)

The licensee shall maintain records of the initial and refresher training for 3 years from the date of the training. The training records must include dates of the training, topics covered, a list of licensee personnel in attendance, and related information.

EXPLANATION:

Refresher training must be provided at least every 12 months and when significant changes have been made to the security program. The subsection specifies what the refresher training must include, and that licensees must keep training records for 3 years.

QUESTIONS/ANSWERS:

Q1: How frequently should licensees provide refresher training?

A1: As required by § 37.43(c)(3), a licensee must conduct refresher training, at a minimum, every 12 months. Licensees must also offer refresher training if there have been significant changes in the security program.

Q2: What should be included in refresher training?

A2: Developers of refresher training should review the training requirements of § 37.43(c)(1) and (2) and address: 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; and 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 how to avoid or mitigate the consequences of a recurrence.

Q3: Under §§ 37.43(c)(3)(ii), (iii), and (iv), what things does the NRC consider “relevant” for purposes of refresher training?

A3: The term “relevant” is a common term and in this case simply refers to items that are related to security. Examples of some items that should be included in refresher training are: areas where staff has had trouble following the security requirements; areas where corrective actions have not been effective or lessons learned have not addressed root causes of past or potential security deficiencies, and new actions are required; violations of Part 37 security requirements, or conditions adverse or potentially adverse to security, that have been discussed in an inspection report; and measures necessary to fix any security issues identified the licensee’s program review or testing and maintenance results.

Q4: When we give LLEA representatives a copy of our security plan, do we have to test them on their understanding?

A4: No. A licensee may, at its discretion, provide a copy of its security plan to the affected LLEA for information, but no licensee is required to provide a copy. Nor are you expected to train an LLEA on your security plan; the plan itself applies only to the licensee and its employees and contractors.

§ 37.43 General security program requirements (cont'd)

§ 37.43(d) Protection of information.

§ 37.43(d)(1)

Except as provided in paragraph (d)(9) of this section, licensees authorized to possess category 1 or category 2 quantities of radioactive material shall limit access to and unauthorized disclosure of their security plan, implementing procedures, and the list of individuals that have been approved for unescorted access.

§ 37.43(d)(2)

Efforts to limit access shall include the development, implementation, and maintenance of written policies and procedures for controlling access to, and for proper handling and protection against unauthorized disclosure of, the security plan and implementing procedures.

§ 37.43(d)(3)

Before granting an individual access to the security plan or implementing procedures, licensees shall:

§ 37.43(d)(3)(i)

Evaluate an individual's need to know the security plan or implementing procedures; and

§ 37.43(d)(3)(ii)

If the individual has not been authorized for unescorted access to category 1 or category 2 quantities of radioactive material, safeguards information, or safeguards information-modified handling, the licensee must complete a background investigation to determine the individual's trustworthiness and reliability. A trustworthiness and reliability determination shall be conducted by the reviewing official and shall include the background investigation elements contained in § 37.25(a)(2) through (a)(7).

EXPLANATION:

Licensees must limit access to and unauthorized disclosure of their security plans, implementing procedures, and lists of individuals approved for unescorted access. Licensees must have written policies and procedures for controlling access to those documents, and for proper handling and protection against unauthorized disclosure. Licensees must evaluate an individual's need to know before allowing access to the security documents. If the individual has not been authorized for unescorted access, he or she must undergo a background investigation to determine his or her trustworthiness and reliability before being provided the protected information.

QUESTIONS/ANSWERS:

Q1: What kinds of information are licensees required to protect under this subsection?

A1: Licensees are required to limit access to their security plans and implementing procedures to prevent unauthorized disclosure. Licensees are also required to limit access to their list of individuals approved for unescorted access. This includes the information contained in the protected documents.

Q2: Should I protect any forms of information other than hard copies of sensitive information?

A2: Yes. You should protect against any form of unauthorized disclosure of the protected information, including spoken and electronic disclosures.

Q3: Who is allowed access to this protected information?

A3: Licensees may allow access to these documents only to those individuals who have a need to know the information to perform their duties and have been determined to be trustworthy and reliable based on the background investigation requirements set forth in § 37.25(a)(2) – (7).

Licensee employees, agents or contractors, and employees of an organization affiliated with the licensee's company (e.g., a parent company,) may be considered employees of the licensee for access purposes.

If there is any indication that the recipient would be unwilling or unable to provide proper protection for the licensee's sensitive information, the licensee should not authorize that individual to receive it. Licensees must also ensure that individuals not authorized to receive such information do not overhear conversations relating to the substantive portions of the sensitive information.

Q4: If I have a documented basis for having found an individual to be trustworthy and reliable for unescorted access to radioactive material under § 37.25(a), can that individual have access to my security plan and procedures without redundant additional screening?

A4: Yes, as long as the individual has a need to know the information.

Q5: If I need to hire a new employee that will need access to the protected security information, can I accept a current background investigation from another licensee for a prospective new hire transferring from that licensee?

A5: Yes. Licensees are encouraged to share information about the current security authorization of employees departing to work for another licensee, not only for access to radioactive material, but access to sensitive information. This can spare all licensees from having to conduct unnecessary additional background investigations. Part 37 does not require the sharing of access authorization information, however. Such background information can only be shared on a voluntary basis by mutual consent. The licensee

will still need to document the basis for the determination but, assuming that the existing background investigation is not older than ten years, will not need to conduct a new reinvestigation.

Q6: What measures are required for adequate information protection?

A6: To ensure that only trustworthy and reliable individuals with a need to know are allowed access to security plans and procedures, licensees must develop, maintain, and implement written policies and procedures. See § 37.43(d)(2). These policies and procedures must ensure the proper handling and protection of security plans and implementing procedures to protect against unauthorized disclosure. The licensee's policies and procedures should:

- Include 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;
- Address how to protect sensitive information while in use, storage, and transit;
- Address the preparation, identification or marking, and transmission of documents or correspondence containing the licensee's security program information;
- Address how access to the licensee's security program information is to be controlled;
- Include methods for destruction of documents containing security program information;
- Include procedures for the use of automatic data processing systems containing security program information; and
- Address removing documents from the licensee's protected information category when they become obsolete or no longer sensitive.

§ 37.43 General security program requirements (cont'd)

§ 37.43(d) Protection of information. (Cont'd)

§ 37.43(d)(4)

Licensees need not subject the following individuals to the background investigation elements for protection of information:

§ 37.43(d)(4)(i)

The categories of individuals listed in § 37.29(a)(1) through (13); or

§ 37.43(d)(4)(ii)

Security service provider employees, provided written verification that the employee has been determined to be trustworthy and reliable by the required background investigation in § 37.25(a)(2) through (a)(7) has been provided by the security service provider.

§ 37.43(d)(5)

The licensee shall document the basis for concluding that an individual is trustworthy and reliable and should be granted access to the security plan or implementing procedures.

§ 37.43(d)(6)

Licensees shall maintain a list of persons currently approved for access to the security plan or implementing procedures. When a licensee determines that a person no longer needs access to the security plan or implementing procedures or no longer meets the access authorization requirements for access to the information, the licensee shall remove the person from the approved list as soon as possible, but no later than 7 working days, and take prompt measures to ensure that the individual is unable to obtain the security plan or implementing procedures.

§ 37.43(d)(7)

When not in use, the licensee shall store its security plan and implementing procedures in a manner to prevent unauthorized access. Information stored in nonremovable electronic form must be password protected.

§ 37.43(d)(8)

The licensee shall retain as a record for 3 years after the document is no longer needed:

§ 37.43(d)(8)(i)

A copy of the information protection procedures; and

§ 37.43(d)(8)(ii)

The list of individuals approved for access to the security plan or implementing procedures.

§ 37.43(d)(9)

Licensees that possess safeguards information or safeguards information-modified handling are subject to the requirements of § 73.21 of this chapter, and shall protect any safeguards information or safeguards information-modified handling in accordance with the requirements of that section.

EXPLANATION:

This section lists the classes of individuals who are exempt from licensee background investigations for the protection of security information.

Security plans and implementing procedures must be stored to prevent unauthorized access, and Information stored in non-removable electronic form must be password protected.

Information protection procedures and the list of individuals approved for access to the security plan or implementing procedures must be kept as records for 3 years.

Licensees that possess safeguards information or safeguards information-modified handling must protect it in accordance with [10 CFR 73.21](#).

QUESTIONS/ANSWERS:

Q1: Is anyone relieved from the background investigation elements?

A1: Yes. The same categories of individuals who have been relieved from the background investigation elements for unescorted access to the radioactive material are also relieved from the background investigation elements for access to security information. See also Q&As on § 37.29. Under § 37.29(a), these categories are:

1. An employee of the Commission or of the Executive Branch of the U.S. Government who has undergone fingerprinting for a prior U.S. Government criminal history records check
2. Members of Congress
3. An employee of a member of Congress or Congressional committee who has undergone a prior U.S. Government criminal history records check
4. A governor of a State or his/her designated State employee representative
5. Federal, State, or local law enforcement personnel
6. State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives
7. Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i. of the AEA
8. Representatives of the IAEA engaged in activities associated with the U.S./IAEA Safeguards Agreement who have been certified by the NRC
9. Emergency response personnel who are responding to an emergency
10. Commercial vehicle drivers for road shipments of category 2 quantities of radioactive material
11. Package handlers at transportation facilities such as freight terminals and railroad yards;
12. Any individual who has an active Federal security clearance
13. Any individual employed by a service provider licensee for which the service provider licensee has conducted the background investigation for the individual and approved the individual for unescorted access to category 1 or category 2 quantities of radioactive material.

Q2: How should a licensee protect sensitive information while in use, storage, and transit?

A2: The licensee should store the information in a locked cabinet, desk, or office. Information stored in non-removable electronic form must be password-protected. Licensees need to address how employees must protect the sensitive information while in their possession both at and away from work. Access to the keys, combinations, passwords or other means used to secure the information needs to be limited to those persons authorized access to the information. Additional information on the protection of sensitive security related information can be found in NRC Regulatory Issue Summary 2005-31, "Control Of Security-Related Sensitive Unclassified Nonsafeguards Information Handled By Individuals, Firms, And Entities Subject To NRC Regulation Of The Use Of Source, Byproduct, And Special Nuclear Material." The document is available on the NRC Web Site at: <http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2005/ri200531.pdf>.

Q3: How should a licensee prepare, identify, mark, and transmit documents or correspondence containing the licensee's security program information?

A3: A good practice is to prepare and mark licensee-generated security program information in such a manner as to ensure easy identification and proper handling. The front and back of folders containing such information should also be marked for easy identification and proper handling.

Documents that do not in themselves contain security program information, but are used to transmit one or more documents containing this information, should be marked to indicate that security program information is contained in the documents transmitted. Although security program information is not typically transmitted to the NRC, if there is a need for such transmittals, they should be marked: "**Withhold from Public Disclosure in Accordance with 10 CFR 2.390.**" These markings should be placed at the top and bottom of only the first page of the transmitted document.

Q4: What methods should a licensee use for destruction of documents containing security program information?

A4: It is a good practice to destroy documents containing this information using a method that will prevent reconstruction of the information. Documents may be destroyed by tearing them into small pieces or by burning, pulping, pulverizing, shredding, or chemical decomposition. Similar methods may be used for film and microform media. ("Microform" is the generic term for any material on film or paper, such as a microfiche, containing a smaller reproduction of a document for transmission, storage, reading, and printing.) Electronic media, such as tapes, floppy discs, compact discs, digital video discs, and thumb drives, may be destroyed by shredding, smashing, burning, or chemical decomposition, and data on hard drives and servers should be erased, or the drives reformatted, before submitting them for recycling. (Note: Regardless of the storage medium, security program information should not be sent to recycling without being destroyed first.)

Q5: What methods should a licensee use to protect security information when using a data processing system to store security program information?

A5: Individuals should protect the information during use by maintaining control and by ensuring that only individuals with the “need-to-know” and determined to be trustworthy and reliable have access to the information. One method that you may use is to password protect documents. You may also use encryption techniques or place the documents on a restricted drive. Whatever method you use should be described in the information protection procedures.

Q6: When should a licensee remove documents from the licensee’s protected information category if they become obsolete or no longer sensitive?

A6: A licensee may remove documents from its protected information category when it no longer needs to have a security plan and procedures, i.e., when it no longer needs to possess an aggregated category 2 or greater quantity of radioactive materials. Until that time, it is unlikely that all of the information in the licensee’s security plan or procedures will become obsolete or no longer sensitive. Neither the plan nor the procedures may be relieved from Part 37 information protection requirements if they retain any sensitive information, and even the original versions of the plan and procedures are likely to retain some sensitive information until the licensee no longer needs to protect a category 2 or greater quantity of material.

Q7: What documents do I need retain under this section? How long must I retain the documents?

A7: You must retain a copy of the procedures on information protection. You also must keep a copy of the list of individuals approved to have access to the security information. These records must be kept for 3 years after the record is no longer needed, or until the NRC terminates the license, as provided by § 37.103.

Q8: Will licensees need to handle SGI?

A8: Some licensees will be required to handle SGI-M, which is a subset of SGI. The licensees considered to be handling this kind of security information include panoramic and underwater irradiators that possess greater than 370 TBq (10,000 Ci) of byproduct material in the form of sealed sources; manufacturers and distributors of items containing source material, or byproduct or special nuclear material in greater than or equal to category 2 quantities of concern; and licensees that transport nuclear material in greater than or equal to category 1 quantities of concern. The security information developed and used by these licensees is considered to be SGI-M, and must be protected under the measures for SGI-M specified in §§ 73.21 and 73.23.

Q9: Would an engineer designing the security systems for a blood irradiator room need to undergo a background investigation to have unescorted access to the irradiator room when it contains radioactive material?

A9: Yes, if the engineer is allowed unescorted access to the security zone containing the irradiator, the engineer would be subject to the access authorization program in Subpart B of Part 37 and would need to undergo a background investigation. If irradiator room was set such that the engineer would not need to enter the security zone or will be escorted while within the security zone, then he/she would not be subject to Subpart B. If the engineer needed access to protected security information, § 37.43(d)(4)(ii) permits a licensee to accept written verification from a security service provider that the provider

has conducted the background investigation required in § 37.25(a)(2) through (a)(7) and has determined its employee to be trustworthy and reliable. This would permit the security service provider's employee to have access to the protected information.

Q10: I have an employee who needs to know some components of my security plan to perform her job, but doesn't need to have access to the plan itself or implementing procedures. Does she need to undergo a background check to have access to parts of my security plan?

A10: Yes. An insider with even a limited knowledge of the security plan or its implementing procedures may be able to use this knowledge or convey it to others for malevolent purposes. A security guard with access only to an alarm-response schematic, for example, or an IT specialist with access only to a communication system for security personnel, could significantly compromise the security of radioactive material against theft, sabotage, or diversion. And if an employee has become familiar with the plan and procedures, you may need to conduct a background investigation and make a T&R determination even if he or she does not have actual access to the document. An individual already approved for access to radioactive material would not need a re-investigation, but would need to have some knowledge of the security plan or procedures to fulfill a job responsibility in order to be authorized access to any part of these documents.

§ 37.45 LLEA coordination.

§ 37.45(a)

A licensee subject to this subpart shall coordinate, to the extent practicable, with an LLEA for responding to threats to the licensee's facility, including any necessary armed response. The information provided to the LLEA must include:

§ 37.45(a)(1)

A description of the facilities and the category 1 and category 2 quantities of radioactive materials along with a description of the licensee's security measures that have been implemented to comply with this subpart; and

§ 37.45(a)(2)

A notification that the licensee will request a timely armed response by the LLEA to any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of material.

EXPLANATION:

Licensees must coordinate, to the extent practicable, with an LLEA for responding to threats to the licensee's facility, including any necessary armed response. The licensee must provide a description of its facilities, radioactive materials, and security measures. The licensee must also say it will request a timely armed response by the LLEA to any actual or attempted theft, sabotage, or diversion.

QUESTIONS/ANSWERS:

Q1: What kinds of LLEA coordination activities are required?

A1: The coordination activities could involve such things as meetings, telephone conferences, plant tours, training in radiation protection, tabletop exercises, and other communications to provide information. As discussed in more detail in the subsequent Qs & As for this section, the licensee must notify the LLEA that it will request an armed response to any actual or attempted theft, sabotage, or malevolent diversion of radioactive material. The licensee must also provide information about the facility, its radioactive materials, and the licensee's current security measures. To facilitate a timely, coordinated, and effective response to a security incident, the licensee should verify site and LLEA contact information.

Q2: What is the purpose of the LLEA coordination?

A2: A timely and effective response to a security incident is part of an effective physical protection system. Because certain situations may necessitate an armed response, a strategy that is consistent in scope and timing with realistic potential vulnerabilities of the subject radioactive material should be coordinated well in advance with the LLEA. Another purpose of coordination is to provide the responsible LLEA with an understanding of the potential consequences associated with malevolent use of the radioactive material, so that the LLEA can determine the appropriate priority of its response. The LLEA response would be needed not only to interdict and disrupt an attempted theft or sabotage of the radioactive material, but possibly also for offsite

coordination to protect public health and safety and mitigate the potential consequences of a theft, sabotage, or malevolent diversion of radioactive material.

Q3: There are many different kinds of agencies responsible for providing security, including private security guard forces on the campuses of universities, hospitals, and other institutions. What kinds of law enforcement organizations should a licensee seek to coordinate with?

A3: The LLEA will need to be authorized by a government entity to make arrests and have the capability to provide an armed response. The LLEA need not be a municipal or county police force, however. If a city or county hospital or state university campus police force is the nearest law enforcement agency to the licensee's operation capable of providing an armed response and making arrests, that police force would meet the definition of an LLEA.

A licensee will also need to 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, and in such cases, the licensee will have to identify and coordinate with the closest LLEA able to provide an armed response and arrest perpetrators when the primary LLEA is off-duty.

Q4: Can an on-site proprietary professional security force with trained and armed officers be considered an LLEA?

A4: No, unless the private security force meets the criteria for an LLEA as defined in § 37.5. An on-site armed force may provide the initial licensee response, but the licensee must still coordinate with an off-site LLEA, unless the on-site force is also authorized by a government agency to bear arms and make arrests, as many university campus police forces are. The off-site LLEA should still be notified of incidents immediately in case additional assistance is needed, and to enable the LLEA to assess the potential for off-site impacts and the need to notify other agencies.

Q5: If I have a written agreement with a third party service that provides off-duty local law enforcement agents on site at all times, would that be acceptable to demonstrate compliance with the LLEA coordination requirement?

A5: Even if the individual off-duty police officers working for the third-party security service are authorized to carry firearms, make arrests, and provide an armed response to a security incident at your facility, the company itself would not qualify as an LLEA, because it must be approved as *an agency* by a federal, state, or local government to carry out these duties. Thus, an agreement with such a third party to provide security for your site is not, in itself, sufficient to demonstrate compliance with the coordination requirement. You would still need to coordinate with an LLEA to request its assistance for either on-site or off-site support, or both, in the event of an attempted or actual theft, sabotage, or diversion. Among other things, you would, for example, still need to coordinate with the LLEA under § 37.45(d) at least every 12 months, or when changes to your facility's design or operation could adversely affect the potential vulnerability of your material to theft, sabotage, or diversion. You may also want to consider whether and how the off-duty police officer employees of the service provider could coordinate with their respective offsite LLEA employers in the event of a security incident at your site.

Q6: What kinds of information should a licensee provide to an LLEA for effective coordination?

A6: The information should include the important aspects of a licensee's physical protection program and other factors that would aid the LLEA to appropriately prioritize and respond to an alarm or other request by the licensee for response. As a good practice, examples of information a licensee could discuss with the LLEA include, but are not limited to:

- 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);
- Site-specific physical protection measures 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; and
- Licensee and LLEA points of contact for plans to recover stolen material that has been removed to an offsite location.

At a minimum, under § 37.45(a) information for coordination activities must include a description of the facility, the quantity and type of radioactive materials, the security measures in place at the licensee's facilities, and a notification that the licensee will request a timely and armed response to any actual or attempted theft, sabotage, or diversion of the licensee's radioactive materials. The licensee is required under § 37.45(c) to document its coordination efforts, including the dates, times, and locations of meetings and a list of licensee and LLEA staff present at the meetings.

Q7: Does the NRC require a licensee's security staff to have firearms?

A7: The rule does not require a licensee's security staff to be armed, nor does it prohibit licensees from arming their security staff. The licensee must comply with applicable state and local law.

Q8: What does the NRC mean by coordinating with an LLEA "to the extent practicable"?

A8: The NRC recognizes that some LLEAs may be reluctant to engage in coordination activities with a licensee, and added "to the extent practicable" to avoid putting licensees into non-compliance for actions they cannot reasonably be expected to control. This phrase allows a licensee to remain in compliance with the rule when a LLEA will not participate in any coordination activities. The licensee can comply with this requirement simply by documenting in accordance with § 37.45(c) that it has initiated and periodically contacted the LLEA during the required timeframe, provided information about its security needs and intent to request an armed response, and requested to

coordinate a response to a security incident involving a category 2 or greater quantity of radioactive materials.

Q9: What should a licensee request as an adequate LLEA response to a threat to a licensee's facility? For example, would a single officer with radio backup be sufficient, or is an entire SWAT team necessary?

A9: The LLEA will decide what is adequate, and respond as appropriate to the event based on the agency's understanding of the situation and its potential consequences. One of the purposes of establishing liaison with the LLEA is to provide it an understanding of the potential consequences associated with malevolent use of the radioactive materials subject to this rule, so that the LLEA can appropriately determine the priority of its response. The LLEA response is needed for offsite coordination to protect the public health and safety, and to mitigate the potential consequences of malevolent use of radioactive material.

Q10: Can LLEAs have access to the licensee's physical protection information?

A10: The licensee is *required* to give an affected LLEA some physical protection information. Under § 37.45(a)(1), the licensee must provide "[a] description of [its] facilities and the category 1 and category 2 quantities of radioactive materials along with a description of [its] security measures that have been implemented to comply with this subpart."

Q11: What are the LLEA's responsibilities for protecting this sensitive information?

A11: LLEAs are not subject to NRC information protection requirements, although they may be subject to other information protection requirements under state or local law. Under § 37.29(a)(5), state, local, and other law enforcement authorities are members of occupational groups deemed to be trustworthy and reliable by virtue of their employment status, and these authorities protect sensitive law enforcement information routinely in the course of their operations.

Q12: Would it be appropriate for a licensee to give a diagram of its facility to an LLEA?

A12: Depending on the size of the licensee's facility and the location of the at-risk material, providing a facility plan to the LLEA may be appropriate. The purpose of coordination is to provide the LLEA with the information it deems necessary to do its job in responding to potential malevolent acts involving lost, stolen, or missing radioactive material from the licensee's facility.

Q13: If a licensee is required to have an emergency plan under [10 CFR 30.32\(i\)](#), can the licensee satisfy any of the requirements of § 37.45 for LLEA coordination by complying with the emergency planning requirements of § 30.32(i)(3)(xii)?

A13: Yes, if the licensee's emergency plan specifically calls for LLEA coordination. Section 30.32(i)(3)(xii) provides, among other things, that an emergency plan under this section must include "[p]rovisions for conducting quarterly communications checks with offsite response organizations ... to test response to simulated emergencies." The quarterly communications checks must include "the check and update of all necessary telephone numbers." Thus, if a licensee possesses at least a category 2 quantity of

radioactive material and has an emergency plan that complies with 10 CFR 30.32(i) and if the plan specifies the nearest LLEA or LLEAs as “offsite response organizations” with which the licensee conducts quarterly communications checks, the licensee may cite the plan as one component of a demonstration of compliance with the general requirement under § 37.45(a) to “coordinate, to the extent practicable, with an LLEA for responding to threats to the licensee’s facility.” These quarterly checks could also enable the licensee to demonstrate compliance with the requirement in § 37.45(a)(2) for “[a] notification that the licensee will request a timely armed response by the LLEA to any actual or attempted theft, sabotage, or diversion,” and would also comply with the requirement in § 37.45(d) to “coordinate with the LLEA at least every 12 months.” Depending on the kinds of information in the emergency plan, it may also enable the licensee to comply with the requirement in 37.45(a)(1) to provide to the LLEA “[a] description of the facilities and the category 1 and category 2 quantities of radioactive materials along with a description of the licensee’s security measures that have been implemented to comply with this subpart.” The plan itself would not, however, enable the affected licensee to comply with the notification requirements of § 37.45(b), the documentation requirements of § 37.45(c), or the requirement in § 37.45(d) to coordinate with the LLEA “when changes to the facility design or operation adversely affect the potential vulnerability of the licensee’s material.”

Q14: Is there some method in place whereby an LLEA may become informed about radioactive materials and the licensee’s possession of such materials, including those in devices?

A14: Yes. The Federal government through the Department of Homeland Security (DHS) is actively working with LLEA organizations to improve their awareness and response capabilities across a wide variety of threats by providing information, training, and funds. LLEAs can obtain additional information about training from the National Domestic Preparedness Consortium at <http://www.ndpc.us/index.html>, the local FBI Field Office Weapons of Mass Destruction Coordinator at <http://www.fbi.gov/contact-us/field>, and the Department of Homeland Security National Network of Fusion Centers at http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

In coordination efforts with the LLEA, the licensee’s information should add to, and help reinforce, the LLEA’s knowledge of radioactive materials and the potential risks associated with both their legitimate and malevolent uses. Licensees can invite the LLEA to attend their annual health and safety and security training sessions.

Q15: Do I have to conduct response exercises with my LLEA or otherwise train my LLEA?

A15: No. You are not required to offer training to the LLEA. Exercising the response portion of your security plan is a good practice, but it is not required. Some LLEAs may not be willing or able to participate, and the NRC also recognizes that requiring all licensees to exercise their response plans may not be cost-effective for small licensees with less complex security plans.

Q16: What are the LLEA coordination requirements for work at a temporary job site?

A16: The rule does not require a licensee to coordinate with an LLEA for work at temporary job sites. However, licensees are not precluded from coordinating with the LLEA as an extra margin of security for work at temporary jobsites.

For licensees that routinely work at temporary job sites for months at fixed locations, you may want to identify and notify the closest LLEA for the benefit of both parties, even though it is not required.

LLEA coordination (cont'd)

§ 37.45(b)

The licensee shall notify the appropriate NRC regional office listed in § 30.6(a)(2) of this chapter within 3 business days if:

§ 37.45(b)(1)

The LLEA has not responded to the request for coordination within 60 days of the coordination request; or

§ 37.45(b)(2)

The LLEA notifies the licensee that the LLEA does not plan to participate in coordination activities.

EXPLANATION:

The appropriate NRC regional office must be notified within three business days if the LLEA has not responded to the licensee's request for coordination within 60 days, or the LLEA notifies that it does not plan to participate in coordination activities.

QUESTIONS/ANSWERS:

Q1: Would an LLEA's decision not to coordinate put a licensee into non-compliance with these coordination requirements?

A1: No, the NRC recognizes that it cannot exercise authority over LLEAs, or any party, over which a licensee has no control and the NRC has no legal jurisdiction. The NRC also recognizes that an LLEA may have good reasons, including resource limitations and the possibility of other coinciding incidents within its jurisdiction, for not engaging in coordination activities with a licensee.

Q2: What happens when an LLEA declines to coordinate with a licensee?

A2: A licensee must notify the NRC whenever an LLEA with jurisdiction over the licensee's facilities declines to engage in coordination activities.

Q3: To trigger the requirement to notify NRC, must a licensee have a written or oral statement from an LLEA stating that it does not plan to participate in coordination activities?

A3: No. Because the rule requires the licensee to notify NRC if the LLEA has not responded within 60 days to a licensee's request for coordination, a licensee need not have an official statement from the LLEA that the LLEA does not plan to participate. The LLEA's actions can demonstrate that the LLEA does not plan to coordinate with the licensee.

Q4: How should a licensee notify the NRC regional office to meet § 37.45(b) requirements?

A4: The licensee may notify the NRC regional office by letter, fax, e-mail, or telephone. Contact information is provided in [10 CFR 30.6](#). If you contact the NRC by telephone, you should document the conversation so you will have a record of the notification.

Q5: Some state or local jurisdictions may have a requirement that the initial response to any emergency involving radioactive materials must be provided by other than armed LLEA personnel, such as hazmat responders. How do I know whether such a requirement affects my LLEA's response to a security incident?

A5: You should ask the LLEA. A convenient time to ask could be during one of your required interactions with the LLEA to develop or maintain effective coordination of responses to a security incident. If there is such a state or local requirement, you should notify the designated first responder organization about the nature of your emergency response needs during a security incident, so that unarmed and unsuspecting responders are not needlessly put in harm's way. You may also ask the hazmat or other designated first responder to coordinate with the LLEA to develop an agreed-upon response protocol that would allow you to contact the LLEA first for a response to a security incident involving your radioactive materials.

§ 37.45 LLEA coordination (cont'd)

§ 37.45(c)

The licensee shall document its efforts to coordinate with the LLEA. The documentation must be kept for 3 years.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

Q1: Besides the documentation of meetings and correspondence, what other information on LLEA coordination activities should a licensee document?

A1: A licensee should also document any written agreement or pre-arranged response plan with an LLEA if the LLEA is willing to enter into such an agreement or plan.

Q2: In cases where an LLEA has decided not to participate in coordination activities, how should a licensee document that it has made a good faith effort to coordinate with that LLEA? Must a licensee send all correspondence to such an LLEA by certified mail, UPS, or other third-party delivery method in order to produce a verifiable record?

A2: No. Using certified mail, UPS, or another third-party delivery method to document the licensee's transmittal of a coordination request would be an acceptable way to comply with the requirement, but the licensee need not use such methods if it keeps a copy of the dated letter, e-mail, or other correspondence and maintains records of calls to the LLEA.

Q3: Must a licensee maintain paper records of its LLEA coordination activities and correspondence? What about e-mails and other electronic communications, including digitized images, and documents generated on a computer?

A3: No. Records do not need to be maintained in paper form. As long as the record is legible and retrievable, the licensee can keep a reproduced copy, microform copy, or electronic copy. Under § 37.45(c) licensees must maintain records of LLEA coordination activities for a period of 3 years

§ 37.45 LLEA coordination (cont'd)

§ 37.45(d)

The licensee shall coordinate with the LLEA at least every 12 months, or when changes to the facility design or operation adversely affect the potential vulnerability of the licensee's material to theft, sabotage, or diversion.

EXPLANATION:

The licensee must coordinate with the LLEA every 12 months.

QUESTIONS/ANSWERS:

Q1: When should I coordinate with the LLEA concerning changes to my facility's design or operation?

A1: You should notify the LLEA as promptly as possible after making any changes to the facility design or operation that could affect the LLEA's response to an incident. If possible, you should notify the LLEA before making such changes. It is also a good practice to afford LLEA response personnel the opportunity to familiarize themselves with the facility once any design or operating changes have been made.

Q2: I understand that I must coordinate with the LLEA at least every 12 months even if there are no significant changes to my facility's design or operation. What topics or issues should I cover when I contact the LLEA in one of these 12-month coordination activities?

A2: The coordination may include, but shouldn't be limited to, a discussion of any recent security developments since your last coordination meeting, and the potential consequences of any planned or potential changes in either your facilities or operations, or in the LLEA's capabilities or policies. Thus, you should be prepared to review any security events or trends over the preceding 12 months that could have involved the LLEA, and for which you have taken or plan to take corrective action. You should also be prepared to discuss any changes in your facility's existing or planned security measures, policies, notification procedures, equipment, or other resources that you anticipate might affect the LLEA's response, or ability to respond, to an actual or attempted theft, sabotage, or diversion of radioactive materials at your facilities over the upcoming 12 months. An example of such a change would be a revision of your security plan or procedures, a new monitoring, alarm, or communication system, or a decision to procure security services from a commercial contractor.

You should also discuss any changes in your LLEA point-of-contact information, either at your facility or at the LLEA. And depending on your and the LLEA's available time and resources, you could offer the LLEA a tour of your facility, and/or an opportunity to participate in planned drills or tabletop exercises.

Q3: Must I convene a face-to-face meeting for 12-month coordinations?

A3: No. Although a face-to-face meeting with LLEA officials would be desirable, the NRC understands that competing demands on the LLEA's time may make such meetings difficult to arrange.

Q4: Who should participate in these coordination activities?

A4: At a minimum, participants on the licensee's side should include the individual with operating responsibility for implementation of the security plan or his or her designee, and the individual identified to the LLEA as the licensee's point of contact for coordination activities, if the two responsibilities are not assigned to the same person. If the participants need a prompt decision from a higher level of licensee management, it would also be useful to have that individual attending. Depending on current demands for LLEA assistance, it may be difficult to get the desired LLEA representative to attend, but for consistency's sake, the licensee should try to ensure that at least the designated LLEA point of contact, if there is one, participates.

§ 37.47 Security zones

§ 37.47(a)

Licensees shall ensure that all aggregated category 1 and category 2 quantities of radioactive material are used or stored within licensee-established security zones. Security zones may be permanent or temporary.

EXPLANATION:

All aggregated category 1 and category 2 quantities of radioactive material must be used or stored within licensee-established permanent or temporary security zones.

QUESTIONS/ANSWERS:

Q1: How do I determine whether I possess an aggregated category 1 or category 2 quantity of radioactive material?

A1: The sum-of-the-fractions method, also known as the unity rule, is used to determine whether the licensee possesses a category 1 or category 2 quantity of radioactive material. A licensee may need to implement Part 37 requirements even if it does not possess any single source or single radionuclide in excess of a category 2 threshold. For examples of unity rule calculations, see Q&A 1 for the definitions of category 1 and category 2 quantities in Subpart A.

Q2: What is a security zone, and what is its purpose?

A2: A security zone is an area, defined by the licensee, that both isolates and controls access to category 1 or category 2 quantities of radioactive material. The purpose of the zone is to define the area containing the quantities of material that must be protected. A security zone effectively defines where the licensee will apply the isolation and access control measures required by Part 37. All category 1 and category 2 quantities of radioactive material must be used or stored only within a security zone.

Q3: Can I use an area established for radiation safety to meet the requirements for a security zone? Can they be the same?

A3: Depending on the licensee's safety and security needs, the boundaries of these two types of areas may differ or be identical. Because the purpose of security zones is different from the radiation safety purposes of the restricted areas and controlled areas defined in [10 CFR Part 20.1003](#), the security zone does not have to be the same as either of these areas, although it may be.

Because measures to control access are required for both radiation protection and security, however, a licensee does have the flexibility to use an area required for radiation protection purposes to fulfill the required functions of a security zone. Section 37.47 is intended to allow licensees flexibility in establishing access control and isolation in a manner that would allow reliance on existing systems and procedures, already in use for radiation protection, for physical security.

Consider, for example, a temporary well-logging operation where the licensee is required by § 39.71 to have a “restricted area” to “maintain direct surveillance ... to prevent unauthorized entry.” A licensee could define a security zone with the same boundaries as this “restricted area,” which is defined in 10 CFR 20.1003. as “an area, access to which is limited by the licensee for the purpose of protecting individuals against undue risks from exposure to radiation and radioactive materials.” In this case, the restricted area required for radiation protection may also serve to provide security from exposure to this radiation.

Similarly, a radiographer could choose to define a security zone with the same boundaries as the “high radiation area” over which radiography licensees are required by 10 CFR 34.51 to “maintain direct visual surveillance ... to protect against unauthorized entry.” (As defined in 10 CFR 20.1003, a “high radiation area” is “an area, accessible to individuals, in which radiation levels from radiation sources external to the body could result in an individual receiving a dose equivalent in excess of a specified dose rate.”)

Q4: How does NRC define a “temporary” security zone?

A4: NRC considers a temporary security zone to be one established by the licensee to provide physical protection for a category 1 or category 2 quantity of radioactive materials for a specified, limited expected time, which may be several minutes to several months, to accomplish a specified task.

Q5: How does a permanent security zone differ from a temporary one?

A5: A permanent security zone uses permanent barriers to provide isolation and aid in controlling access to the material. These barriers may consist of: fences; gates; free standing walls for exterior areas; exterior or interior building walls; doors; locked windows; bars; or grillwork. The barriers or walls control access to the security zone through established access control points, deter and delay penetration by unauthorized person or unauthorized people, and aid detection by providing an indication of forced penetration.

Temporary security zones need not have permanent barriers at their boundaries, although licensees may make use of permanent barriers if they are available at the location of the work. Isolation of the material and the people using the material in a temporary security zone may be provided by other devices used to warn passersby of the restricted nature of the area. Access control can also be accomplished through surveillance of the material, persons, and area by an authorized individual.

Q6: If I'm an NRC licensee servicing a sealed source or other device in an Agreement State, and my customer's Agreement State regulatory agency hasn't yet adopted Part 37-compatible implementing regulations, am I still required to follow the Part 37 requirements of my license?

A6: Yes. You will need to follow the security requirements of both your license and the Agreement State you're working in. Although you will have to meet the requirements of both your NRC license and your customer's Agreement State license, the points at which these requirements apply may differ according to whether and when possession of the source changes hands. If, for example, you're doing maintenance that does not require you to remove the source and take possession for offsite shipment you will be

subject to the applicable access control, monitoring, documentation, and other requirements of your customer's Agreement State license. If you're bringing a replacement source onto your customer's site, however, your license's requirements apply, along with those of your customer's license, when you arrive onsite, until you have installed the replacement source in the customer's device and completed any remaining testing and maintenance required by your license, and the customer has taken possession of the source. In any case, both you and your customer licensee need to have a clear understanding from the outset about which of you is responsible for compliance with what requirement. Both of you should know, for example, which one of you is responsible for calling an LLEA in the event of a theft, sabotage, or diversion.

If your Agreement State customer licensee believes that compliance with your license would cause a violation of the customer's license requirements, however, you and your customer should contact your regional NRC Office and the appropriate Agreement State regulatory agency for further guidance.

§ 37.47 Security zones (cont'd)

§ 37.47(b)

Temporary security zones must be established as necessary to meet the licensee's transitory or intermittent business activities, such as periods of maintenance, source delivery, and source replacement.

EXPLANATION:

Licenseses must establish temporary security zones as necessary for such time-limited or intermittent business activities as source maintenance, delivery, and replacement.

QUESTIONS/ANSWERS:

Q1: When should I establish a temporary security zone?

A1: You should establish a temporary security zone whenever you have a periodic or unplanned short-term operating requirement for the use or storage of a category 1 or category 2 quantity of radioactive material outside of a permanent security zone. Examples of such a requirement could be a need to repair, maintain, or calibrate a radioactive source or a device containing a source at a location where the source or device is not routinely used or stored. You should also establish a temporary security zone when you take delivery of a source or device outside of your established, permanent security zone. Additionally, work at a temporary job site will require establishment of a temporary security zone at the job site.

Q2: How do I establish a temporary security zone?

A2: Although you may be able to take advantage of permanent barriers if they are available at the site, you may establish a security zone simply by keeping the area under direct supervision and control by an approved individual or individuals.

Q3: May I station someone who is not an approved individual outside a temporary security zone with a radio or other means of communication to notify people inside the zone about an impending intrusion?

A3: Nothing in the rule prevents you from using an unapproved individual to provide additional continuous direct surveillance, but under § 37.47(c)(2), you may not rely on any individual who has not been approved for unescorted access to be a monitor of access to a temporary or permanent security zone unless that individual is himself monitored by an approved individual. Allowing an individual, who has not been determined trustworthy and reliable under this Part, to monitor a security zone without surveillance by an approved individual could provide an opportunity for insiders to compromise the security of the material.

Q4: How large should a temporary security zone be?

A4: The rule does not specify the size of a security zone. Locations are configured differently and do not lend themselves to generically defined physical areas, the security

zone concept permits significant flexibility for licensees to account for a range of site-specific concerns. Its physical dimensions will be determined by the licensee on an individual basis and can change based on operating status and security needs. The security zone may be as small as a locked cabinet, or as large as a warehouse area.

Q5: If I routinely work in a large plant facility, and move frequently from one location to another within the same facility, do I have to establish a different temporary security zone for each location, or can I consider the whole facility to be a temporary security zone that encompasses all my on-site work locations?

A5: Your decision about the proper size of your temporary security zone is yours alone to make, because only you can know the conditions at the site and the requirements of your work. In making your decision, however, you will need to consider the basic performance requirements for establishing a security zone (see § 37.47(c)). Under § 37.47(c) these requirements are to isolate the subject radioactive materials to allow unescorted access only to approved individuals, using either: direct control of the security zone by approved individuals at all times; continuous physical barriers that allow access to the security zone only through established access control points; or a combination of continuous physical barriers and direct control. If the facility is small enough to provide continuous physical barriers that allow access only through an established access control point that you control, for example, you may be able to consider the entire facility a temporary security zone. For those spaces where you will be using your source or device between access-controlled permanent zones, your temporary security zone need be no larger than the space you need to control access.

Q6: How do I meet Part 37 requirements for controlling unescorted access to a temporary security zone if I'm at a temporary job site that doesn't have such continuous physical barriers as lockable doors?

A6: When work needs to be done inside a temporary security zone that doesn't have physical barriers or special equipment, a licensee could meet the requirements for controlling unescorted access by having the material, persons, and area within the zone under the direct control of approved individuals at all times.

Q7: When would a temporary security zone have to be considered permanent?

A7: The rule does not specify a time limit by which a temporary security zone must become permanent, but § 37.47(b) does require that a temporary security zone "necessary to meet the licensee's transitory or intermittent business activities, such as periods of maintenance, source delivery, and source replacement." Most licensees will probably have a business interest in maintaining temporary security zones for only a limited time, since the cost of isolating radioactive material behind permanent physical barriers is likely to be cheaper than the labor cost of maintaining continuous direct surveillance.

§ 37.47 Security zones (cont'd)

§ 37.47(c)

Security zones must, at a minimum, allow unescorted access only to approved individuals through:

§ 37.47(c)(1)

Isolation of category 1 and category 2 quantities of radioactive materials by the use of continuous physical barriers that allow access to the security zone only through established access control points. A physical barrier is a natural or man-made structure or formation sufficient for the isolation of the category 1 or category 2 quantities of radioactive material within a security zone; or

§ 37.47(c)(2)

Direct control of the security zone by approved individuals at all times; or

§ 37.47(c)(3)

A combination of continuous physical barriers and direct control.

EXPLANATION:

Security zones must allow unescorted access only to approved individuals by either: isolating the radioactive materials with continuous physical barriers that allow access only through established control points; controlling the security zone directly by approved individuals at all times; or a combination of physical barriers and direct control.

QUESTIONS/ANSWERS:

Q1: For the purposes of Part 37, what is an “approved individual?”

A1: As defined in § 37.5 of this Part, an approved individual is an individual whom the licensee has determined to be trustworthy and reliable in accordance with Subpart B of this Part and who has completed the training required by § 37.43(c).

Q2: For the purposes of Part 37, what is a “continuous physical barrier?”

A2: A continuous barrier must limit access to the security zone only through one or more established access control points. The continuous barrier should have no openings, other than access control points, including windows, 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 floor to structural ceiling, and openings (such as vents) greater than 96 square inches, where 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 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.

Q3: If I need to use locks, what controls are required to limit access to the keys to my facilities?

A3: Access to the keys to locks for security zones and category 1 or 2 materials or devices within those zones must be limited solely to those individuals who must have access to perform their assigned tasks, and who have been determined trustworthy and reliable in accordance with Subpart B. But a better 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 new approved individuals. The same is true for the control of lock combinations over time. Key cards, cipher locks, or some other type of electronic access control device should be used where feasible instead of keyed or combination locks. Additionally, each approved individual should have a unique access code. With these devices, the access code can be deleted after an individual no longer requires access to the security zone or if a key card is lost or stolen.

Q4: Does Part 37 require that locks for different rooms be re-keyed to different keys or combinations?

A4: No. Different keys or lock combinations for different rooms would, however, improve security by making it more difficult for an adversary to aggregate radioactive material into a category 1 or category 2 quantity. It is up to the licensee to determine how access to the facility will be controlled.

Q5: Shouldn't the features of a device containing a category 1 or category 2 quantity of radioactive material be given credit for providing some isolation for purposes of access control?

A5: No. Part 37 requirements were written with full awareness of the features of devices licensees commonly use, as well as the quantities of licensed material these devices typically contain. The devices are designed to limit access to the sources for radiation protection purposes, whereas Part 37 also requires controlling access to devices containing the radioactive material. The requirements were designed to provide a defense-in-depth strategy for the protection of radioactive material in category 1 or category 2 quantities. No single control can provide the same level of protection as the combination of controls required by Part 37.

Q6: Self contained irradiators have shown themselves to be very safe for day-to-day use without operators having access to the radioactive material. Controlling access to this material is generally much easier than controlling access to the irradiator itself. Are the Part 37 requirements expected to address access to the radioactive material, or to the irradiator?

A6: Both. To address potential misuse with malevolent intent, Part 37 requirements are designed to control access both to the radioactive material and to the irradiator by controlling access to the security zone. The NRC has engaged the expertise of national laboratories that have shown that these devices may be vulnerable to theft, sabotage, or diversion under certain scenarios. For this reason, and the possibility that malevolent acts could be assisted by a trained insider, the NRC has determined that certain additional security measures are necessary in the current threat environment. Part 37 uses a layered, defense-in-depth approach to enhance the security of radioactive material in category 1 and category 2 quantities. No single measure can provide the required security for this material. Therefore, a licensee must implement all applicable Part 37 requirements unless the licensee requests and NRC approves an exemption.

Q7: Can the requirements for controlling access be waived if compliance is overly burdensome?

A7: A licensee may seek and the NRC may grant an exemption from any NRC requirement on a case-by-case basis, but the NRC is unlikely to grant relief from an access control requirement simply because the licensee considers it burdensome.

Q8: What if a licensee's truck carrying a category 1 or category 2 quantity of radioactive material breaks down and must be towed to a shop for repairs, and the repair shop doesn't allow licensee personnel into the repair bay to keep the on-board security zone under continuous surveillance?

A8: The licensee must still meet the applicable requirements of Part 37 to ensure that the sources and their shielding devices are not removed. In this case, an approved individual could lock the truck, remain at the shop, and keep the truck in sight to control and maintain constant surveillance of licensed material. Alternatively, the licensee could remove the device and maintain control of the material until the truck is repaired or the source(s) can be returned to a licensed facility.

Q9: Can the requirements of § 37.53 for independent physical barriers for mobile sources be used to control access and prevent an unescorted individual from entering a room where a radioactive source is located?

A9: No. Section 37.53 is not intended to achieve total access control, but to provide additional delay in removing a mobile device from the facility, temporary job site, or vehicle. For mobile devices, delay barriers are required *in addition to* the access controls required by § 37.47. Without the additional barriers, a portable or mobile device could more easily be stolen, sabotaged, or diverted.

Q10: If I have a room with a conventional door lock and entry alarms, what else do I need for an effective security zone?

A10: To protect against unauthorized access to and removal of material behind conventional door locks with entry alarms, you may need to consider such additional means as guards, closed circuit television, or motion detectors.

The specific system and means to protect material is left to your discretion, but to meet Part 37 requirements, you should consider reasonably foreseeable actions by adversaries and the methods they could use to gain unauthorized access. Walls should be continuous from floor to ceiling, for example. Vents and other openings greater than 96 square inches, where the smallest dimension is greater than 6 inches, should have metal grates, expanded metal, bars, or some other barrier that cannot be removed from outside the security zone. For additional technical guidance on the capabilities and applications of different access control system technologies, you may refer to [NUREG-1964, Access Control Systems](#).

Q11: For facilities that may store radioactive materials or devices, such as dosimetry calibrators, outside a protected area, what constitutes an adequate physical barrier? Would an unlocked concrete container be adequate, for example, if it could not be opened without the use of a mobile crane?

A11: The adequacy of a barrier around a storage area would depend on site-specific factors that the licensee should consider. These should include, for example: the configuration of the storage area, and whether it abuts and uses the perimeter fence at the site boundary; the proximity of the radioactive materials to the fence and their vulnerability to theft or diversion; and the proximity of other means of access, such as vehicles or cranes, or ladders or other tools that could readily be used to defeat the barrier.

In assessing the adequacy of any physical barrier, it is generally good practice to consider its contribution to an integrated security system designed to provide defense in depth through effective detection, assessment, and response to a security event without delay. The licensee is responsible for ensuring that any barrier will perform as designed to enable the security zone as a system to meet the performance objective of isolating the material and allowing access only through established access control points under § 37.47(c)(1). The licensee may also want to consider whether a barrier could delay intruders sufficiently to contribute to the overall security program's ability to meet its performance objective of detecting, assessing, and responding to an actual or attempted unauthorized access "without delay" under § 37.41(b).

Q12: How do I meet Part 37 requirements for controlling unescorted access to a temporary security zone if I'm at a temporary job site that doesn't have physical barriers or special equipment, such as lockable doors?

A12: A licensee could meet the requirements for a temporary security zone simply by keeping the area under "direct supervision" by authorized personnel.

§ 37.47 Security zones (cont'd)

§ 37.47(d)

For category 1 quantities of radioactive material during periods of maintenance, source receipt, preparation for shipment, installation, or source removal or exchange, the licensee shall, at a minimum, provide sufficient individuals approved for unescorted access to maintain continuous surveillance of sources in temporary security zones and in any security zone in which physical barriers or intrusion detection systems have been disabled to allow such activities.

EXPLANATION:

Licensees must provide sufficient individuals approved for unescorted access to maintain continuous surveillance of category 1 quantity sources when physical barriers or intrusion detection systems have been disabled.

QUESTIONS/ANSWERS:

Q1: When are special additional measures for category 1 quantities of radioactive material required?

A1: During equipment maintenance or source receipt, installation, replacement, or preparation for shipping, tamper-indicating devices and other intrusion detection equipment typically must be disabled to permit the device to be opened without tripping alarms. After replacement, the removed sources must be prepared onsite for shipment back to the manufacturer or for storage and eventual disposal. These non-routine operations during a time when devices for detecting theft or diversion are disabled require additional measures to compensate for the temporary increase in vulnerability.

Q2: Does the approved individual who must perform the continuous surveillance of the source replacement or maintenance work have to remain on duty for the duration of the work?

A2: No. An approved individual must perform the continuous surveillance but need not be the same individual for the duration of the work. If the original approved individual observing the work must be relieved, the second observer must begin surveillance before the original observer departs.

§ 37.47 Security zones (cont'd)

§ 37.47(e)

Individuals not approved for unescorted access to category 1 or category 2 quantities of radioactive material must be escorted by an approved individual when in a security zone.

EXPLANATION:

Individuals not approved for unescorted access must be escorted by an approved individual when in a security zone.

QUESTIONS/ANSWERS:

Q1: What is an escort's responsibility?

A1: The objective of escorting is to maintain effective control of access to protected radioactive material, including access by unapproved individuals who require access to a security zone to perform their duties. The escort must maintain continuous surveillance of the escorted individual(s) and carry out assigned responsibilities for detection, assessment, and response as required. The purpose of the escort is to ensure that escorted individuals perform their duties as intended and do not misuse their access to the protected radioactive materials. Procedures for escorts should be tailored to each facility's operations. Licensees should consider limiting the number of people assigned to an escort so as to avoid degrading the escort's effectiveness in completing other assigned safety and security responsibilities.

Q2: Do licensees have to visually distinguish (e.g., with badges) all individuals who have not been granted unescorted access?

A2: No. This is not a requirement, but licensees should consider methods for distinguishing individuals approved for unescorted access from those requiring escort. For example, those approved for unescorted access to category 2 or greater quantities of radioactive material could wear colored badges or other identifying articles. Colored badges or identification cards may be appropriate for a larger organization, while simple face recognition may be appropriate in a smaller one. The ability to visually distinguish approved individuals from those who require escort is considered a best security practice, although there may be other ways to distinguish these individuals, such as by electronically coded badges. In any case, the method used to distinguish individuals requiring escort should help facility personnel in early detection and timely assessment of unauthorized access incidents.

Q3: Can we assume that patients can be granted unescorted access during treatments?

A3: No. Patients who are being treated with devices containing category 1 or category 2 quantities of radioactive material must be escorted. The escort does not need to be physically with the patient in the treatment room but can observe from outside the room. Access to loaded teletherapy devices by patients who are receiving treatment

with these devices should be restricted during treatment, and the licensee must comply with Part 37 requirements. Patients should not be permitted access to areas where radioactive material is stored without being escorted by approved individuals.

Q4: Must an escort always maintain line-of-sight surveillance of an unapproved individual in a security zone?

A4: No. The escort must, however, maintain “direct continuous visual surveillance,” which may be conducted using video surveillance in some but not all cases. . For example, video surveillance of patients during a treatment is appropriate, but video surveillance where the “escort” is in another building would not.

Q5: Must the escort always be physically present when an individual who is not approved for unescorted access is in the security zone?

A5: Generally, yes, although an escort may monitor an unapproved individual remotely (using a closed circuit TV system or a window into the room, for example) as long as the escort maintains continuous visual surveillance over the individual at all times. There are some circumstances, such as when a patient undergoes teletherapy, for which remote surveillance might be preferable to actual physical accompaniment of an unapproved individual.

Q6: How can a single individual, such as a medical technologist assigned to be an escort, maintain “direct control” of the security zone sufficiently to prevent an incident or even raise an alarm in the event that someone is armed and intent upon gaining access to radioactive material?

A6 There is no absolutely assured way to prevent a determined, well-conceived, and well-equipped effort to gain unauthorized access to radioactive material. The purpose of the escort is to identify, assess and respond if possible to unauthorized activities by a visitor or another individual who has not been granted unescorted access. The escort should also observe behavior that may suggest an interest in defeating the security system. For example, the escort should notice if the visitor shows an unusual interest in the system, equipment, and procedures used to protect the security zone.

§ 37.49 Monitoring, detection, and assessment

§ 37.49(a) *Monitoring and detection.*

§ 37.49(a)(1)

Licensees shall establish and maintain the capability to continuously monitor and detect without delay all unauthorized entries into its security zones. Licensees shall provide the means to maintain continuous monitoring and detection capability in the event of a loss of the primary power source, or provide for an alarm and response in the event of a loss of this capability to continuously monitor and detect unauthorized entries.

EXPLANATION:

Licensees must continuously monitor and detect without delay all unauthorized entries into security zones. Continuous monitoring and detection capability must be maintained whenever the primary power source is lost, or the licensee must provide for an alarm and response when the capability to continuously monitor and detect unauthorized entries is lost.

QUESTIONS/ANSWERS:

Q1: Is there a need to provide security monitoring for locations other than windows, doors, and access ways?

A1: Yes. The detection system must be capable of detecting *all* unauthorized access to the security zone, including breaches of barriers used to isolate and control access to the protected radioactive material. This may require security monitoring beyond that installed on windows, doors, and access ways.

Q2: If a licensee opts to provide an alarm system for a loss of the primary power source for monitoring and detection systems, must the system be calibrated to alarm for power surges, brownouts, or other anomalies in the electricity supply system? What would constitute a “loss” of the primary power source? What other sources of information can I use for monitoring and detection methods and equipment?

A2: An alarm system for a power source impairment should be calibrated to trip for power surges, brownouts, and other anomalies that would cause a loss of the monitoring or detection system’s functionality. A licensee should consider a “loss” of its primary power source to be any anomaly that impairs the ability of a monitoring or detection system to perform as expected. If the licensee chooses instead to use an alternate or auxiliary power source, such as a gasoline-fueled generator, the alternate power source should be set to power the monitoring and detection system automatically.

Q3: What other sources of information can I use for monitoring and detection methods and equipment?

A3: For additional technical information on the capabilities and applications of different backup power intrusion detection technologies, you may refer to [NUREG-1959](#),

Intrusion Detection Systems and Subsystems. For technical information on the capabilities and applications of various access control systems you may refer to [NUREG-1964](#), *Access Control Systems*.

§ 37.49 Monitoring, detection, and assessment (cont'd)

§ 37.49(a)(2)

Monitoring and detection must be performed by:

§ 37.49(a)(2)(i)

A monitored intrusion detection system that is linked to an onsite or offsite central monitoring facility; or

§ 37.49(a)(2)(ii)

Electronic devices for intrusion detection alarms that will alert nearby facility personnel; or

§ 37.49(a)(2)(iii)

A monitored video surveillance system;

§ 37.49(a)(2)(iv)

Direct visual surveillance by approved individuals located within the security zone; or

§ 37.49(a)(2)(v).

Direct visual surveillance by a licensee designated individual located outside the security zone.

EXPLANATION:

Monitoring and detection must be performed by: a monitored intrusion detection system linked to a central monitoring facility; electronic intrusion detection alarms that will alert nearby facility personnel; a monitored video surveillance system; or direct visual surveillance.

QUESTIONS/ANSWERS:

Q1: Would implementation of an area monitor connected to a silent alarm, key-card access to the area, and a video monitoring system be adequate for meeting Part 37 requirements?

A1: The regulation was designed to allow licensees flexibility to choose methods that work best in each licensee's specific circumstances. Therefore, the adequacy of a system will depend on the system's capabilities and site-specific requirements. It is the licensee's responsibility to choose monitoring and detection methods and technologies for effective compliance with the requirements of this section. Effective detection and monitoring can be accomplished in different ways tailored to different facility-specific operating conditions. The licensee's choices must also ensure that there are dependable means in place to transmit information between and among the various components used to detect and identify an unauthorized intrusion, to inform the licensee security staff, and to summon the appropriate responder.

Q2: May I use a less sensitive monitoring system during the routine workday? May I rely on visual inspection by approved individuals during the normal workday, and a system depending on an off-site monitoring facility at night?

A2: Detection and monitoring requirements can be met using electronic devices, visual monitoring, or a combination of these methods. The chosen method(s) must, however, be effective in providing the required capability of immediate detection, assessment, and response. Personnel must be trustworthy and reliable, trained in appropriate security procedures, equipped for reliable communications, and capable of meeting the immediate detection requirements. Electronic devices must be capable of alerting trained on-site or off-site facility personnel upon first detection of an intrusion. Visual monitoring must also be capable of alerting trained assessment and response personnel without delay. For additional technical guidance on the capabilities and applications of different intrusion detection system technologies, you may refer to [NUREG-1959](#), *Intrusion Detection Systems and Subsystems*.

Q3: If a licensee uses electronic intrusion detection alarms, what minimum performance should these devices be capable of?

A3: To meet the requirements of § 37.49(a)(2)(ii), a licensee must use intrusion detection alarms that will alert nearby facility personnel of unauthorized access to the security zone. These alarms may be visual, like strobe lights, for example, but if you rely on audible alarms to fulfill this function, their sound should be distinguishable from other alarms and should be at least 65 decibels above ambient background noise level at the farthest location of a responder. (See, e.g., Department of Energy (DOE) [M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests](#), p. 55.) If you decide to use magnetic switches on doors and windows as part of an intrusion alarm system, the NRC considers it a best practice to use balanced magnetic switches, which are more difficult for an adversary to defeat. If you use motion detectors, you must use enough detectors to cover all potential entrance and egress points for radioactive material from the security zone. To meet the intent of § 37.49(a), the detection system must be capable of detecting *all* unauthorized access to the security zone, including breaches of barriers used to isolate and control access to the protected radioactive material.

The licensee's security plan should explain how any method used to alert facility personnel will be reliable and effective in permitting immediate detection on a continuous basis. For additional technical guidance on the capabilities and applications of different intrusion detection system technologies, you may refer to [NUREG-1959](#), *Intrusion Detection Systems and Subsystems*.

Q4: May I use silent alarms, as some experts recommend, for duress situations?

A4: You may use silent alarms to meet the requirement in § 37.49(a)(2)(i) for a monitored intrusion detection system linked to an on-site or off-site central monitoring facility. You may deploy silent alarms in the immediate vicinity of the security zone in addition to the intrusion detection alarms to respond to situations where anyone threatens or assaults another approved individual once inside the security zone. Silent alarms for such duress situations can give responders the advantage of surprise and provide an additional increment of time to assess and more effectively intervene. If the licensee does choose silent alarms, however, to comply with § 37.49(a)(2)(ii) they must be continuously monitored by direct visual surveillance or a monitored video or audio surveillance system connected to a central monitoring station.

Q5: May I use radiation safety monitoring and detection systems for material security purposes?

A5: Yes, if their use does not adversely affect radiation safety. To comply with this Part, you may use any monitored motion detection systems or alarms used to control access to high radiation areas, for example, or other alerting systems used for radiation protection. These systems may also be modified, but only if the modifications do not compromise the equipment's original safety purpose. An integrated motion detection and alarm system originally installed at one location for radiation safety purposes, for example, should not be relocated to serve a security zone if the relocation would diminish the system's sensitivity at its original location. Radiation detection alarms would generally not enable you to detect intrusions as required by § 37.49(a)(2)(ii), but these alarms may be used to comply with the requirement in § 37.49(a)(3) to detect unauthorized removal of radioactive material from a security zone. Your security plan should describe how any radiation safety systems used for security purposes will provide the required intrusion or removal detection without impairing these systems' performance or functionality for radiation protection.

§ 37.49 Monitoring, detection, and assessment (cont'd)

§ 37.49(a)(3)

A licensee subject to this subpart shall also have a means to detect unauthorized removal of the radioactive material from the security zone. This detection capability must provide:

§ 37.49(a)(3)(i)

For category 1 quantities of radioactive material, immediate detection of any attempted unauthorized removal of the radioactive material from the security zone. Such immediate detection capability must be provided by:

§ 37.49(a)(3)(i)(A)

Electronic sensors linked to an alarm; or

§ 37.49(a)(3)(i)(B)

Continuous monitored video surveillance; or

§ 37.49(a)(3)(i)(C)

Direct visual surveillance.

§ 37.49(a)(3)(ii)

For category 2 quantities of radioactive material, weekly verification through physical checks, tamper indicating devices, use, or other means to ensure that the radioactive material is present.

EXPLANATION:

Licensees with category 1 quantities of material must provide immediate detection capability through electronic sensors linked to an alarm, continuous monitored video surveillance, or direct visual surveillance. Licensees with category 2 quantities must ensure that the material is present through use, tamper indicating devices, physical checks, or other means

QUESTIONS/ANSWERS:

Q1: What does NRC mean by the requirement in § 37.49(a)(3)(i) that my detection capability be “immediate?”

A1: The common dictionary meaning of “immediately” is “at once, instantly, without any intervening time.” Thus, your detection system must be capable of alerting you of any attempted unauthorized removal of radioactive material from the security zone instantly, without delay.

Q2: To meet the additional requirement of § 37.49(a)(3)(i) for immediate detection of an attempted removal of a category 1 quantity of material from a security zone, can a licensee rely only on its main site-wide intrusion detection system linked to a monitoring facility?

A2: No. This requirement is in addition to the requirement to detect, assess, and respond to unauthorized access to the security zone. Methods that the licensee may

use to meet the requirement to detect removal include, but are not limited, to the following:

- Alarming electronic tamper indicating device;
- Radiation detectors that will alarm when material is removed from a security zone; or
- Continuous visual surveillance by an approved individual.

If a licensee uses electronic tamper indicating alarms, the alarm should be capable of alarming either when an attempt is made to remove a category 1 quantity of radioactive material from a device, or when an attempt is made to remove the device itself. The tamper indicating alarms should be armed at all times, except during periods of maintenance.

If a licensee decides to use alarms that will alert nearby facility personnel to unauthorized access to the security zone, the audible alarm should be distinguishable from other alarms and should be at least 65 decibels above ambient background noise level at the farthest location of a responder. (See, e.g., DOE [M 5632.1C-1](#), p. 55.)

The licensee's security plan should explain how any method used to detect unauthorized removal will be reliable and effective in providing immediate detection on a continuous basis.

Q3: Would licensees with continuous staffing on-site 24 hours a day, 7 days a week still be required to implement Part 37 requirements for immediate detection of a removal?

A3: Licensees will still be required to implement Part 37 requirements, but may be able to take credit for 24/7 staffing to meet some of these requirements. Having staff that can identify anyone without a clear work-related duty to be near a protected device, and immediately call for assistance when needed, can be considered as part of the licensee's response to unauthorized removal of radioactive material.

Q4: May I use approved individuals to monitor for unauthorized removals of category 1 material if these individuals are moving about constantly and may not always be watching the area under access controls?

A4: You may use any of a number of methods to detect an unauthorized removal, but the method you select must meet the Part 37 requirements to respond immediately to any actual or attempted theft, sabotage, or diversion of protected radioactive material. Thus, if you rely on approved individuals to detect removal immediately as required by § 37.49(a)(3)(i), at least one individual must be observing at all times, unless another approved individual is escorting an unapproved individual in the affected security zone. No one method of monitoring may be right for all licensees, however.

Q5: Would periodic checking by a trained security guard meet the requirement for "immediate detection" of an actual or attempted removal of a category 1 quantity? Why would 15 minutes not permit an adequate response to an alarm?

A5: As noted earlier, “immediate” is commonly defined as “instant,” or “without delay.” While trained individuals can be used to monitor and immediately detect, assess, and respond as required, periodic checks, even those at intervals shorter than 15-minutes, will not meet the immediate detection requirement. Immediate detection is essential to reduce the risk that an adversary will be able to remove the material even if he is able to gain unauthorized access to it. Immediate detection is also essential to enhance the likelihood of recovering the material before it can be misused, or to mitigate the consequences of misuse even if the adversary is able to remove it from its authorized location.

Q6: Is there any way to monitor without an alarm system?

A6: Trained individuals may be used to fulfill some requirements of Part 37, but to comply with the requirement of § 37.49(a)(1) to “maintain the capability to continuously monitor and detect without delay all unauthorized entries into ... security zones,” a licensee must maintain this capability 24 hours a day, 7 days a week. An appropriate method of monitoring, detection, and assessment should also provide a dependable means to transmit information between the various components used to detect an unauthorized intrusion, inform security staff, and summon the appropriate responder. An integrated alarm system may be the most cost-effective method to provide such continuous compliance.

Q7: Can a partial exemption from § 37.49 be granted to licensees at extremely remote locations, such as off-shore and wilderness sites, where access is limited and communication difficult?

A7: Any licensee may request an exemption from any NRC requirement, but a licensee seeking an exemption from immediate detection requirements solely on the basis of remoteness would need to address the potential security risks of such relief. Remoteness may allow an intruder to gain undetected and unauthorized access more readily than in more populated environments. An additional lag in communications about an unauthorized removal may also provide advantages to an intruder’s planning to steal or sabotage material. Licensees must therefore meet all applicable Part 37 requirements unless the NRC approves an exemption request.

If a licensee does request an exemption from a Part 37 requirement because of remoteness or the difficulty of timely communication, the licensee must justify the request and should propose compensatory measures to mitigate the consequences of not meeting the specified requirement. Exemption requests will be evaluated on a case-by-case basis. See Q&As for § 37.11

Q8: Could radiation detection equipment connected to a silent alarm be used to alert local law enforcement of an attempted theft of radioactive material?

A8: Yes. Depending on the configuration of shielding surrounding the radioactive source and other factors, radiation meters could be a means to detect and alert an LLEA of an attempted theft of radioactive material. A licensee would be prudent, however, to avoid overreliance on any single method for detecting an unauthorized removal of radioactive material. Part 37 requirements were designed to provide a defense-in-depth strategy, and the NRC expects licensees to consider all credible scenarios when

developing and implementing a security program to implement the requirements of Part 37.

Q9: If a licensee with a category 2 quantity of radioactive material does not use the material weekly or make weekly physical checks to verify its continuing presence, what “other means” may this licensee use to detect the removal of a category 2 quantity of radioactive material under § 37.49(a)(3)(ii)?

A9: The provision for “other means” to detect removal of a category 2 quantity of material is intended to give the licensee flexibility to use the method that works best for its facility. Although electronic sensors for detecting removal of a category 2 quantity of material are not required, it is a good practice to consider the application of these devices to category 2 quantities where feasible for immediate detection capability. For additional technical guidance on the capabilities and applications of different intrusion detection system technologies, you may refer to [NUREG-1959](#), *Intrusion Detection Systems and Subsystems*.

If a licensee decides to use an electronic tamper-indicating device for detecting removal, the NRC recommends that the system be designed to alarm, silently or audibly, on any attempt to remove a device, or a source from its device. The tamper-indicating alarm should be armed at all times other than those for equipment maintenance or calibration. The licensee’s security plan should also explain how any method used to detect the unauthorized removal of a category 2 quantity of material will be reliable and effective in meeting the requirements of § 37.49(a)(3).

§ 37.49 Monitoring, detection, and assessment (cont'd)

§ 37.49(b)

Assessment. Licensees shall immediately assess each actual or attempted unauthorized entry into the security zone to determine whether the unauthorized access was an actual or attempted theft, sabotage, or diversion.

EXPLANATION:

A licensee must assess each actual or attempted unauthorized entry into a security zone immediately to determine whether there was an actual or attempted theft, sabotage, or diversion.

QUESTIONS/ANSWERS:

Q1: Can a licensee use automated devices to assess an intrusion and alert an LLEA?

A1: Yes, if the licensee is able to meet the requirements of Part 37 using these devices. Assessment may be done by either automated devices or trained personnel who can initiate the appropriate response, but in either case, the assessment must enable the licensee to request assistance and begin any other mitigating measures immediately. Depending on the security system, the layout of security zones, and the design capabilities of the sensors, automated devices or systems may be programmed to summon LLEA assistance automatically in response to an intrusion alarm. The security plan and implementing procedures must describe how the licensee would assess and respond to unauthorized access. In developing its plan and procedures, the licensee should consider the possibility of simultaneous alarms at multiple locations.

Q2: Can licensees perform their own vulnerability assessment and change Part 37 time requirements for detection and response?

A2: Licensees are welcome to conduct vulnerability assessments as a good practice, but may not change the rule's time requirements for detection and response unilaterally. Part 37 requires licensees to detect, assess, and respond to any unauthorized access to the security zone "without delay," and the LLEA must be notified as soon as possible. If for some reason a licensee cannot comply with a specific requirement, or believes the requirement to be counterproductive, the licensee should inform the NRC and request an exemption. The exemption request should propose compensatory measures to mitigate the consequences of not meeting the specified requirement.

Q3: Must I summon LLEA assistance in response to *any* intrusion alarm?

A3: No. You are required to assess the situation immediately to determine whether the alarm signals an actual or attempted intrusion and decide whether the intrusion justifies LLEA involvement. In certain instances, however, you may determine in advance that an alarm from an electronic tamper-indicating device calls for an automatic summons to the LLEA, but it would be good practice not to summon an LLEA for every unauthorized intrusion. Such intrusions could be either unknowing or inadvertent, and it would be counterproductive to request LLEA assistance automatically for such

insignificant security events as an inadvertent activation of an alarm. Frequent alerts to your LLEA(s) are likely to result in a delayed or inadequate response to a real security incident.

§ 37.49 Monitoring, detection, and assessment (cont'd)

§ 37.49(c)

Personnel communications and data transmission. For personnel and automated or electronic systems supporting the licensee's monitoring, detection, and assessment systems, licensees shall:

§ 37.49(c)(1)

Maintain continuous capability for personnel communication and electronic data transmission and processing among site security systems; and

§ 37.49(c)(2)

Provide an alternative communication capability for personnel, and an alternative data transmission and processing capability, in the event of a loss of the primary means of communication or data transmission and processing. Alternative communications and data transmission systems may not be subject to the same failure modes as the primary systems.

EXPLANATION:

Licensees must maintain continuous capability for personnel communication and electronic data transmission and processing among site security systems. Licensees must also provide alternative personnel communication and data transmission and processing capabilities in case the primary means is lost. Alternative systems may not have the same failure modes as primary systems.

QUESTIONS/ANSWERS:

Q1: What do I have to do to "maintain continuous capability" under § 37.49(c)(1)??

A1: You must have a dependable means to transmit information to all the various components involved in the detection and assessment of an intrusion, including the appropriate responder, 24 hours a day, 7 days a week, 365 days a year. Land line phones, auto dialers, cellular phones, pagers, radios, and other similar modes of communication may be used to fulfill this requirement. When using more than one person for detection and assessment, the licensee must also provide a means for the various monitoring personnel to communicate with each other.

Q2: What personnel communications and data transmission systems are subject to the requirement for an alternative capability?

A2: You are required to have alternative capability for any primary system of communication or data transmission and processing you rely on to meet requirements. The alternative means must be able to provide continuous communication or data transmission capability. Land line phones, auto dialers, cellular phones, pagers, radios, and other similar modes of communication could be used to fulfill this requirement, so long as they are not subject to the same failure mode as the primary systems they would be required to replace. A radio or cellular phone, for example, could be considered as a backup to a land line phone. An alternative cell phone system, however, may not rely on the same cell tower and transmission system as the primary cell phone system.

Q3: To comply with the requirement that the alternative communication system not be subject to the same failure mode, may a licensee use a different cell phone service as a backup to a primary cell phone service?

A3: Yes, but the licensee will need to show that the alternative cell phone service does not use the same satellite communications system, signal processing, or receiving tower as the primary service.

§ 37.49 Monitoring, detection, and assessment (cont'd)

§ 37.49(d)

Response. Licensees shall immediately respond to any actual or attempted unauthorized access to the security zones, or actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material at licensee facilities or temporary job sites. 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's response shall include requesting, without delay, an armed response from the LLEA.

EXPLANATION:

Licensees must respond immediately to any actual or attempted theft, sabotage, or diversion of category 1 or category 2 material or unauthorized access to the security zones at licensee facilities or temporary job sites. The licensee must request an armed LLEA response without delay.

QUESTIONS/ANSWERS:

Q1: What do I need to do if I detect an intrusion into a security zone?

A1: Your response would depend on your assessment of the purpose of the intrusion, but a response is required without delay. If you assess the intrusion to be an actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material, you must notify and request an armed response from the appropriate LLEA immediately, followed soon after by a call to the NRC Operations Center at (301) 816-5100. An immediate response by the licensee would permit a more timely response from law enforcement, thereby reducing the consequences of the incident.

Your decision to call the LLEA and NRC would depend not only on your assessment of the intent of the unauthorized access, but also on whether the area where the breach occurred is an area you had previously determined needed to be monitored in order to meet NRC physical protection requirements. Thus, your assessment and response to an intrusion alarm in the business office section of your facility could be entirely different from your assessment and response to an intrusion alarm in a radioactive material storage area if the two areas are not adjacent.

Q2: Could radiation detection meters connected to a silent alarm be used to alert local law enforcement of an attempted theft of radioactive material?

A2: Yes, radiation meters could be used as part of a system to alert an affected LLEA of an actual or attempted theft of radioactive material, if this method is acceptable to the LLEA. The rule is designed to provide a defense-in-depth strategy for radioactive material security, and the NRC expects licensees to consider other measures for requesting LLEA assistance if they would also be necessary.

Q3: Since licensed facilities are also broken into to obtain equipment items other than radioactive materials, would coordination require licensees to summon the LLEA every time there is a break-in?

A3: No. The licensee's decision about whether to call the LLEA would depend on what areas the licensee determines need to be controlled for access to the radioactive material, and the licensee's assessment of the intent of the unauthorized access. A licensee's assessment and response to an intrusion alarm in a conference room or office supply storage area could be entirely different from its assessment and response to an intrusion alarm in a security zone for a radioactive materials storage area.

Q4: Do I have to conduct response exercises with my LLEA?

A4: No. Exercising the response portion of your security plan is a good practice, but it is not required. Some LLEAs may not be willing or able to participate, and the NRC also recognizes that requiring all licensees to exercise their response plans may not be cost-effective for small licensees with less complex security plans. However, licensees' security programs may benefit from exercising their response plans with their affected LLEA(s).

§ 37.51 Maintenance and testing

§ 37.51(a)

Each licensee subject to this subpart shall 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, are capable of performing their intended function when needed. The equipment relied on to meet the security requirements of this part must be inspected and tested for operability and performance at the manufacturer's suggested frequency. If there is no suggested manufacturer's suggested frequency, the testing must be performed at least annually, not to exceed 12 months.

EXPLANATION:

A licensee must implement a maintenance and testing program to ensure that intrusion alarms, associated communication systems, and other physical components of their detection systems remain operable and can perform their intended function when needed. Inspection and testing must be performed at the manufacturer's suggested frequency, or at least annually if there is no suggested frequency.

QUESTIONS/ANSWERS:

Q1: What minimum measures should a licensee implement for a maintenance and testing program?

A1: A licensee should:

- Identify all alarms, communication systems, and other physical components necessary to secure radioactive materials or 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) to be conducted on each component, and the minimum quantitative or qualitative results of the test(s) required for the component to be found operable and capable of performing its intended function;
- Identify the testing equipment to be used and any device-specific procedures for using or maintaining this equipment;
- Identify the measures the licensee 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 for detecting unauthorized access; and

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

Q2: Do I have to inspect and test my facility's security systems every month or every quarter-year to meet this requirement?

A2: No. Under § 37.51(a), inspection and testing for operability and performance needs to be conducted at the manufacturer's suggested frequency. If there is no suggested frequency, the testing must be performed at least annually, not to exceed 12 months. But the operability and performance of some components, such as personnel and data communications systems, may be confirmed by regular daily or weekly use.

Q3: Must I test and maintain every intrusion detection system or other security system on my facility site? If I determine that a detection or security device is unnecessary to meet Part 37 requirements, but still keep it energized, must I keep testing and maintaining it?

A3: No. You're required to test and maintain only those components you rely on to meet the security requirements of this Part for category 2 or greater quantities of radioactive material. Because you are also required under § 37.49(c)(2) to provide alternative communication capabilities for personnel and data transmission and processing in the event of a loss of the primary capability, you must also test and maintain the systems for these alternative communication capabilities.

Q4: What's the difference between maintaining a system or component in operable condition and ensuring that it is capable of performing its intended function when needed? Would licensees have to administer different tests for performance than for operability?

A4: The need for different tests would depend on the intended function of the system or component, and whether that function of the system or component could be fulfilled if the system or component were only in operable condition. A locking deadbolt on a door isolating radioactive materials, for example, would generally not need to be subject to any additional testing so long as it could be locked and unlocked when needed. An intrusion alarm, however, might be considered "in operable condition" if it can be turned on and made to produce an audible sound, but it would not necessarily be "capable of performing its intended function" if it could not reliably detect the movement of an intruder with sufficient sensitivity at a given distance, or could not produce a sound of sufficient volume to be audible at the nearest work area equipped to assess and respond.

Q5: What kinds of tests for intrusion alarms would be acceptable for demonstrating compliance?

A5: You should refer to the manufacturer's recommended testing protocol, if one is available, for each system or piece of equipment subject to testing and maintenance under § 37.51. For additional guidance on intrusion detection system testing and maintenance, you may also refer to Chapters 8.6 and 8.7 of [NUREG-1959, Intrusion Detection Systems and Subsystems](#). This NUREG also covers testing and maintenance for backup power sources in Chapters 9.4 and 9.5.

Q6: What should a licensee consider to be an “associated communication system” subject to testing and maintenance? Would a closed circuit television monitoring system be considered a communication system, even if it’s intended primarily for the timely detection of an intrusion?

A6: NRC considers a communications system to be “associated” if it fulfills any function essential for the operability or performance of the security or detection system as a whole, not just for the performance of intrusion alarms. For the purposes of this section, the NRC considers a “communication system” to be any device or network of devices used to transmit voice, video, data, or other information from a person or machine at one location to a recipient person or machine at another. This could include such things as a land-line phone, a walkie-talkie system, or a cell phone. A closed-circuit television monitoring system could also be considered a communication system within the meaning of this definition even if the system also performs monitoring or detection functions. An alarm system that incorporates motion-sensing devices could also be considered a communications system even if it also performs monitoring and detection functions. In either case, however, the testing and maintenance requirements of this section would apply, because § 37.51 applies both to systems for securing radioactive materials and systems for detecting unauthorized access to these materials. Any system designed to perform multiple functions would be subject to this section as long as one of the system’s functions supported either security or detection. For this example, the lines or cabling that allows transmission of the data from the closed-circuit television (CCTV) cameras to the recipient monitoring station comprise the associated communication system. Such data lines or cabling is also subject to testing and maintenance.

Q7: Specifically, what “other physical components of the system” used for securing or monitoring access to radioactive material would be subject to the requirements for testing and maintenance? Aren’t all “components” of these systems inherently “physical?”

A7: To enable licensees to identify physical components of security systems other than alarms and communications systems, the NRC is using the word “physical” to distinguish tangible material components, such as architectural structures and equipment, from system “components” comprised of human beings and their actions, including the plans and procedures that govern those actions. Thus, for a system that secures category 1 or category 2 quantities of radioactive material from unauthorized access within a security zone under §37.47(c)(1), any other component should be considered an “other physical component” if it meets both of the following two criteria:

- It is not otherwise integrated into an alarm or communications system, nor an employee or contractor performing security-related work at the licensee’s site; and
- Its intended function supports the isolation of these radioactive materials by the use of continuous physical barriers that allow access only through established access control points.

Examples of “other physical components” of security systems may thus include walls, doors, remotely-operated doors, ceilings, floors, windows, storage containers, shielding,

scales, mounting bolts, fasteners, key card systems, locks, keys if applicable, emergency alternate power generators, and lighting.

Correspondingly, a component of a system for maintaining the capability to continuously monitor and detect without delay all unauthorized entries into its security zones under §37.49(a)(1) should be considered an “other physical component” if it meets both of the following two criteria:

- It is not otherwise integrated into an alarm or communications system, nor an employee or contractor performing security-related work at the licensee’s site; and
- Its intended function supports the continuous monitoring and immediate detection of all unauthorized entries into the licensee’s security zone(s).

Examples of “other physical components” of detection systems may include video surveillance cameras and monitors, night-vision devices, motion sensors for self-illuminating floodlights, and tamper-indicating devices not otherwise integrated into an alarm or communication system. If a licensee opts to provide an alarm system for a loss of the primary power source for monitoring and detection systems, that system is also an example of an “other physical component” subject to testing and maintenance. If the licensee chooses instead to use an alternate or auxiliary power source, such as a gasoline-fueled generator, that alternate power source would also be subject to testing and maintenance. See Q&A 2 for § 37.49(a)(1) above.

The NRC recognizes that not all physical barriers will need to be “tested” in the sense of the term commonly understood to involve a rigorous, documented administration of specified evaluation procedures under controlled and often non-routine conditions. The purpose of testing in this regulatory context is to confirm that the subject system component is operable and capable of performing its intended function when needed. There are a number of ways to obtain this confirmation, and not all require the quantitative methods often associated with instrumentation and testing protocols. The operability of some physical barriers, such as keys, key cards, doors, walls, windows, two-way mirrors, and floors, are regularly and satisfactorily confirmed in the course of routine operations. The NRC recognizes that the performance capability of many physical barrier system components, such as tamper-indicating devices and jersey barriers, may not be tested for performance as a security barrier without risking or resulting in a degradation of their performance. Other barriers, such as the locked entrance to a panoramic irradiator, serve a safety function for which testing could complicate the ALARA principle of radiation safety. In these cases, NRC does not expect a licensee to conduct testing for a physical barrier’s performance if the test itself could compromise either radiation safety or the future performance of the component or system.

Q8: Will testing and maintenance have to be performed by approved individuals meeting the access authorization requirements of Subpart B?

A8: No. However, individuals not approved for unescorted access will need to be escorted when performing maintenance or testing activities within a security zone.

Q9: Will testing equipment need to be secured within a security zone?

A9: No. If the testing equipment is susceptible to tampering by an insider, keeping this equipment within the security zone could be a practicable way for some licensees to control unauthorized access to this equipment, but NRC recognizes that, for space, operational, and other considerations, storage of security-sensitive testing equipment inside a security zone may not be feasible. In such cases, the licensee should consider other ways to control access to this equipment, such as a locker with a key pad, controlled key, key card, or combination lock.

Q10: What do I have to do to have an acceptable testing and maintenance program for my intrusion detection system (IDS)?

A10: Under § 37.51(a), your program must cover the testing and maintenance of all IDSs you rely on to detect unauthorized access to radioactive material. The program must ensure that these systems and components are maintained in operable condition and capable of performing their intended function when needed. To maintain functionality, you must periodically test the IDS and perform maintenance on malfunctioning components. The testing program is considered acceptable if the IDS operates in a manner consistent with your physical security plan. You are required to test the entire IDS or components of the IDS at the frequency specified by the manufacturer or at least annually. You may choose to test the entire IDS or components of the IDS throughout the 12 months of the testing cycle.

§ 37.51 Maintenance and testing (cont'd)

§ 37.51(b)

The licensee shall maintain records on the maintenance and testing activities for 3 years.

EXPLANATION:

Maintenance and testing records must be kept for 3 years.

QUESTIONS/ANSWERS:

Q1: What kinds of records of maintenance and testing activities should a licensee maintain?

A1: For each maintenance activity, a record should identify:

- The name(s) of the person(s) who performed the maintenance;
- The date the maintenance was performed;
- The component(s) or system(s) on which the maintenance was performed;
- The purpose of the maintenance, identifying as appropriate the deficiencies in operability or performance; and
- 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 name(s) of the person(s) who performed the testing;
- The date of the testing;
- The component(s) or system(s) tested;
- The purpose of the testing;
- The performance expected to fulfill the component's or system's intended function;
- The results of the testing; and
- Any maintenance activities needed to remove any deficiency in the operability or performance of the component or system.

§ 37.53 Requirements for mobile devices.

§ 37.53

Each licensee that possesses mobile devices containing category 1 or category 2 quantities of radioactive material must:

§ 37.53(a)

Have two independent physical controls that form tangible barriers to secure the material from unauthorized removal when the device is not under direct control and constant surveillance by the licensee; and

EXPLANATION:

Mobile devices containing category 1 or category 2 quantities of radioactive material must have two independent tangible barriers to secure the material when the device is not under direct control and constant surveillance.

QUESTIONS/ANSWERS:

Q1: What is the performance objective of the requirement for two independent physical controls against the unauthorized removal of radioactive material when it's not under direct control and constant surveillance?

A1: Because they can often be easily concealed and transported, mobile devices are particularly vulnerable to attempted theft or diversion. A mobile device could even be removed before the licensee has an opportunity to respond to an intrusion. The objective of this requirement, therefore, is to delay an attempt to steal the device by making it harder to steal. Achieving this objective would provide additional time for the licensee to detect, assess, and respond to an attempt, by notifying an LLEA if necessary.

Q2: What does NRC mean by "independent" physical controls?

A2: For purposes of compliance with this requirement, an "independent" physical control does not rely on any other system to deter or delay unauthorized removal of the radioactive material when the mobile device containing it is not under the licensee's direct control and constant surveillance. Such a physical control must provide a barrier against unauthorized removal regardless of whether any other barrier or system is disabled.

Examples of two independent physical controls for category 1 or category 2 quantities of radioactive material in a mobile device at a licensed facility would be:

- Storage of the device inside a locked storage shed within a secured outdoor area, such as a fenced parking area with a locked gate; or
- Storage of the device in a room with a locked door within a secured building for which access is controlled by a separate lock and key or by a security guard; or

- Storage of the device inside a locked, non-portable cabinet inside a room with a locked door if the building is not secured.

When securing the radioactive material in or on a transportation vehicle, examples of two independent physical controls would be:

- Storage of the mobile device in a container physically attached to a vehicle, with the container secured by two separate chains or steel cables, each of which is locked and separately attached to the vehicle in such a manner that the container cannot be opened without the removal of both of the chains or cables; or
- Storage of the device in a container inside a locked trunk, camper shell, van, or other similar enclosure, with the container physically secured to the vehicle by a locked chain or steel cable in such a manner that the container could not be opened and the mobile device removed without both breaking into the enclosure on the vehicle and removing the chain or cable.

At a temporary job site or a location other than a licensed facility or licensee's vehicle, examples of two independent physical controls would be:

- Storage of the mobile device inside a locked building in a locked non-portable structure with the device physically secured by a locked chain or steel cable to the non-portable structure in such a manner that the device could not be removed without removing the chain or cable. (A construction trailer, sea container, or parked and locked truck should not be considered a non-portable structure, however. See Q&As below, and those for the definition of "mobile device" in [§ 37.5](#).)
- Storage of the device in a locked garage within a locked vehicle, or physically secured by a locked chain or steel cable to a disabled vehicle in such a manner that the device could not be removed without removing the chain or cable.

For large mobile devices on wheels that are used inside a facility, additional delay may be accomplished by a variety of other independent physical controls, including:

- Speed bumps too large for the device to traverse on the facility floor;
- Elevated doorway thresholds;
- Protective storage enclosures;
- Channels in a floor large enough to catch the device's wheels;
- Fixed or retractable bollards;
- Wheel locks, including steering wheel locks (made of hardened material) that require a key or special tool to release; or
- A hardened chain and lock that cannot be easily cut.

These additional physical controls for security purposes should not, however, compromise safety. If improperly implemented, some of the suggested controls, such as elevated door thresholds and channels in a floor, may compromise occupational safety, and a licensee intending to use such controls should address these issues.

Q3: Does this section require two physical barriers *in addition* to the physical barrier required for the security zone, or does a barrier for a security zone count as one of the two required barriers?

A3: A barrier for a security zone may count as one of the two required barriers if it is independent of the other barrier and has not been defeated (e.g., for lock replacement or the servicing of a key card device). Although the two barriers may be of the same type, such as a locked room within a locked room, the barriers have different purposes in order to contribute to defense-in-depth security. The tangible barriers required by § 37.53 are to secure the material from unauthorized *removal* when the device is not under the licensee's direct control and constant surveillance. The security zones required by § 37.47 are to control unescorted access, and licensees may accomplish this by using continuous physical barriers that allow access to a security zone only through established access control points. A physical barrier for a security zone could both control access to radioactive material and secure it from unauthorized removal, but it must serve both purposes simultaneously and may not rely on any other measures, such as remote monitoring of the security zone entrance, to fulfill both functions

Q4: If mobile devices are stored in one room, does that mean the licensee has an aggregated quantity of radioactive materials?

A4: The regulation provides that radioactive materials are to be considered aggregated if:

- Their total quantity at a single location equals or exceeds a category 2 quantity using the sum-of-the-fractions method. See Q&As on the definition of "aggregated" in § 37.5; and
- If breaching a common physical security barrier (e.g., a locked door at the entrance to a storage room) would allow access to the radioactive material or devices containing the radioactive material. See Q&As on physical barriers in § 37.47.

Thus, for example, if several mobile devices, each below the category 2 quantity threshold, were stored in one room without any physical barriers between them, they would be considered aggregated if their combined activity equaled or exceeded the category 2 threshold.

Q5: If I have a category 1 or 2 quantity of radioactive material in a container that isn't mounted on wheels or casters and can't be carried by hand, and I secure it in a pickup truck bed or on a trailer, would NRC consider this source or device "mobile?"

A5: Yes, because the device would be “mounted on wheels” (i.e., the truck/trailer wheels) and “equipped for moving without a need for disassembly or dismounting” under the definition of “mobile device.” A container or device on a pickup truck bed or on a trailer would also subject the truck or tractor to the requirement of § 37.53(b) for disabling the vehicle when not under direct control and constant surveillance by the licensee. See Q&As on § 37.53(b).

Q6: If I have a radiography camera or other mobile device with a category 1 or 2 quantity of radioactive material, under what conditions would that device meet the exclusion for “stationary equipment installed in a fixed location” under the definition of “mobile device?”

A6: Under this definition, the device would need to be welded, bolted, or otherwise affixed to an immovable piece of equipment, such as an assembly line, in a manner that would require additional equipment to be disassembled or dismounted before the device could be moved. The device could also be excluded as “stationary equipment installed in a fixed location” if it were chained or cabled to a stationary piece of equipment and secured with a lock, but the licensee would need to control access to the combination, key, password, or other means of unlocking the lock.

§ 37.53 Requirements for mobile devices. (cont'd)

§ 37.53(b)

For devices in or on a vehicle or trailer, unless the health and safety requirements for a site prohibit the disabling of the vehicle, the licensee shall utilize a method to disable the vehicle or trailer when not under direct control and constant surveillance by the licensee. Licensees shall not rely on the removal of an ignition key to meet this requirement.

EXPLANATION:

Unless health and safety requirements for a site prohibit disabling of vehicles, they must be disabled when not under direct control and constant surveillance. Licensees may not rely on removing an ignition key to meet this requirement.

QUESTIONS/ANSWERS:

Q1: What are acceptable methods to disable a vehicle or trailer when it is not under direct control and constant surveillance by the licensee?

A1: The objective of the vehicle disabling requirement is to delay unauthorized removal of a device by stealing the vehicle it is secured to. Examples of acceptable vehicle disabling methods would include: trailer hitch locks, wheel locks ("boots"), or methods to disable the vehicle's engine.

Removing a standard key from a vehicle's ignition cannot be considered sufficient for disabling a vehicle's engine because there are means to start a vehicle without the key, such as using a duplicated key, or hot-wiring techniques. There are currently many advances in ignition and key technology that may provide for additional barriers that would cause delay in accessing the radioactive material. An example is a key implanted with an electronic chip that is only recognizable to the computer programmed in the vehicle. Only this key, and not a duplicated key, would be able to start the vehicle. A licensee with this key system may request an exemption from 37.53(b) for that specific vehicle, but would need to address the possibility of hot-wiring or other techniques to defeat the system. A similar disabling function may also be provided by biometric recognition systems when they become commercially available. Such technologies, allowing operation of a vehicle only by a means that is not easily defeated, would be considered an appropriate means to disable a vehicle. Deflating the tires should not by itself be relied upon as an effective immobilization technique, however, because an adversary could too easily re-inflate them with an air pump or pressurized gas cartridge.

Q2: When a device in or on a vehicle is not under the licensee's direct control and constant surveillance, this paragraph requires the licensee to disable the vehicle "unless health and safety requirements at a site "prohibit" such disabling. What kind of health and safety requirements at a site would NRC deem to "prohibit" vehicle disabling?

A2: The facility or site requirements or procedures would need to specify that vehicles cannot be disabled or need to remain accessible for immediate relocation in an

emergency. Disabling of a vehicle or trailer will not be required at any site where a known or reasonably foreseeable operational hazard, such as an explosion, fire, or release of a toxic substance, could require an individual to operate the vehicle immediately, either to escape or mitigate the hazard.

Q3: Does the requirement to secure mobile devices mean that all trucks will need an alarm system when they carry a device containing a category 1 or category 2 quantity of radioactive material?

A3: No, but if the truck is left unattended, the licensee must have a way to monitor and immediately detect, assess, and respond to an actual or attempted theft, sabotage, or diversion. An alarm system is an acceptable method.

Q4: Can 1/8 inch wire cables be used to secure a radiography camera instead of chains? Is the lock then more of a vulnerability than the cable?

A4: Yes, a heavy-duty twisted steel wire cable may be used instead of a chain to secure mobile devices. Ideally the wire should be thick enough that it can only be removed with a heavy duty cable cutter (i.e., thickness greater than a No. 10 wire - 1/8 inch or 2 mm).

Any system is only as effective as its weakest component, however, and other components of the securing mechanism, including the lock, will need to have similar strength such that it too would require a heavy duty bolt cutter for removal (typically, tensile force: 2,000 lbf and shackle cutting force test: 4,000 lbf). [Regulatory Guide 5.12](#) "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials" may provide some useful information. Other references include: [NUREG/CR-5929, Locking Systems for Physical Protection and Control](#); [NUREG-0274, Part 5, Catalog of Physical Protection Equipment, book 2, Volume III, Entry Control Components](#); [Army Regulation 190-11, Physical Security of Arms, Ammunition and Explosives](#); and DOE [M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests](#).

Q5: Can two or more barriers with separate locks that share the same key or lock combination qualify as "two independent physical controls" as stipulated in the requirement for securing mobile devices?

A5: Yes; two or more barriers with separate locks that share the same key or lock combination could qualify as "two independent physical controls." Whether separate locks use the same or different keys or combinations is an aspect of the licensee's access control program, and does not determine whether two barriers can be considered as "two independent physical controls." Regardless of the number of keys or combinations used, the most important test for ensuring that there are two independent physical controls is that each barrier is separate from the other and neither relies on the other to perform its intended function. The same guidance applies when considering barriers for purposes of determining whether material is aggregated.

An important aspect of a licensee's physical protection program is controlling access at the licensee's facility. If a key-based system is used, it is essential that the licensee distribute the keys only to personnel who have been granted unescorted access and have a need for access in order to perform their assigned duties. It is important to

ensure that those who are part of a licensee's physical protection program understand the importance of their roles and responsibilities for controlling access, especially if these individuals control combinations or keys that secure material.

§ 37.55 Security program review.

§ 37.55(a)

Each licensee shall be responsible for the continuing effectiveness of the security program. Each licensee shall ensure that the security program is reviewed to confirm compliance with the requirements of this subpart and that comprehensive actions are taken to correct any noncompliance that is identified. The review must include the radioactive material security program content and implementation. Each licensee shall periodically (at least annually) review the security program content and implementation.

§ 37.55(b)

The results of the review, along with any recommendations, must be documented. Each review report must identify conditions that are adverse to the proper performance of the security program, the cause of the condition(s), and, when appropriate, recommend corrective actions, and corrective actions taken. The licensee shall review the findings and take any additional corrective actions necessary to preclude repetition of the condition, including reassessment of the deficient areas where indicated.

§ 37.55(c)

The licensee shall maintain the review documentation for 3 years.

EXPLANATION:

Each licensee must review its security program's content and implementation at least annually. Each review report must identify adverse conditions and the causes of each condition. When appropriate, the report must recommend corrective actions and review corrective actions taken. The licensee must review the report's findings and take any additional corrective actions and reassessments necessary to preclude recurrence of the adverse condition(s).

QUESTIONS/ANSWERS:

Q 1: How should a licensee evaluate the "effectiveness" of its security program to comply with NRC requirements for program reviews?

A1: A licensee should consider several things when evaluating the continuing effectiveness of its security program. Specifically, it should consider its ability to confirm compliance with all the applicable requirements of this subpart and to take comprehensive and effective actions to correct identified non-compliances. Most importantly, however, the licensee should keep in mind that continuing effectiveness is not a static condition. Continuing improvements are an essential part of an effective program. To minimize the potential for false negatives, the licensee's program reviews must address each applicable requirement of this Part. These reviews should identify adverse conditions, non-compliances, and root causes, and provide recommended corrective actions. The licensee should follow up on the implementation of these actions and reassess their impacts. The hallmark of an effective program is not, therefore, the

absence of recorded adverse conditions or non-compliances. It is the documented evidence that the licensee has made diligent efforts to find problems and is continuing to reassess the effectiveness of its actions to prevent them from reoccurring.

Q2: What does NRC mean by its requirement to review the security program content and implementation “at least annually?”

A2: Recognizing that some demands on licensees’ time and resources are beyond their control, the NRC will consider you to be conducting a program review “at least annually” if you conduct it each year at about the same time of year. You will comply if you review your program at regular intervals not to exceed 12 months.

Q3: Must a licensee engage an outside contractor to conduct security program reviews?

A3: No. Although hiring an independent party to conduct security program reviews would be one way for licensees to demonstrate compliance, the regulation does not require it. To the extent possible, however, the licensee should try to avoid the situation where the implementers of the program and their supervisors are reviewing their own work. If the licensee has a large enough staff, the licensee could establish a review team of approved individuals led by an individual, such as the reviewing official for access authorization decisions, who works outside the management chain of the licensee’s security staff. If the licensee conducts activities with category 1 or category 2 quantities of radioactive material at more than one location with a different security staff at each location, it could have the review team at one location review the program implemented by the staff of a different facility.

Q4: Does a licensee need to report to NRC any noncompliance identified during a security program review?

A4: No, but in accordance with the regulation, the licensee must “ensure ... that comprehensive actions are taken to correct any noncompliance that is identified” by the review. The licensee is also required to document the corrective actions taken and “take any additional corrective actions ... to preclude repetition of the condition.” This documentation must be made available for NRC inspection.

Q5: What would NRC consider a “condition adverse to the proper performance of the security program?”

A5: NRC would consider as an adverse condition any occurrence or continuing state that degrades, or if not corrected, could degrade, the ability of the physical security system to detect or respond to an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material without delay. An example of an adverse condition might be a breach in a physical barrier, a missing or misdirected motion detector, or a door that fails to latch and lock itself when closed. An adequate program review should never be limited to looking only for existing or imminent noncompliances. It should assess or reassess all conditions that may call into question the continuing effectiveness of the licensee’s security program.

Q6: The regulation requires the report resulting from a program review to recommend corrective actions “when appropriate.” When should a licensee recommend corrective actions?

A6: The rule does not specify particular conditions for which corrective action is required, but it would be prudent practice for a program review report to recommend at least one corrective action for each noncompliance or “condition adverse to the proper performance of the security program” identified as a result of the review.

Q7: What should a licensee consider as “review documentation” for the purposes of this subsection?

A7: The licensee should retain the approved final version of its annual review report and any attachments or enclosures related to that report. Related records should include the membership and leadership of the review team if applicable, a description of the management approval process for the annual report if applicable, root cause analyses for identified non-compliances or adverse conditions, recommended corrective actions, evaluations of the effectiveness of past corrective actions, and other documents that were considered in the review. Review documentation should also include minority views on issues in the report on which there has been significant professional disagreement. NRC does not expect a licensee to retain meeting records, the notes of each member of a review team, or rough drafts of its annual security program reviews.

Q8: This section introduces the term “radioactive material security program.” Is there a difference between this term and the term “security program” for the purposes of this section?

A8: No. Both refer to the security program required by Part 37.

§ 37.57 Reporting of events

§ 37.57(a)

The licensee shall immediately notify the LLEA after determining that an unauthorized entry resulted in an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. As soon as possible after initiating a response, but not at the expense of causing delay or interfering with the LLEA response to the event, the licensee shall notify the NRC Operations Center ((301) 816-5100). In no case shall the notification to the NRC be later than 4 hours after the discovery of any attempted or actual theft, sabotage, or diversion.

EXPLANATION:

A licensee must notify the LLEA immediately after determining that an unauthorized entry resulted in an actual or attempted theft, sabotage, or diversion of radioactive material. The licensee must also notify the NRC Operations Center as soon as possible (no later than 4 hours after discovery), but not at the expense of causing delay or interfering with the LLEA response to the event,

QUESTIONS/ANSWERS:

Q1: The regulation requires a licensee to notify the LLEA immediately after initiating “an appropriate response” to an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. What kind of response by the licensee would NRC consider “appropriate?” Under what circumstances, if any, would an armed licensee response before the arrival of the LLEA be considered appropriate?

A1: As soon as the licensee has determined that an actual or attempted theft, sabotage, or diversion is in progress, an appropriate licensee response pending the arrival of LLEA assistance would depend on the licensee’s assessment of the intruder’s intent and ability to carry out theft, sabotage, or diversion. A single unarmed individual who has only made an unauthorized entry at the perimeter of a security zone may call for a different response than the intrusion of several armed individuals who had removed or were about to remove a category 1 or category 2 quantity of radioactive material. The appropriateness of the licensee’s response should also consider the applicability of the licensee’s written procedures to the actual circumstances. These procedures could, for example, require the licensee to consider the proximity of the intrusion to the target material, the quantity of material at risk of sabotage or unauthorized removal, the quality and quantity of any remaining physical barriers to the removal of the material or escape of the intruders, and whether the physical barriers are likely to delay the intruders sufficiently for the anticipated arrival of the LLEA.

The regulation does not require a licensee’s security staff to be armed for its response to be deemed appropriate. A decision to arm a facility’s security personnel is solely up to the licensee and would depend on applicable State laws.

Q2: The regulation requires the licensee to notify the NRC Operations Center “as soon as possible” after initiating a response, “but not at the expense of causing delay or interfering with the LLEA response to the event ... [and] [i]n no case ... later than 4

hours after [its] discovery.” What would NRC consider to be causes of delay or interferences with the LLEA’s response sufficient to justify a licensee decision to postpone notifying the NRC?

A2: Any justification for postponing a notification to the NRC would depend on the circumstances of the event. Perhaps the most compelling justification would be a situation requiring a licensee to devote all available resources to restoring its facility to a safe condition or protecting individuals from actual or threatened physical harm, as in the case of a fire or explosion, or an armed hostage-taking. An ongoing attempt to steal the material or use it for sabotage could also require the licensee to assist the LLEA before or after its arrival. A similar necessity for the licensee’s assistance could be the threat of a bomb hidden somewhere on the facility site. Under such circumstances, the responding licensee staff could be justified in postponing notification of the NRC until the LLEA had determined that the licensee’s assistance in the response is no longer required. If, however, an employee of the licensee outside of its on-site security staff became aware of the emergency and was not immediately needed to help the security staff respond to the event, NRC would expect that employee to notify his or her management, and the licensee to notify the NRC, as soon as possible. The same would be true if the licensee discovered an apparent theft of a category 1 or category 2 quantity of radioactive material after the fact; the NRC would expect the licensee to notify it immediately after notifying the LLEA and initiating measures to ascertain whether the missing material was still on the premises.

The NRC can envision none but the most extreme and unusual circumstances to justify delaying a notification more than 4 hours after the discovery of any attempted or actual theft, sabotage, or diversion, however.

Q3: To avoid an NRC notice of violation after the event, would I have to obtain confirmation from the LLEA that a delay in the licensee’s notification of the NRC was necessary to avoid delaying or interfering with the LLEA’s response?

A3: No, although you’re not prohibited from seeking the LLEA’s endorsement of your decision to delay NRC notification. The NRC would take the LLEA’s judgment into account, but the NRC’s determination of compliance or noncompliance with this notification requirement would rest principally on an assessment of the specific facts and circumstances of the situation, not the LLEA’s judgment.

Q4: Should notification to the LLEA be made by a radiographer at a temporary job site if a device is stolen from the temporary job site?

A4: Yes. The licensee should contact the LLEA that can provide the most prompt and effective response. (See also Q&As for §§ 37.45(d) and 37.49(d).)

Q5: When I determine that an actual or attempted theft, sabotage, or diversion of radioactive materials has begun, what information must I report to what organization (NRC or LLEA)?

A5: In the event of any actual or attempted theft, sabotage, or diversion of radioactive material protected under Part 37, you must notify the LLEA immediately, followed soon thereafter by a call to the NRC Operations Center at (301) 816-5100. Telephone calls to

notify the NRC should be as prompt as possible, but not at the expense of causing delay or interfering with the LLEA's response to the event.

Your notification to the LLEA should provide at minimum a basic who-what-when-where description of the event. To facilitate a timely and effective LLEA response, you should also answer any follow-on questions from the LLEA. These could request information on, for example: landmarks at the affected facility's location; an estimate of the kinds and quantities of radioactive material that could be affected, and how it is contained, such as whether it is in a stationary or a mobile device, or another type of container; the number of intruders believed to be involved and available information about their weaponry, equipment, and apparent objectives; the location(s) of the unauthorized activity within the facility, and the closest safe access point for incoming LLEA personnel; a description of the physical barrier system deployed to isolate the radioactive materials from unauthorized access; and a summary description of the licensee's other security measures and resources available to assist LLEA responders. Information regarding the licensee's physical protection of radioactive materials may be given to the LLEA without violating the information protection requirements of § 37.43(d).

Your notification to the NRC should provide at minimum a basic who-what-when-where description of the event. Depending on the NRC's need for additional information, you could also provide some of the information already provided to the LLEA. This could include, for example, the number of intruders believed to be involved and available information about their weaponry, equipment, and apparent objectives; a description of the physical barrier system deployed to isolate the radioactive materials from unauthorized access; and a summary description of the licensee's other security measures and resources available to assist responders.

For either kind of agency notification, however, you should consider the known and potential needs of the recipient agency for mission-related information, and address these issues if possible beforehand in your security plan and procedures. You should also consider that compliance with these notification requirements will not relieve you from making other reports as required by other State or local laws.

Q6: Since facilities are also broken into in order to obtain equipment or valuables other than radioactive materials, do licensees need to notify the LLEA and the NRC Operations Center every time there is a break-in?

A6: No. The regulation does not require a licensee to request LLEA assistance and notify NRC offices except in response to an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. Thus, the licensee's decision about whether to call the police and affected regulators would depend on an assessment of whether the detected break-in was intended assumed to perpetrate an unauthorized use of the radioactive material. This assessment of intent could in turn depend, among other things, on the proximity of the detected intrusion to any security zone the licensee has established to isolate the radioactive material from unauthorized access. A licensee's assessment and response to an intrusion alarm in an office supply stockroom could be entirely different from its assessment and response to an intrusion alarm in the radioactive materials storage area. The NRC would expect, however, that the licensee's security plan and procedures would address ways to distinguish an actual or attempted theft, sabotage, or diversion of the subject radioactive material from a break-in for other purposes. While you would probably still call the LLEA

for a break-in to the office area, you would not need to notify the NRC unless radioactive materials were involved.

Q7: If someone reports lost or missing category 1 or category 2 quantities of radioactive material, how would the NRC respond?

A7: If such an incident occurs, the NRC will expect the licensee to implement the appropriate elements of its security plan. The NRC will also monitor the situation to ensure that appropriate actions are being taken to locate and recover the missing material. As required by the National Response Framework, the NRC will notify and coordinate with other Federal Agencies as needed.

§ 37.57 Reporting of events (cont'd)

§ 37.57(b)

The licensee shall assess any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material and notify the LLEA as appropriate. As soon as possible but not later than 4 hours after notifying the LLEA, the licensee shall notify the NRC Operations Center ((301) 816-5100).

EXPLANATION:

A licensee must assess any suspicious activity related to possible theft, sabotage, or diversion of radioactive material, and notify the LLEA as appropriate. The licensee must also notify the NRC Operations Center as soon as possible, but not later than 4 hours after notifying the LLEA.

QUESTIONS/ANSWERS:

Q1: Why am I required to report suspicious activities to the NRC?

A1: The reporting of suspicious activities is important for evaluating the threat against licensed facilities and material. The NRC reviews individual notifications of suspicious activities to evaluate whether potential preoperational activities (i.e., multiple events at a single site or multiple events at multiple sites) may be part of a larger plan and to integrate this information with other agencies in the homeland security and intelligence communities. The NRC is not requesting that licensees actively gather intelligence but rather that they report information they believe is relevant to the security of their facility or activity. The reporting requirements provide a consistent means of communicating this information to the NRC.

Q2: Do I need to call the NRC after the LLEA for issues not related to my-licensed activities with radioactive materials?

A2: No, unless you conclude that such issues could affect the security or safety of your materials (e.g., if you discover an unauthorized weapon, drugs, or other contraband inside a controlled area). Both the regulations and guidance in this area are worded broadly to provide licensees flexibility.

Q3: Where can I find additional guidance on what NRC considers suspicious activities that should be reported?

A3: [Annex C](#) at the end of the Subpart C discussion provides examples of activities that could be considered suspicious activities, but these examples are not all-inclusive. Each licensee is responsible for developing and periodically reassessing its own criteria for identifying suspicious activities based on local conditions, recent events, and lessons learned by others. For this purpose, licensees may find useful the [Safeguard New York](#) publication of the New York State Division of Homeland Security and Emergency Services, which provides examples of suspicious activities and indicators for heightened surveillance. For a more exhaustive analysis, there is also a 2006 [University of](#)

[Arkansas study](#) funded by the National Institute of Justice, *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct*. There are numerous other sources available on and off the internet as well.

Q4: If I don't think an unusual activity is "suspicious" and don't report it, and it turns out to be related to a security incident, will I be in violation of this requirement?

A4: No. The NRC recognizes that judgments about what is "suspicious" are inherently subjective, often influenced by personal experience and community history. After an event, it should be more important to learn from it and take measures to prevent its reoccurrence than to assign individual blame. For this reason, it is critical that you report, even if after the fact, any unusual but seemingly nonthreatening activity that in retrospect is found to have been a precursor to an actual or attempted theft, sabotage, or diversion. The NRC, law enforcement agencies, and the intelligence community need this information to help identify the likely perpetrators of similar tactics in the future, and to integrate as much credible evidence as possible into a pattern that might indicate an ongoing adversary strategy. Prompt licensee reporting of suspicious activities also enables the NRC to alert other licensees to look for similar activities as possible early indicators of a pending attack.

Q5: What if one of my employees or contractors thinks *everything* is suspicious and frequently reports any non-routine activity as suspicious? How can I discourage over-reporting that could have the counterproductive effect of making my LLEA(s) *less* inclined to respond?

A5: You can develop criteria for identifying suspicious activities based on Appendix C and any other pertinent sources, including one or more of those cited above. You should incorporate these criteria into your site security procedures, make these procedures available to all facility staff and contractors, and require all observers of suspicious activities to refer to the procedures in after-action reports. Depending on the size of your workforce and the possibility of unwanted chilling effects on reporting, you can also require a first observer to report to the site security officer or his or her designee before reporting to the LLEA and NRC. It may also be useful to note that § 37.57(b) does not require reporting of all activities that might at first appear suspicious; the section requires reporting "as appropriate," which allows licensees to investigate before deciding whether the activity warrants reporting.

§ 37.57 Reporting of events (cont'd)

§ 37.57(c)

The initial telephonic notification required by paragraph (a) of this section must be followed within a period of 30 days by a written report submitted to the NRC by an appropriate method listed in § 37.7. The report must include sufficient information for NRC analysis and evaluation, including identification of any necessary corrective actions to prevent future instances.

EXPLANATION:

The licensee must submit a written report within 30 days for NRC analysis and evaluation. The report must identify any necessary corrective actions.

QUESTIONS/ANSWERS:

Q1: Other than identifying “any necessary corrective actions,” what, at a minimum, should a licensee’s written report on a security incident contain in order to provide “sufficient information for NRC analysis and evaluation?”

A1: The content and detail of the report would depend on a number of considerations, including: the nature and severity of the security incident; whether it was a first occurrence or a reoccurrence, and whether it has a significant potential to recur; the adequacy of the licensee’s monitoring efforts; the timeliness of the initial detection; the accuracy of the assessment; and the timeliness and potential effectiveness of the measures implemented in response to the incident. If the incident had occurred for the first time, the report should discuss whether it had been anticipated in the licensee’s security plan and procedures. In addition to an identification of corrective actions, the report should describe the data and analyses that supported the licensee’s identification of the root and significant contributing cause(s) of the incident, and how these data and analyses supported the licensee’s selection of corrective actions identified. If the incident was a recurrence of a similar incident, the report should briefly describe past corrective actions and the findings of past reassessments, and identify likely reasons that the past corrective actions have not prevented a recurrence of the condition. The report should then explain the basis for the licensee’s determination that the proposed new or revised corrective actions, or changes in the licensee’s implementation of these actions, are likely to prevent a recurrence of the condition or mitigate its effects.

Annex C

Examples of Reportable Suspicious Activities under § 37.57(b):

A licensee should not consider security events reported under § 37.57(b) as performance failures. Rather, the NRC considers timely and comprehensive communication of matters relating to threats, attacks, or suspicious activities a vital component of its efforts to assess the current threat environment. Since our adversaries have demonstrated the ability to attack multiple independent targets, timely reporting of nonthreatening but suspicious activities is important to the NRC, law enforcement agencies, and the intelligence community in order to integrate potential adversary plans, intentions, and suspicious event reports into a current threat assessment. Prompt reporting of actual or imminent hostile actions permits the NRC to execute its strategic missions of communicating to senior Federal officials and other licensees about hostile actions against the facilities and activities it regulates, thereby protecting public health and safety, the common defense and security, and the environment.

Following are examples of security-related events involving suspicious activity that may indicate preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees or their facilities. These events should be reported under § 37.57(b):

- Individual(s) with non-routine interests or inquiries related to security measures, personnel or vehicle entry points and access controls, or vehicle barrier systems, including fences, walls, or other barriers.
- Individual(s) conducting unapproved photographing or videotaping of licensed facilities.
- Suspicious attempts to recruit or compromise employees or staff, including contractors, knowledgeable of key personnel, facilities, or systems, into providing SGI-M or other sensitive physical security.
- Loitering for no apparent purpose in areas where intelligence could be gathered or preoperational reconnaissance could be performed.
- Suspicious behavior (e.g., fleeing, moving quickly away from licensee or certificate holder personnel, unexpected vehicular movement).
- Secretive sketching, making maps, or taking notes on the facility.
- Eliciting information from security or other site personnel regarding security systems or vulnerabilities.
- Unusual challenges to security systems that could represent attempts to gather information on system performance or personnel or equipment response actions.
- Unauthorized attempts to probe or gain access to the licensee's business secrets or other sensitive information or to control systems, including the use of social engineering techniques (e.g., impersonating authorized users).

- Theft or suspicious loss of official company identification documents, uniforms, or vehicles necessary for accessing plant facilities.
- Use of forged, stolen, or fabricated documents to support access control or authorization activities.
- Unusual attempts to obtain information or documents related to site security training, techniques, procedures, or practices.
- Discovery of Internet site postings that make violent threats related to specific licensed facilities or activities.
- Unusual threats or terrorist-related activities that become known to facility security or management involving the following: (1) unusual surveillance, probing or reconnaissance, (2) attempts to gain unauthorized access, (3) attempts to gain access to or acquire hazardous or dangerous materials, (4) unusual use of materials, or (5) financing to support terrorist activities.
- Stated threat(s) against the licensee's facility or staff, unless they are determined to be unsubstantiated.
- Unsubstantiated bomb or extortion threats that are considered to be related to harassment, including those representing tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations.
- Fires or explosions of suspicious or unknown origin.
- The unauthorized operation, manipulation, or tampering with radioactive material in quantities of concern or the unauthorized operation, manipulation, or tampering with security-related structures system and components that could prevent the implementation of the licensee's protective strategy.
- The intentional cutting of wires that does not affect the facility or security operations.
- The modification of security equipment that renders the equipment inoperable.
- The overt changing of equipment or control settings.

The NRC does not consider this list to be exclusive or exhaustive. Additionally, licensees should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of Part 37.

Subpart D – Physical Protection in Transit

37.71 Additional requirements for transfer of category 1 and category 2 quantities of radioactive material.

37.73 Applicability of physical protection of category 1 and category 2 quantities of radioactive material during transit.

37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material.

37.77 Advance notification of shipment of category 1 quantities of radioactive material.

37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment.

37.81 Reporting of events.

§ 37.71 Additional requirements for transfer of category 1 and category 2 quantities of radioactive material

A licensee transferring a category 1 or category 2 quantity of radioactive material to a licensee of the Commission or an Agreement State shall meet the license verification provisions listed below instead of those listed in § 30.41(d) of this chapter:

§ 37.71(a)

Any licensee transferring category 1 quantities of radioactive material to a licensee of the Commission or an Agreement State, prior to conducting such transfer, shall verify with the NRC's license verification system or the license issuing authority that the transferee's license authorizes the receipt of the type, form, and quantity of radioactive material to be transferred and that the licensee is authorized to receive radioactive material at the location requested for delivery. If the verification is conducted by contacting the license issuing authority, the transferor shall document the verification. For transfers within the same organization, the licensee does not need to verify the transfer.

§ 37.71(b)

Any licensee transferring category 2 quantities of radioactive material to a licensee of the Commission or an Agreement State, prior to conducting such transfer, shall verify with the NRC's license verification system or the license issuing authority that the transferee's license authorizes the receipt of the type, form, and quantity of radioactive material to be transferred. If the verification is conducted by contacting the license issuing authority, the transferor shall document the verification. For transfers within the same organization, the licensee does not need to verify the transfer.

§ 37.71(c)

In an emergency where the licensee cannot reach the license issuing authority and the license verification system is nonfunctional, the licensee may accept a written certification by the transferee that it is authorized by license to receive the type, form, and quantity of radioactive material to be transferred. The certification must include the license number, current revision number, issuing agency, expiration date, and for a category 1 shipment the authorized address. The licensee shall keep a copy of the certification. The certification must be confirmed by use of the NRC's license verification system or by contacting the license issuing authority by the end of the next business day.

§ 37.71(d)

The transferor shall keep a copy of the verification documentation as a record for 3 years.

EXPLANATION:

Before transferring category 1 or category 2 quantities of radioactive material, the shipping licensee must verify that the transferee's license is valid. This verification can be conducted using the NRC's license verification system or by contacting the agency (NRC or Agreement State) that issued the transferee's license. Verification documentation must be maintained for 3 years.

QUESTIONS/ANSWERS:

Q1: Is verification of the transferee's license necessary?

A1: Yes. Licensees are required by § 37.71 to verify that recipients of category 1 or category 2 quantities of radioactive material are licensed and authorized to receive them. Under § 37.71(a), the verification is required to occur before the radioactive material is actually transferred. Verification is not required for transfers within the same organization or company.

Q2: What information needs to be verified?

A2: Under § 37.71(a), the licensee must verify that the transferee's license authorizes receipt of the type, form, and quantity of radioactive material to be transferred. For transfers of category 1 quantities of radioactive material, the shipping licensee would also be required to verify that the receiving licensee is authorized to receive radioactive material at the address requested for delivery.

Q3: How does a licensee conduct the verification?

A3: These verifications would be conducted by using the NRC's license verification system (LVS), or if it is not available, by contacting the license issuing authority, i.e., the NRC or the appropriate Agreement State agency. Licensees should contact the appropriate NRC regional office to verify the validity of NRC licensees. Information on Agreement State contacts is provided on the NRC web page at

<http://nrc.stp.ornl.gov/asdirectory.html>. Use of LVS when it becomes available will be the preferred method for license verification.

Q4: May I use a fax or e-mail to verify the validity of a license, or just keep a copy of the recipient's license on file?

A4: No. Neither faxing or e-mailing provide the positive identification needed for verifying the validity of a license because an individual can alter an electronic image of the license to change its possession limits, authorized location of use, or even the name of the person who received the license. Keeping a copy of the recipient's license on file is also inadequate for verifying the validity of a license because the license could be amended or terminated and the licensee shipping the material would not know that the intended recipient's license was no longer valid. Licensees are required by § 37.71(a) either to use the LVS or contact the regulatory agency (NRC or Agreement State) to verify that a license is valid before shipping category 1 or category 2 quantities of radioactive material to a domestic company.

Q5: What is the License Verification System?

A5: The LVS is a new web-based NRC system designed to enable users to verify electronically the validity of a license issued by either NRC or an Agreement State. Use of the LVS is the preferred method for license verification. If the system is not available, licensees would need to contact the appropriate licensing agency. More information will be available once the system is fully developed and operational.

Q6: If the licensee is transferring the material to DOE or to an entity that does not have an NRC or Agreement State license (e.g., for exporting the material), does it still need to verify the transfer?

A6: No. The license verification requirement is only applicable if the licensee is transferring category 1 or category 2 quantities of radioactive material to a licensee of the NRC or an Agreement State. License verification is not required to transfer material to DOE or to any other federal entity that does not have an NRC or Agreement State license. Licensees exporting material, however, would need to meet the requirements in [10 CFR Part 110](#) for checking the documentation that the recipient has the necessary authorization under the laws and regulations of the importing country.

Q7: Why are there differences between the category 1 and category 2 verification requirements?

A7: Because category 1 quantities of radioactive material are considered to be of greater concern than category 2, the licensee transferring category 1 quantities is subjected by § 37.71(a) to the additional requirement of verifying that the receiving licensee is authorized to receive radioactive material at the address requested for delivery.

Q8: When should a licensee document the verification, and how should it be documented?

A8: The rule only requires documentation if the shipping licensee (the licensee sending the licensed material) conducts the verification by contacting the NRC or

Agreement State license issuing authority. If the licensee uses the LVS, the system will save the record and the licensee would not need to keep further documentation.

If contacting the license issuing authority, you should document the communication. If the contact was by phone, you should prepare a note to file that contains information on the transfer (company name, license number, and material being transferred and address for category 1 shipments), the date of the communication, and the name of the individual at the licensing agency. If the communication was conducted by e-mail or fax, a copy of the e-mail or fax from the licensing agency should be retained.

Q9: If I can't reach the regulatory agency or access the LVS to verify that the recipient of my shipment is licensed to receive and possess the material, do I have to postpone the shipment until I obtain the verification?

A9: No. The rule provides an alternative that allows licensees to ship in situations where the regulator can't be reached or the LVS is inaccessible. Under § 37.71(c), the shipping licensee may obtain a written certification from the receiving licensee noting that it is authorized to receive the requested radioactive material. The certification must include the license number, current revision number, issuing agency, expiration date, and, for a category 1 shipment, the authorized address. The shipping licensee must follow up with LVS or the license-issuing authority by the end of the next business day to confirm that the recipient's license is valid. A copy of the certification must be retained. The certification can be faxed or e-mailed and does not need to be received through the mail.

Q10: If I rely on the recipient licensee's certification to ship material under the provisions of § 37.71(c) for emergencies, what do I do if I discover that the recipient's license is not valid for the transfer after the shipment has been sent?

A10: First, you should contact the regulatory agency to determine if the recipient's license authorizes the shipment. If you used LVS, it is possible that information in the system had not yet been updated to reflect a license amendment. If the regulatory agency confirms that the recipient is not authorized to receive the material, you should discuss with the regulatory agency what should be done. Possible actions include contacting the carrier to determine if the shipment has been delivered. If it has not, you may be able to request that the carrier return the shipment. If the shipment has been delivered, you may need to notify the LLEA at the licensee's location and the NRC's Operation Center. Another possible action is for the recipient to request a license amendment that would authorize the radioactive material in question.

Q11: Do I need to verify a transfer if I am sending the material to another location within the company?

A11: No. For transfers within the same organization, you do not need to verify the transfer.

Q12: What should I do if I receive an unusual order?

A12: Part 37 does not require a shipping licensee to notify its regulatory agency of an unusual order, but it is a good practice to carefully review orders from unfamiliar entities, even if their licenses and possession limits can be verified. Similarly, also it is a good

practice to carefully review an order from a previous recipient licensee if the order appears unusual compared to previous shipments to that licensee with respect to the type, form, destination, and/or quantity of material to be shipped. Unusual orders raise heightened security concerns, including attempts to obtain radioactive materials, and shipping licensees should take appropriate precautions. These include contacting the receiving licensee and/or the governing regulatory authority.

Q13: Typical source or device manufacturer and distributor licensees (M&Ds) could ship 50 to 60 sources a day to user licensees in many different jurisdictions. An M&D could thus be making 50 or 60 calls a day – or more, if the M&D hasn't gotten an immediate response on its first call -- to get the regulatory authority's verification for each shipment. The same problem could arise for user licensees returning these sources or devices to the M&D; every single user licensee would have to call the appropriate Agreement State or NRC office to verify that the M&D is authorized to receive the sources. Is verification necessary for each shipment, even for returns to the M&D licensee?

A13: Yes, verification of each shipment is necessary. One of the recommended actions of the 2006 [Radiation Source Protection and Security Task Force Report](#) was that NRC consider imposing “additional measures to verify the validity of licenses, before transfer of risk-significant radioactive sources, on all licensees authorized to possess Category 1 and 2 quantities of radioactive material.” (See Action 4-1, p. xxvii, pp. 48-50.) The NRC agrees with the recommended action and maintains that verification of the intended recipient's license before transfer is important to enhance the security of the material by validating the licensee's legitimacy. Use of the LVS instead of calling the regulatory agency should significantly reduce the burden, and allow 100 percent validation of licenses before transfer of category 1 or category 2 quantities of radioactive material. The Radiation Source Protection and Security task Force is an interagency task force mandated by the EPA Act.

§ 37.73 Applicability of physical protection of category 1 and category 2 quantities of radioactive material during transit

§ 37.73(a)

For shipments of category 1 quantities of radioactive material, each shipping licensee shall comply with the requirements for physical protection contained in §§ 37.75(a) and (e); 37.77; 37.79(a)(1), (b)(1), and (c); and 37.81(a), (c), (e), (g) and (h).

§ 37.73(b)

For shipments of category 2 quantities of radioactive material, each shipping licensee shall comply with the requirements for physical protection contained in §§ 37.75(b) through (e); 37.79(a)(2), (a)(3), (b)(2), and (c); and 37.81(b), (d), (f), (g), and (h). For those shipments of category 2 quantities of radioactive material that meet the criteria of § 71.97(b) of this chapter, the shipping licensee shall also comply with the advance notification provisions of § 71.97 of this chapter.

§ 37.73(c)

The shipping licensee shall be responsible for meeting the requirements of this subpart unless the receiving licensee has agreed in writing to arrange for the in-transit physical protection required under this subpart.

§ 37.73(d)

Each licensee that imports or exports category 1 quantities of radioactive material shall comply with the requirements for physical protection contained in §§ 37.75(a)(2) and (e); 37.77; 37.79(a)(1), (b)(1), and (c); and 37.81(a), (c), (e), (g), and (h) during the domestic portion of the shipment.

§ 37.73(e)

Each licensee that imports or exports category 2 quantities of radioactive material shall comply with the requirements for physical protection during transit contained in §§ 37.79(a)(2), (a)(3), (b)(2), and (d); and 37.81(b), (d), (f), (g), and (h) during the domestic portion of the shipment.

EXPLANATION:

This section establishes which provisions apply for shipments of category 1 and category 2 quantities of radioactive material. The shipping licensee is responsible for meeting the requirements unless the receiving licensee agrees in writing to assume responsibility. For ease of reference, see the following table.

Applicability Table for Subpart D Requirements

	§37.75(a)	§37.75(a)(2)	§ 37.75(b)	§ 37.75(c)	§ 37.75(d)	§ 37.75(e)	§ 37.77	§ 37.79(a)(1)	§ 37.79(a)(2)	§ 37.79(a)(3)	§ 37.79(b)(1)	§ 37.79(b)(2)	§ 37.79(c)	§ 37.81(a)	§ 37.81(b)	§ 37.81(c)	§ 37.81(d)	§ 37.81(e)	§ 37.81(f)	§ 37.81(g)	§ 37.81(h)
Category 1 shipments	x	x				x	x	x			x		x	x		x		x		x	x
Category 2 shipments			x	x	x	x			x	x		x	x		x		x		x	x	x
Domestic portion of Category 1 imports/ exports		x				x	x	x			x		x	x		x		x		x	x
Domestic portion of Category 2 imports/ exports									x	x		x			x		x		x	x	x

* For shipments of category 2 quantities that meet the criteria of [10 CFR 71.97\(b\)](#), the shipping licensee must also comply with the advance notification provisions of § 71.97.

QUESTIONS/ANSWERS:

Q1: Would Subpart D requirements apply to a shipment of two or more packages if each package contains less than a category 2 quantity but that in aggregate equals or exceeds a category 2 quantity?

A1: Yes. Each NRC licensee is required to meet the requirements of Subpart D for any radioactive material quantity that meets or exceeds a category 2 quantity regardless of how many individual packages may be in the shipment. This question assumes that the material in the two or more individual packages aggregates to a category 2 quantity, and § 37.73(c) provides that “[f]or shipments of category 2 quantities of radioactive material, each shipping licensee shall comply” with the requirements of Subpart D referenced in this subsection. Because this provision applies to all shipments and does not refer to the number of packages in each shipment, a licensee cannot avoid meeting these requirements by partitioning the total shipping quantity into multiple packages on the same vehicle. An adversary, (including an insider), in control of the transport vehicle would have unauthorized access to the total quantity of radioactive material in the shipment.

Q2: Which licensee is responsible for meeting the requirements of Subpart D?

A2: Generally, the shipping licensee is responsible for meeting the requirements of Subpart D. The receiving licensee may, however, choose to agree in writing to arrange for the required in-transit physical protection measures. In that case, compliance with the physical protection requirements of this Subpart would be the responsibility of the licensee receiving the shipment.

Q3: During what portion of the shipment are the security requirements applicable for category 1 or category 2 quantities of imports?

A3: The category 1 and category 2 import requirements are applicable only from the point that the material enters the United States (i.e., the domestic portion of the shipment after the package clears Customs).

Q4: For material being exported, is the licensee required to follow the security requirements for the entire trip?

A4: No. The licensee is responsible only for following the security provisions for the domestic portion of the trip up to the time when the shipment comes under the jurisdiction of a U.S. Government agency (e.g., Federal Aviation Administration (FAA), or the DHS at a port, border crossing, or airport).

Q5: Do the security provisions for category 1 and category 2 quantities of radioactive material apply during the time when shipments are placed in interim storage at the shipping licensee’s facility awaiting pickup?

A5: Yes, the security provisions do apply. Licensees shipping category 1 or category 2 quantities should ensure that any interim storage is minimized, or when it cannot be avoided, that required security provisions are met.

Q6: Do the security provisions apply to transshipments?

A6: No. The security provisions of Subpart D do not apply to transshipments of category 1 or category 2 quantities of radioactive material. Transshipments are shipments that are originated by a foreign entity in one country, pass through the United States, and continue on to a recipient in another country.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material

§ 37.75(a)

Each licensee that plans to transport, or deliver to a carrier for transport, licensed material that is a category 1 quantity of radioactive material outside the confines of the licensee's facility or other place of use or storage shall:

§ 37.75(a)(1)

Preplan and coordinate shipment arrival and departure times with the receiving licensee;

§ 37.75(a)(2)

Preplan and coordinate shipment information with the governor or the governor's designee of any State through which the shipment will pass to:

§ 37.75(a)(2)(i)

Discuss the State's intention to provide law enforcement escorts; and

§ 37.75(a)(2)(ii)

Identify safe havens; and

§ 37.75(a)(3)

Document the preplanning and coordination activities.

EXPLANATION:

Each licensee that ships category 1 quantities of radioactive material must conduct preplanning and coordination activities with the receiving licensee and with each State that the shipment crosses.

QUESTIONS/ANSWERS:

Q1: What happens if a shipment has to be re-routed during transport because of bad weather or other developments that neither I nor my carrier can control? How can I be sure in advance of the states my category 1 shipment will pass through and that I'll need to coordinate with under this subsection?

A1: You can be reasonably sure about the alternative routes for a shipment because the carrier is subject to federal DOT [49 CFR 397.101](#) regulations on highway-route-controlled quantities (HRCQ) of radioactive materials. These regulations require carriers to minimize the shipment's time in transit and use a preferred route, which is defined as "an Interstate System highway" unless a State routing agency designates an alternative route.

To ensure your compliance with § 37.75(a) requirements for pre-planning and coordination with states through which the shipment will pass, a good practice would be to ensure that your shipment contract with the carrier clearly obligates the carrier to also comply with these requirements when an unusual event, such as a blizzard, requires a

rerouting of the shipment through a state other than those along the originally-planned route.

Q2: What type of documentation is required under § 37.75(a)(3)?

A2: Section 37.75(a)(3) requires licensees to document the preplanning and coordination activities required in § 37.75(a)(1) and (2) for shipments of category 1 quantities of radioactive materials. The shipping licensee should therefore document any phone conversations or e-mail communications it has with the receiving licensee, to include the names of the individuals participating in the call or e-mail communications, a general description of the shipment, and the departure and arrival times. The shipping licensee should also document any interactions with the governor's designee to include names of the individuals participating in the call or e-mail, route-affected states' decisions on escorts, safe havens identified, and any other information the licensee considers pertinent to document compliance with the requirements of this subsection.

Q3: What does the NRC consider to be a safe haven?

A3: A safe haven is defined as “[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 authorities.” For additional discussion of this definition, see pertinent Q&As under §37.5, *Definitions*.

Licensees should use the following criteria in identifying safe havens for shipments: close proximity to the route, i.e., readily available to the transport vehicle; security from local, State, or Federal assets is present or is accessible for timely response; the site is well lit, has adequate parking, and can be used for emergency repair or to wait for the LLEA response on a 24-hour a day basis; and additional telephone facilities are available should the communications system of the transport vehicle not function properly. Possible safe haven sites include: Federal sites having significant security assets, such as military base gates or guarded agency parking lots; secure company terminals; state weigh stations; state welcome stations or rest areas; scenic overlooks or visitors centers; truck stops with secure areas; and LLEA sites, including state police barracks.

Identifying safe havens is the licensee's responsibility. If a licensee is having difficulty identifying a safe haven, the licensee can contact the NRC, the appropriate Agreement State agency, or state or local law enforcement officials.

Q4: Must I have more than one safe haven for a category 1 quantity shipment? How many should I identify?

A4: The rule does not specify a minimum number of safe havens for any shipment, but the shipping licensee and carrier have an important interest in identifying available places to stop along the route where the transport vehicle could securely remain or safely wait for assistance.

Q5: How far apart should these safe havens be? Is there a minimum distance for which at least one safe haven is required?

A5: The rule does not specify a minimum distance between safe havens. The NRC recommends 50 miles, but recognizes that safe havens at that interval may not be available in some more remote areas. In most areas, however, commercial truck stops, service stations, state weigh stations, welcome stations, rest areas, and paved scenic overlooks or visitor parking for historic sites should provide ample alternatives to shipment pre-planners and coordinators.

Q6: Is there a list of approved safe havens I can refer to?

A6: No, but if a licensee is having difficulty identifying a safe haven, the licensee may contact the NRC, the appropriate Agreement State agency, or state or local law enforcement officials.

Q7: If a state imposes other transportation security requirements outside the scope of Part 37, do I have to meet those too?

A7: Yes. Unless those transportation security requirements are preempted by any U.S. Department of Transportation (DOT) requirement under Chapter 49 of the U.S. Code of Regulations, any State may apply additional requirements beyond those requirements required for Agreement State compatibility under Part 37 while the shipment is within the State's borders. Part 37 does not preempt other State requirements that may be applicable, such as state police escorts for radioactive material shipments. Licensees must comply with these State requirements as well as the requirements of NRC or the Agreement State agency with jurisdiction.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material (cont'd)

§ 37.75(b)

Each licensee that plans to transport, or deliver to a carrier for transport, licensed material that is a category 2 quantity of radioactive material outside the confines of the licensee's facility or other place of use or storage shall coordinate the shipment no-later-than arrival time and the expected shipment arrival with the receiving licensee. The licensee shall document the coordination activities.

EXPLANATION:

Licensees shipping category 2 quantities of radioactive material must coordinate the expected arrival time and the no-later-than arrival time with the receiving licensee.

QUESTIONS/ANSWERS:

Q1: If I'm a shipping licensee, how soon after I "plan to transport" must I coordinate with a receiving licensee?

A1: You may begin your coordination activities with the receiving licensee at any time after you've decided to ship the material, but under this subsection you must complete these activities before you begin transporting it or consign it to a carrier for transport. You need not begin coordinating with the receiving licensee as soon as you confirm an incoming order or decide to transfer the material.

Q2: What does it mean to "coordinate," and how much is enough?

A2: Under this subsection, you need only contact the receiving licensee and establish an expected arrival time and NLT arrival time for the shipment. This can be as simple as sending an e-mail stating that the shipment is expected to arrive via FedEx by noon, for example, on a specified date, and that the NLT arrival time is 6:00 p.m. on that day. Although this is the only kind of coordination required, you and the recipient licensee are free to negotiate any other understandings, such as times and methods of communication, contact information for the carrier, contact information for local law enforcement agencies through which the shipment will pass, or any other information you both agree would better enable both parties to anticipate and be prepared for sources of delay, or otherwise make the shipment as incident-free as possible. Coordination may be done by phone, fax, e-mail, or face-to-face meetings, although this activity and the agreements it produces will have to be documented as this subsection requires.

Q3: We have two facilities, and need to ship a category 2 quantity of radioactive material from one facility across town to the other. Do we still need to "coordinate" an estimated and a NLT arrival time, even though we're coordinating with ourselves?

A3: If your shipping and receiving facilities operate under different licenses and you're using a commercial carrier to transport the material, coordination is required, as it is in all cases involving different licensees. If your transferring and receiving facilities are

operating under the same license, and your company is providing its own transportation, coordination with the receiving facility is not required. You may want to consider some elements of coordination, however, such as having the shipping facility notify the destination facility of the shipment's departure and estimated arrival time, if your two facilities are separated by property or roads not under your control that you believe such coordination might be prudent.

Q4: We are part of a university, and plan to ship a category 2 quantity of radioactive material from one facility to another on the same campus. Do we still need to coordinate an estimated and NLT arrival time between the two on-site facilities? What if the two facilities operate under different licenses?

A4: Facilities on the same site operating under the same license do not need to coordinate, even if the facilities are not at contiguous locations, and even if the material has to cross or travel on a public road crossing the site. If the shipping and receiving facilities are different licensees, however, coordination of estimated and NLT arrival time is required, because possession of the material will be transferred from one licensee to another.

Q5: Does an industrial radiographer carrying a camera containing a category 2-quantity sealed source have to coordinate under this section to transport the source from a company site to a temporary job site or from one temporary job site to another?

A5: A licensed industrial radiographer is not subject to these coordination requirements for either kind of shipment, because the radiographer is required to maintain control of a mobile source at all times, and there is no transfer from one licensee to another, at the company site or either of the temporary job sites.

Q6: What is meant by NLT arrival time?

A6: As defined in § 37.5 of this rule, NLT arrival time means "the date and time that the shipping licensee and receiving licensee have established as the time at which an investigation will be initiated if the shipment has not arrived at the receiving facility." It is not the estimated arrival time; licensees do not have to begin investigating if the shipment doesn't arrive by the estimated arrival time. For a category 2 shipment, the no-later-than-arrival time may not be more than 6 hours after the estimated arrival time. The NLT date and time effectively requires verification that the shipment arrived within the expected timeframe. If the shipment hasn't arrived by the agreed-upon NLT arrival time, the shipping licensee must trace the location of the shipment and decide whether to report to affected law enforcement authorities an unusual occurrence that could lead to a theft or diversion of the material.

Q7: What types of records are required to document coordination activities?

A7: The last sentence of this subsection requires a licensee to "document the coordination activities" required to coordinate the shipment NLT arrival time and the expected shipment arrival with the receiving licensee. The shipping licensee should document any phone conversations or e-mail correspondence with the receiving licensee to include the names of the individuals participating in the calls or correspondence and the agreed-upon estimated arrival time and NLT arrival time. E-

mails may be printed or stored electronically. A copy of any fax and the confirmation information should also be maintained.

Q8: Am I allowed to use the NSTS as a method to fulfill the preplanning and coordination requirements of § 37.75(b)?

A8: No. Although the NSTS is used, among other things, to track transfers of radioactive materials subject to reporting under [10 CFR 20 Appendix E](#), the NSTS is not designed for the kind of detailed interactions needed for effective pre-shipment planning and coordination. The NSTS does not, for example, track estimated or NLT arrival times -- only the dates of estimated and actual arrivals -- and reporting is not required until after the transfer has been made. This deadline alone could make it useless for determining when and whether to begin tracing a missing shipment. In addition, the NSTS does not require reporting of shipments that include bulk material or consist of several category 3 quantities that add up to a category 2 quantity. Thus, the NSTS does not cover all shipments that are subject to Part 37 requirements.

Q9: I'm an NRC licensee shipping a category 2 quantity of material to an Agreement State licensee, and that State's regulatory agency hasn't yet adopted the new regulations required to implement Part 37. Section 37.75(c) requires the receiving Agreement State licensee to notify me if the shipment hasn't arrived by the NLT arrival time, and I'm required under § 37.79(c) to investigate "immediately" if the shipment has missed that deadline. But if the receiving licensee is operating under existing Agreement State regulations, it isn't required to notify me when a shipment misses its NLT arrival time. Will I be in violation of my NRC license if I don't start investigating by that time?

A9: This should not be an issue. The security orders issued by the NRC and the legally binding requirements issued by the Agreement States required licensees to confirm receipt of transferred radioactive material, and if the material is not received at the expected time of delivery, the recipient licensee must notify the originator and assist in any investigation. This notification would actually occur earlier than the notification required under Part 37.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material (cont'd)

§ 37.75(c)

Each licensee who receives a shipment of a category 2 quantity of radioactive material shall confirm receipt of the shipment with the originator. If the shipment has not arrived by the no-later-than arrival time, the receiving licensee shall notify the originator.

EXPLANATION:

The receiving licensee must confirm receipt of a shipment with the shipping licensee. The receiving licensee must also notify the shipping licensee if the shipment has not arrived by the NLT arrival time.

QUESTIONS/ANSWERS:

Q1: When must the receiving licensee confirm to the shipping licensee that the shipment has arrived?

A1: For a category 2 quantity, the receiving licensee should strive to notify the shipping licensee as soon as practicable after the shipment has arrived, but must report that it has not arrived by the agreed-upon NLT arrival time. Under the definition of no-later-than-arrival time in § 37.5, this interval may not be more than 6 hours after the estimated arrival time. If the shipment arrives on time, confirmation by the delivery service (e.g., Fed Ex, DHS, or UPS) may be acceptable if the shipping and receiving licensee have agreed to this method during their preplanning and coordination discussions,

Q2: How should the receiving licensee notify the shipping licensee?

A2: Part 37 does not specify a particular way for the receiving licensee to notify the shipping licensee. The receiving licensee may contact the shipping licensee by phone, e-mail or facsimile. The method of notification to be used should be decided by the licensees during their preplanning and coordination activities.

Q3: Am I allowed to use the NSTS as a method to fulfill the requirements of § 37.75(c) to confirm receipt of the category 2 shipment and notify the shipping licensee if the shipment has not arrived by its NLT arrival time?

A3: No. The use of NSTS will not meet the requirement in § 37.75(c) to notify that a shipment has been received and the requirement to report to NSTS. A report to the NSTS is a report to a system; it does not notify the shipping licensee that a source has been received.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material (cont'd)

§ 37.75(d)

Each licensee, who transports or plans to transport a shipment of a category 2 quantity of radioactive material, and determines that the shipment will arrive after the no-later-than arrival time provided pursuant to paragraph (b) of this section, shall promptly notify the receiving licensee of the new no-later-than arrival time.

EXPLANATION:

If a shipment is delayed, the shipping licensee must notify the receiving licensee promptly of any new NLT arrival time.

QUESTIONS/ANSWERS:

Q1: How “promptly” must a category 2 shipping licensee notify the receiving licensee if the NLT arrival time must be changed?

A1: The shipping licensee’s notification should be as soon as practicable to avert a needless alarm by the receiving licensee under § 37.75(c) when the shipment is not delivered by the originally-established NLT arrival time. More specifically, notification should be as soon as practicable after the driver or other authorized member of the transfer crew determines that the category 2 shipment in question cannot be safely expedited enough to arrive before the NLT arrival time. (The requirement for an NLT arrival time does not apply to shipments of category 1 quantities of radioactive material.)

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material (cont'd)

§ 37.75(e)

The licensee shall retain a copy of the documentation for preplanning and coordination and any revision thereof, as a record for 3 years.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

Q1: What kinds of preplanning and coordination documents must a licensee retain to satisfy this recordkeeping requirement?

A1: For shipments of category 1 quantities of radioactive materials, § 37.75(a)(3) requires licensees to document the preplanning and coordination activities required in § 37.75(a)(1) and (2). The shipping licensee should therefore document any phone conversations or e-mail communications it has with the receiving licensee, to include the names of the individuals participating in the call or e-mail communications, a general description of the shipment, and the departure and arrival times. The shipping licensee should also document any interactions with the governor's designee to include names of the individuals participating in the call or e-mail, route-affected states' decisions on escorts, safe havens identified, and any other information the licensee considers pertinent to document compliance with the requirements of this subsection. (See also Q&A 3 for § 37.75(a) above.)

To document preplanning and coordination activities for shipments of category 2 quantities of radioactive material, the shipping licensee need only retain records of the expected arrival time and NLT arrival time. The record should contain the company name receiving the shipment and general information as to the shipment. (See also Q&A 7 for § 37.75(b) above.)

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material

§ 37.77

As specified in paragraphs (a) and (b) of this section, each licensee shall provide advance notification to the NRC and the governor of a State, or the governor's designee, of the shipment of licensed material in a category 1 quantity, through or across the boundary of the State, before the transport, or delivery to a carrier for transport of the licensed material outside the confines of the licensee's facility or other place of use or storage.

EXPLANATION:

Licensees must provide advance notification to the NRC and the governor of any State (or the governor's designee) of a shipment of a category 1 quantity of licensed material that passes through or across the boundary of the State.

QUESTIONS/ANSWERS:

Q1: What constitutes an "advance notification" for the purposes of this requirement?

A1: An advance notification is a communication to the NRC and the governor or governor's designated official of an affected State that a shipment of a category 1 quantity of radioactive material will be made into or within that State's jurisdiction on a set date at a best-estimated time. The communication must be written, must follow the procedures set forth in § 37.77(a), and must contain the information specified in § 37.77(b). You may send it by mail, e-mail, or fax. An example of an advance notification template that would satisfy the NRC is provided in Annex D to this Subpart.

Q2: Are advance notifications required for any category 2 shipments?

A2: No. Advance notifications are not required for shipments of category 2 quantities of radioactive material unless the shipment falls within the scope of [10 CFR 71.97\(b\)](#) or is an export or import shipment requiring notification under [10 CFR 110.50\(c\)](#).

Q3: Where does a licensee obtain contact information for the governor's designee?

A3: A list of the contact information for the governor's designees is published annually in the *Federal Register*, typically in July or August. The 2011 update appeared on October 31, 2011. An updated list is posted on the NRC website at <http://nrc-stp.ornl.gov/special/designee.pdf>. Copies may also be obtained by contacting the Director, Division of Intergovernmental Liaison and Rulemaking, Office of Federal and State Materials and Environmental Management Programs, Nuclear Regulatory Commission. Note, however, that the currently available list provides governor-designated contact information only for SNF shipments, and the contacts for Part 37 shipments may not be the same. Part 37 contact information will be added to the latest available listing before the effective date of the rule.

Q4: Whom must the shipping licensee notify?

A4: If the license was issued by the NRC, the licensee must notify the NRC and each state through which the shipment will pass, including the state of the destination. If the license was issued by an Agreement State agency, the licensee must notify that agency and each state through which the shipment will pass, including the destination state.

Q5: Does the NRC share advance notification information about a shipment with other agencies?

A5: Yes. When NRC receives advance notification information, it may share the information with other affected Government agencies, such as DOT and DHS.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material (cont'd)

§ 37.77(a)

Procedures for submitting advance notification.

§ 37.77(a)(1)

The notification must be made to the NRC and to the office of each appropriate governor or governor's designee. The contact information, including telephone and mailing addresses, of governors and governors' designees, is available on the NRC website at <http://nrc-stp.ornl.gov/special/designee.pdf>. A list of the contact information is also available upon request from the Director, Division of Intergovernmental Liaison and Rulemaking, Office of Federal and State Materials and Environmental Management Programs, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Notifications to the NRC must be to the NRC's Director, Division of Security Policy, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555. The notification to the NRC may be made by e-mail to RAMQC_SHIPMENTS@nrc.gov or by fax to (301) 816-5151.

§ 37.77(a)(2)

A notification delivered by mail must be postmarked at least 7 days before transport of the shipment commences at the shipping facility.

§ 37.77(a)(3)

A notification delivered by any means other than mail must reach NRC at least 4 days before the transport of the shipment commences and must reach the office of the governor or the governor's designee at least 4 days before transport of a shipment within or through the State.

EXPLANATION:

Advance notifications of a shipment must be made in writing and postmarked 7 days before the shipment begins. Notifications delivered by any other means than mail must reach the office of the governor or the governor's designee at least 4 days before transport within or through the State.

QUESTIONS/ANSWERS:

Q1: Why does the mail notification requirement differ from that of other notifications?

A1: Mail delivery is not instantaneous; additional time is required to allow the mail notification to reach the appropriate party no later than the date required for other means of delivery. Under § 37.77(a)(3), this delivery date is "at least 4 days before the transport of the shipment commences" for a notification to NRC, and "at least 4 days before transport of a shipment within or through the State" for a notification to a governor or governor's designee. To make the notification's arrival by this date more likely to occur, a mailed notification must be sent sufficiently early -- postmarked at least 7 days

before the shipment commences -- to allow it to be received no later than it would be received if sent by such other means as by fax or e-mail.

Q2: Does a licensee have to mail the advance notification via the U.S. Postal Service?

A2: No. A licensee is not required to use the U.S. Postal Service. Delivery services such as Federal Express or United Parcel Services, as well as other delivery services, may be used.

Q3: What "other means" of advance notification besides the U.S. Postal Service or a commercial delivery service would be acceptable under § 37.77(a)(3)?

A3: A licensee may also fax or e-mail notifications. If the licensee uses a fax or e-mail for this purpose, however, the licensee should first verify the correct fax number or e-mail address with the recipient. The licensee should also confirm the receipt of the message with its intended recipient, so that both parties will know if the information has gone to an unauthorized third party.

Although an NRC licensee may use any of the delivery methods discussed above, the NRC recommends e-mail for NRC notification, because the NRC headquarters operations office is staffed 24 hours a day, 7 days a week, and will be able to confirm receipt of the notification in short order.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material (cont'd)

§ 37.77(b)

Information to be furnished in advance notification of shipment. Each advance notification of shipment of category 1 quantities of radioactive material must contain the following information, if available at the time of notification:

§ 37.77(b)(1)

The name, address, and telephone number of the shipper, carrier, and receiver of the category 1 radioactive material;

§ 37.77(b)(2)

The license numbers of the shipper and receiver;

§ 37.77(b)(3)

A description of the radioactive material contained in the shipment, including the radionuclides and quantity;

§ 37.77(b)(4)

The point of origin of the shipment and the estimated time and date that shipment will commence;

§ 37.77(b)(5)

The estimated time and date that the shipment is expected to enter each State along the route;

§ 37.77(b)(6)

The estimated time and date of arrival of the shipment at the destination; and

§ 37.77(b)(7)

A point of contact, with a telephone number, for current shipment information.

EXPLANATION:

This provision lists the information that must be provided in an advance notification of shipment.

QUESTIONS/ANSWERS:

Q1: What information must be included in an advance notification?

A1: Each licensee is expected to make a good faith effort to provide all the information required in § 37.77(b) available when making the initial advance notification. Any information not available at the time of the initial notification, however, must be provided in a revised notification under § 37.77(c)(1) as soon as the information becomes available, but no later than the commencement of the shipment. An example of an advance notification template that would satisfy the NRC is provided in Annex D to this Subpart.

Q2: What if I don't have all the shipment information listed in this subsection? Should I make the notification with the information I have, and provide the outstanding information when I'm able to obtain it?

A2: Yes. A shipping licensee may make the initial notification with the information available at that time. The remaining information must be provided in a revision notice as soon as the information becomes available.

Q3: If I don't have all the shipment information listed in this subsection before the scheduled shipment, can I still ship on the date originally specified in my first advance notification, or must I delay until I can provide all the information?

A3: You may ship on the date originally specified in your first advance notification if the only shipment information still missing is the exact quantity of radioactive material to be shipped. Prior operating experience has shown that in some cases, the exact quantity of the radionuclides to be shipped is the information most likely to be unknown until shortly before the shipment. Before commencement of the shipment, however, the shipping licensee must provide all of the information required by this subsection, including the quantity of material being shipped.

Q4: Must the "point of contact ... for current shipment information" under § 37.77(b)(7) be someone accompanying the shipment?

A4: No. The point of contact (PoC) should in fact *not* be someone accompanying the shipment, because communication to that person could be lost during an accident or security incident. The PoC should be someone with access to the information on the shipment available at the movement control center as it is defined under § 37.5.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material (cont'd)

§ 37.77(c)

Revision notice.

§ 37.77(c)(1)

The licensee shall provide any information not previously available at the time of the initial notification, as soon as the information becomes available but not later than commencement of the shipment, to the governor of the State or the governor's designee and to the NRC's Director of Nuclear Security, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

§ 37.77(c)(2)

A licensee shall promptly notify the governor of the State or the governor's designee of any changes to the information provided in accordance with paragraphs (b) and (c)(1) of this section. The licensee shall also immediately notify the NRC's Director, Division of Security Policy, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555 of any such changes.

§ 37.77(d)

Cancellation notice. Each licensee who cancels a shipment for which advance notification has been sent shall send a cancellation notice to the governor of each State or to the governor's designee previously notified and to the NRC's Director, Division of Security Policy, Office of Nuclear Security and Incident Response. The licensee shall send the cancellation notice before the shipment would have commenced or as soon thereafter as possible. The licensee shall state in the notice that it is a cancellation and identify the advance notification that is being cancelled.

EXPLANATION:

The shipping licensee is required to notify each of the previously notified States and the NRC, if the schedule for a shipment is revised or cancelled.

QUESTIONS/ANSWERS:

Q1: What should a licensee do if the shipment of a category 1 quantity is cancelled?

A1: If the shipment is cancelled, the shipping licensee must notify the States to which the initial advance notice had been sent, and the regulatory agency (NRC or Agreement State agency) with jurisdiction in the state of the shipment's origin.

Q2: What should a licensee do if the shipment schedule of a category 1 quantity is revised?

A2: If the shipment schedule is revised, the shipping licensee must notify the State through which the shipment is passing and the States it is scheduled to enter for the remainder of its itinerary.

Q3: Under § 37.77(c)(2), how “promptly” must a category 1 shipping licensee notify the governor of the State or the governor’s designee of any changes in the shipment information provided in the first advance notification, or any new information not previously available?

A3: The shipping licensee’s notification of any affected State’s governor or designee should be without delay. More specifically, assuming that there is no change in the names, addresses, or telephone numbers of the shipper, carrier, or receiving licensee, or change in the shipping and receiving licensees’ license numbers, notification should be as soon as the shipping licensee discovers or is advised of:

- A change in the description of the radioactive material to be shipped, including the radionuclides or quantity;
- A change in the shipment’s point of origin or estimated time or date of commencement;
- A change in the estimated time or date that the shipment is expected to enter each State along the route. (A 6-hour delay in the estimated entry time should be notified, for example, but notification of a 15-minute delay is not necessary);
- A change in the estimated time (a 6 hour delay should be notified, a 15 minute delay is not necessary) or date of arrival of the shipment at the destination. (A 6-hour delay in the estimated arrival time should be notified, for example, but notification of a 15-minute delay is not necessary);; and
- A change in the name or telephone number of the point of contact for current shipment information.

Notification of any changes in shipment information enroute should take place as soon as the driver or other authorized member of the transfer crew determines and informs the movement control center of a change in this information.

Prompt notification of significant schedule changes is particularly important if a state plans to provide an escort for the shipment.

Q4: Under § 37.77(c)(2), the licensee must also notify the NRC “immediately.” Is there a meaningful difference between notifying a governor or governor’s designee “promptly,” and notifying NRC “immediately?”

A4: No. NRC considers the words to be interchangeable for the purposes of part 37.

Q5: What mechanism should a licensee use to notify the States and the NRC of revisions or changes in the shipment information?

A5: The rule does not specify a mechanism for notifying the States and the NRC of revisions or changes in the shipment information. Each licensee may therefore use the

method that works best for that licensee. For cancellations, however, the licensee must “send a cancellation notice.” E-mailed, faxed, or written correspondences are all acceptable methods. The cancellation notice must be received before the shipment would have commenced or as soon thereafter as possible. This provides time for a state to cancel any planned escorts. A telephone call may sometimes be necessary to ensure that the notice is received in a timely manner.

Q6: Why do I have to notify the governors or their designees and the NRC under § 37.77(c)(2) if information about the shipment changes during the shipment?

6: The notification to the governor(s) allows States to be aware of shipments in their jurisdictions, to provide escorts if they consider them necessary, and to respond to any incidents that require a State response. The notification to NRC provides information that allows the NRC and other federal agencies to respond in the event of an incident.

Q7: Other than the requirement to notify NRC of any revision or changes to the advance notification, are any other notifications required?

A7: No, but one voluntary good practice would be helpful: to notify the NRC of the shipment’s actual arrival or departure times if these differ from the original advance notification. As noted above in Q&A 5 for § 37.77, the NRC shares information about shipments of category 1 quantities of radioactive material with other federal government agencies, such as DOT and DHS. Confirmation of actual shipment departure and arrival dates would enable the NRC staff to provide more accurate data for the tracking and current status of these shipments without having to make assumptions or contact the shipper by telephone to get updates. Notification to the NRC within 24 hours of the actual departure and arrival dates should be sufficient for this purpose.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material (cont'd)

§ 37.77(e)

Records. The licensee shall retain a copy of the advance notification and any revision and cancellation notices as a record for 3 years.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

Q1: For purposes of this record retention requirement, what constitutes a “revision” of an advance notification? Do I have to retain records of revisions for typos?

A1: You should retain a record of any notification revision that was important enough to have sent to NRC and the affected State. An error in one of the digits for a shipment date or time, for example, should be considered to require a revision of the initial notification, and would therefore have to be retained. You need not, however, issue a revised notification to correct a misspelling of a common word if the misspelling does not have the potential to cause confusion.

Q2: When does the 3-year clock start for the required retention of an advance notification document?

A2: The licensee should start the document retention period on the date the notification was sent.

Q3: If I have to cancel a planned shipment by phone to assure that I give the NRC or State official notice as soon as possible, how should I document that phone call?

A3: If you have to provide a revision or cancellation notification by telephone to the NRC or State official, you should record the date and time of the call, the name of the caller, the name of the person called, and the purpose of the call (revision or cancellation.) To meet the requirement here to “retain a copy” of these revision and cancellation notices, you should keep this documentation of the conversation in electronic or hard copy form for three years after the date of the call. You are encouraged to notify the NRC by e-mail.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material (cont'd)

§ 37.77(f)

Protection of information. State officials, State employees, and other individuals, whether or not licensees of the Commission or an Agreement State, who receive schedule information of the kind specified in § 37.77(b) shall protect that information against unauthorized disclosure as specified in § 73.21 of this chapter.

EXPLANATION:

Schedule information for shipments of category 1 quantities of radioactive material is considered to be SGI, and anyone receiving the information must protect it as specified in § 73.21.

QUESTIONS/ANSWERS:

Q1: What do the information protection requirements in § 73.21 specify?

A1: [10 CFR 73.21](#) mostly addresses general performance requirements for the protection of Safeguards Information, including SGI with the designation or marking: “Safeguards Information – Modified Handling” (SGI-M). Section 73.21(a)(ii) specifies that the transportation of source, byproduct, or special nuclear material in greater than or equal to category 1 quantities of concern must meet the requirements of [§ 73.23](#), *Protection of Safeguards Information – Modified Handling: Specific Requirements*.

Q2: Who is required to protect the schedule information?

A2: Any individual who receives the schedule information or any other SGI or SGI-M must protect it in accordance with the requirements in §§ 73.21 - 73.23.

Q3: What do I need to do, if anything, to ensure that those to whom I provide shipment schedule information comply with 10 CFR §73 requirements to protect it?

A3: NRC recognizes that licensees have no control over the use or misuse of this information by persons they are required to notify. Accordingly, NRC or an affected Agreement State agency will not hold a licensee responsible for the compliance of others. You must, however, mark any hard copy document you provide in accordance with § 37.23(d), and transmit any electronic information in accordance with § 37.23(g), to inform the individual who receives the schedule information or any other SGI or SGI-M information that he or she must protect it in accordance with the requirements in §§ 73.21 and 73.23. If you use a delivery service (e.g., FedEx, DHL, or UPS) or other commercial carrier (e.g., EnergySolutions, AATCarriers, or Edlow International) to transport your radioactive material, you should make sure that the carrier understands its responsibility to protect shipment-related information.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment

§ 37.79(a)

Shipments by road.

§ 37.79(a)(1)

Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 1 quantity of radioactive material shall:

§ 37.79(a)(1)(i)

Ensure that movement control centers are established that maintain position information from a remote location. These control centers must monitor shipments 24 hours a day, 7 days a week, and have the ability to communicate immediately, in an emergency, with the appropriate law enforcement agencies.

§ 37.79(a)(1)(ii)

Ensure that redundant communications are established that allow the transport to contact the escort vehicle (when used) and movement control center at all times. Redundant communications may not be subject to the same interference factors as the primary communication.

§ 37.79(a)(1)(iii)

Ensure that shipments are continuously and actively monitored by a telemetric position monitoring system or an alternative tracking system reporting to a movement control center. A movement control center must provide positive confirmation of the location, status, and control over the shipment. The movement control center must be prepared to promptly implement preplanned procedures in response to deviations from the authorized route or a notification of actual, attempted, or suspicious activities related to the theft, loss, or diversion of a shipment. These procedures will include, but not be limited to, the identification of and contact information for the appropriate LLEA along the shipment route.

§ 37.79(a)(1)(iv)

Provide an individual to accompany the driver for those highway shipments with a driving time period greater than the maximum number of allowable hours of service in a 24-hour duty day as established by the Department of Transportation Federal Motor Carrier Safety Administration. The accompanying individual may be another driver.

EXPLANATION:

These provisions establish the security requirements for shipping category 1 quantities of radioactive material by road.

QUESTIONS/ANSWERS:

Q1: When is the use of a movement control center necessary under § 37.79(a)(1)?

A1: To meet § 37.79(a)(1)(i), any licensee that ships category 1 quantities of radioactive material by road must either establish, or use a carrier that has established, movement control centers that maintain position information from a location remote from the transport vehicle or trailer. The control centers would be required to monitor shipments on a continuous and active basis 24 hours a day, 7 days a week, and have the ability to communicate immediately, in an emergency, with the appropriate law enforcement agencies. The movement control center must provide positive confirmation of the location, status, and individuals in control over the shipment, and must be prepared to implement preplanned procedures in response to deviations from the authorized route or to a notification of actual or attempted theft or diversion, or suspicious activities related to the theft, loss, or diversion of a shipment. These procedures include the identification of, and contact information for, the appropriate LLEA along the shipment route.

Q2: What is meant by “active” monitoring?

A2: A movement control center is monitoring on an active basis whenever it employs a method of tracking a shipment that provides the capability for the control center operators to be immediately aware if a shipment has deviated from the shipping plans. For example, the movement control center must have the capability to be immediately aware if: (1) the shipment deviates from the planned route; (2) any unscheduled stops occur; or (3) any scheduled stops take longer than expected.

Q3: Where can the movement control center be located? Does it need to be on the licensee’s property?

A3: The movement control center may be located at either the licensee’s or a third party’s site, but it must be a stationary facility, not a mobile vehicle. Regardless of location, the movement control center must be able to monitor the category 1 shipment at all times and communicate with appropriate law enforcement agencies should the need arise.

Q4: Why are redundant communications necessary, and what must these redundant devices or systems be able to do under § 37.79(a)(1)(ii)?

A4: Redundant communications are required to mitigate an interruption caused by either natural events such as storms, or deliberate actions such as signal jamming, that may cause communications to be lost on the primary communication device. One or more additional communication devices must 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.

Redundant communications must be in place at all times to allow the transport vehicle to contact the movement control center and nearest LLEA if assistance is needed. An escort vehicle is not required, but if it is used it must also be able to communicate with the transport driver and the movement control center. The redundant communication

method must not be subject to the same interference factors as the primary communication method. To meet this requirement that the primary and redundant methods are not subject to the same interference factors, the licensee must ensure that the two systems do not rely on the same hardware or software (e.g., cell tower or proprietary network) to transmit their signal.

Q5: What is a “telemetric position monitoring system” under § 37.79(a)(1)(iii)?

A5: A telemetric position monitoring system is a data transfer system that captures, by instrumentation and/or other measuring devices, information about the location and status of a transport vehicle or package between the departure and destination locations. The gathering of this information permits remote monitoring and reporting of the location of a transport vehicle or package. Systems that use radiofrequency identification (RFID) or satellite-based global positioning technologies are examples of telemetric position monitoring systems.

Q6: Is a global positioning system (GPS) required?

A6: No. For category 1 material, continuous and active monitoring for shipments is required without regard to the technology that provides these capabilities. Continuous and active monitoring means that at any time while the shipment is enroute, the licensee must know the shipment’s whereabouts. Not specifying a particular technology provides licensees flexibility to design a continuous and active monitoring system that meets their unique circumstances. GPS would be considered an acceptable method.

Q7: When is a second individual needed for the shipment under § 37.79(a)(1)(iv)?

A7: An accompanying individual must be provided for the shipment when the driving time period is greater than the maximum number of allowable hours of service in a 24-hour duty day as established by the DOT Federal Motor Carrier Safety Administration. (See [49 CFR 395](#).) This security measure provides reasonable assurance that the material will be protected from theft or diversion when it is stationary and in emergency situations where it becomes necessary for the driver to stop or leave the vehicle. The accompanying individual may be another driver.

Q8: What should the driver and a second accompanying individual do during the shipment of a category 1 quantity?

A8: The driver (and/or the accompanying individual) should periodically call into the movement control center to provide a verbal status of the shipment and delivery. Each individual should maintain constant visual surveillance of the surrounding environment during transport. If the driver requires a break and stops the transport vehicle, either the driver or the accompanying individual should maintain constant visual surveillance of the immediate environment of the transport vehicle while it is not in motion. At least one of the individuals should periodically walk around the transport vehicle during the time it is not in motion to help confirm that there are no apparent safety-related or security-related issues associated with the vehicle. In addition, the periodic walk-around should include visual surveillance of the surrounding area to confirm that there is no evidence of tampering with the contents of the vehicle, or unusual or suspicious activity in the immediate vicinity. Note that the accompanying individual should undertake the

communication and surveillance measures discussed above if the driver is sleeping during the break.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment (cont'd)

§ 37.79(a)(1) Shipments by road. (cont'd)

§ 37.79(a)(1)(v)

Develop written normal and contingency procedures to address:

§ 37.79(a)(1)(v)(A)

Notifications to the communication center and law enforcement agencies;

§ 37.79(a)(1)(v)(B)

Communication protocols. Communication protocols must include a strategy for the use of authentication codes and duress codes and provisions for refueling or other stops, detours, and locations where communication is expected to be temporarily lost;

§ 37.79(a)(1)(v)(C)

Loss of communications; and

§ 37.79(a)(1)(v)(D)

Responses to an actual or attempted theft or diversion of a shipment.

§ 37.79(a)(1)(vi)

Each licensee who makes arrangements for the shipment of category 1 quantities of radioactive material shall ensure that drivers, accompanying personnel, and movement control center personnel have access to the normal and contingency procedures.

EXPLANATION:

These provisions require the use of written normal and contingency procedures for shipping category 1 quantities of radioactive material by road.

QUESTIONS/ANSWERS:

Q1: Under § 37.79(a)(1)(v), each licensee that makes arrangements for the shipment of category 1 quantities of radioactive material must develop written “normal” and “contingency” procedures. How do I decide what I should address in my “normal” procedures and what should go into my “contingency” procedures?

A1: Normal operating procedures should describe activities conducted to meet regulatory requirements that would be applicable under expected routine operating conditions. Examples of such activities include refueling and comfort stops, meal stops, and routine check-ins. Contingency procedures should identify what could interfere with compliance during preparations for transport or during actual transport of the radioactive material. Examples of such interferences include bad weather, suspicious activities, mechanical breakdown, road or bridge closures, detours, accidents, and acute illness.

Contingency procedures should address appropriate actions for both anticipated aberrant situations as well as those that are known to have been previously encountered during transport of radioactive material or storage incident to transport.

Q2: Section 37.79(a)(1)(v)(A) requires my procedures for category 1 shipments to address “notifications to the communication center and law enforcement agencies.” What kind of events must I develop notifications for, and what means of communications must I use i.e., satellite phone, cell phone, e-mail, text messaging, two-way radio?

A2: The licensee’s procedures must address notifications for all normal and contingency conditions covered by the procedures. The choice of communications technology is the licensee’s, but the licensee should bear in mind that e-mail and text messaging may not be conducive to communication without delay in the event of an emergency.

Q3: Section 37.79(a)(1)(v)(B) requires me to develop communication protocols for category 1 shipments that, among other things, include “a strategy for the use of authentication codes and duress codes and provisions for refueling or other stops, detours, and locations where communication is expected to be temporarily lost.” What are acceptable methods for authentication and duress codes, and acceptable technologies for applying them?

A3: An acceptable protocol may use a number of methods and technologies or combinations of them for duress and authentication codes. The rule does not specify which methods and technologies to use because the optimum strategy may differ from licensee to licensee. In choosing a strategy for authentication and duress codes, however, a licensee should consider the purpose of each. The 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, or an authorized representative of the NRC, an Agreement State agency, or an LLEA. 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 is responding to the licensee’s or communication center’s call is not being forced to provide false information.

To frustrate any attempt by an unauthorized individual to delay an investigation or call off an ongoing recovery effort prematurely, for example, 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. This may be accomplished by using an agreed-upon separate radio frequency or alternative communication method, by asking the caller to come before a video camera on the vehicle to display a photo identification badge, by asking for the correct answer to one or more agreed-upon questions, or by a combination of these. If questions are used, they should require specific responses that are either of a personally-distinguishing nature (e.g., the name of a first pet) or otherwise 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 it on his or her own initiative without prompting, and may involve seemingly

mission-related technical questions and answers, apparently offhand remarks, or some other conversational technique. The purpose of the duress code should be to enable the offsite individual to signal without arousing suspicion that he or she is making a false report under threat by an adversary not visible or obviously malevolent to licensee or call center personnel.

Q4: Under § 37.79(a)(1)(v)(C), my communications protocols for category 1 shipments must address “loss of communications.” What constitutes such a “loss of communications?” A loss of a minute’s duration? A loss of a half-hour? One dropped call? Two, or more dropped calls? Would static be considered “a loss of communication?”

A4: The NRC considers a loss of communication to be any curtailment in the availability of, impairment in the timeliness of, or degradation in the clarity of a message such that the intended recipient of the message is unable to understand it or receive it when needed. Only a shipping or receiving licensee, a movement control center operator, or a transport crew can determine what constitutes a loss of communications in the context of the importance and urgency of the message for safe and secure delivery of the material. The rule therefore leaves this determination to those best able to make it under the operating conditions prevailing during the shipment. These conditions necessarily frame any decision on when to switch from the primary to an alternate communications system.

To determine what should be considered a loss of communication, the licensee should identify foreseeable normal and contingency scenarios, and 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. In an accident or a security emergency, for example, there should be no delay in resorting to the secondary means of communication. The protocol should also allow the communicator to take the severity of static into account as well as the perceived urgency of a situation in determining the extent to which the degradation of communication clarity justifies switching to the alternate communication technology.

Q5: As a shipper of category 1 quantities under § 37.79(a)(1)(vi), I have to “ensure” that drivers, accompanying personnel, and movement control center personnel have access to the normal and contingency procedures. How do I “ensure” that drivers, transport crew members, and movement control center staff have adequate access? If I give them hard copies of the protocols, am I in violation if one of them loses the hard copy and forgets to replace it before an inspection?

A5: The NRC understands that there are limits on the extent to which a licensee can “ensure” that drivers, transport crew members, and movement control center staff actually use the licensee’s procedures for normal and contingency conditions, but there are measures a licensee can take to demonstrate compliance with the requirement to “ensure” that these individuals “have access” to these procedures. Possible measures could include, among others, requiring in the shipping contract that the carrier’s driver, accompanying individual, and movement control center staff sign a statement before the shipment can begin that they have in their possession a copy of these procedures and have read them. Another measure could be another clause in the shipping contract with a similar signoff procedure requiring the driver to keep a copy of the procedures in the glove box or other readily accessible location inside the vehicle. The licensee could also

offer and encourage training of the carrier's employees responsible for category 1 shipments in the shipping licensee's procedures. The shipping licensee could also have the procedures delivered to the carrier's movement control center by a commercial delivery service before the first shipment, and retain a receipt for documentation.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment (cont'd)

§ 37.79(a)(2)

Each licensee that transports category 2 quantities of radioactive material shall maintain constant control and/or surveillance during transit and have the capability for immediate communication to summon appropriate response or assistance.

§ 37.79(a)(3)

Each licensee who delivers to a carrier for transport, in a single shipment, a category 2 quantity of radioactive material shall:

§ 37.79(a)(3)(i)

Use carriers that have established package tracking systems. An established package tracking system is a documented, proven, and reliable system routinely used to transport objects of value. In order for a package tracking system to maintain constant control and/or surveillance, the package tracking system 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.

§ 37.79(a)(3)(ii)

Use carriers that maintain constant control and/or surveillance during transit and have the capability for immediate communication to summon appropriate response or assistance; and

§ 37.79(a)(3)(iii)

Use carriers that have established tracking systems that require an authorized signature prior to releasing the package for delivery or return.

EXPLANATION:

These provisions establish this Part's security requirements for shipping category 2 quantities of radioactive material by road.

QUESTIONS/ANSWERS:

Q1: I possess a category 2 quantity of radioactive material and transport it without using a commercial carrier service. What are the physical protection requirements for road shipments of these quantities of material?

A1: A licensee that does not use a commercial carrier, and itself transports by road category 2 or greater quantities of material, must meet the requirements of § 37.79(a)(2). To comply with § 37.47(a), the licensee must establish a security zone around the radioactive material, and may use the transport vehicle as the security zone boundary. Access to the security zone must under § 37.47(c) be limited to authorized individuals, and under § 37.49, the licensee must monitor, detect, assess, and respond to any unauthorized access. The licensee will also need to comply with the preplanning and coordination requirements of § 37.75, and with the investigation and reporting

requirements of § 37.81 if a shipment is lost. For those shipments of category 2 quantities of radioactive material that meet the criteria of § 71.97(b) of this chapter, the shipping licensee must also comply with the advance notification provisions of that section.

Q2: What requirements do I have to meet when I deliver a category 2 quantity of radioactive material to a carrier to ship in a single shipment?

A2: Under § 37.79(a)(3)(i), you must use a carrier that has an established, documented package tracking system that reliably enables you as the shipping licensee to know the last location of the package, what time it was there, and when it should arrive at the next control point. To meet this requirement, the carrier's tracking system should also let you see the chain of custody for the package and show who's accountable for it at each stage of the trip, so that you or the carrier can determine promptly whether the shipment is lost or missing. The tracking system must also require an authorized signature before releasing the package for delivery or return. Under §37.79(a)(3)(iii), your carrier must maintain constant control and surveillance during transit, and must be able to summon an armed LLEA response or other emergency or urgent assistance immediately when necessary.

Q3: If I'm not using an established nationwide delivery system like DHL, FedEx, or UPS, what can I do to ensure that my carrier has the equivalent tracking capabilities?

A3: You should ascertain in advance whether the carrier maintains a package tracking system with a reliable on-demand capability to ascertain the last location and current status of the shipment. If the licensee's carrier does not have such a capability, you must either require it as a condition for shipment, or find another carrier that meets the requirements of § 37.79(a)(2) and (3) and other applicable provisions of this Part.

Q4: What must a package control system for a category 2 shipment be able to do to "maintain constant control and/or surveillance?" Would I be in violation if there are any lapses or interruptions?

A4: The performance requirements for "constant control and/or surveillance" are clarified in § 37.79(a)(3)(i), which says that for a package tracking system to maintain these capabilities, the package tracking system "must allow the shipping licensee or transporter to identify when and where the package was last and when it should arrive at the next point of control." Thus, although you should take all reasonable measures to prevent or minimize tracking system malfunctions, you will not be in violation if the carrier's package control system is not able to pinpoint the location of the shipment moment by moment in real time.

Q5: Section 37.79(a)(2) requires me to maintain constant control and/or surveillance "during transit." When does "transit" begin and end for the purposes of this requirement?

A5: In general, transit begins when the organization with physical control over the material begins to move it offsite. Unless the licensee itself takes the material offsite to the carrier for shipment, transit begins when the carrier accepts the consignment of radioactive material for shipment and begins moving the loaded transport vehicle. Transit ends when the receiving licensee accepts the shipment from the carrier and

unloads or allows the radioactive material to be unloaded at the agreed-upon destination.

Q6: What kind of equipment must I use to “have the capability for immediate communication” under § 37.79(a)(2) to summon help? Satellite phones? Cell phones? Laptops for e-mails? Text messaging? Two-way radios? How “immediate” must this communication be?

A6: The rule does not specify any particular communications technology. That choice is left to the licensee’s discretion. The licensee’s or carrier’s chosen technology must, however, permit “immediate communication to summon appropriate response or assistance” the same as under § 37.79(a)(3)(ii). Cell or satellite phones and two-way radios meet this requirement. E-mailing or text messaging does not, because you cannot always be certain that the message has been received, and it could remain unopened too long to enable an immediate response.

Q7: Do I have to have a backup communications system to maintain the capability for “immediate communication?”

A7: A backup system is not required for transfers of category 2 quantity shipments, but it could provide a greater degree of assurance that the licensee or carrier will be able to maintain its capability for immediate communication in the event of a malfunction or damage to the primary communications system.

Q8: What’s the difference between “response” and “assistance?”

A8: The word “response” is generally used in Part 37 to denote a response by law enforcement personnel to an apparent or actual security event, and/or a response by trained emergency services personnel to prevent or mitigate any collateral safety impacts of a security event. “Assistance” is used in Part 37 to denote other kinds of emergency or urgent conditions under which the transport crew or vehicle(s) require outside help, such as towing or roadside repair service, to avoid or minimize an unplanned delay in the shipment. The NRC has used both words in § 37.79(a)(2) and (3) to signify that the licensee or carrier must have the capability for immediate communications for both security-related and non-security-related incidents.

Q9: Under § 37.79(a)(3)(iii), licensees must use carriers with tracking systems that require an “authorized signature” before the package can be released for delivery or return. How will I know that an individual who signs the shipping papers for a package is “authorized?”

A9: The individual should be an employee or contractor of the receiving licensee. Since that individual is subject to reassignment and may be unknown to you, it is a good practice to ask the carrier to ask for government- or licensee-issued photo identification to verify the individual’s identity, and company-issued documentation that the individual works for the receiving licensee or its contractor.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment (cont'd)

§ 37.79(b)

Shipments by rail.

§ 37.79(b)(1)

Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 1 quantity of radioactive material shall:

§ 37.79(b)(1)(i)

Ensure that rail shipments are monitored by a telemetric position monitoring system or an alternative tracking system reporting to the licensee, third-party, or railroad communications center. The communications center shall provide positive confirmation of the location of the shipment and its status. The communications center shall implement preplanned procedures in response to deviations from the authorized route or to a notification of actual, attempted, or suspicious activities related to the theft or diversion of a shipment. These procedures will include, but not be limited to, the identification of and contact information for the appropriate LLEA along the shipment route.

§ 37.79(b)(1)(ii)

Ensure that periodic reports to the communications center are made at preset intervals.

EXPLANATION:

These provisions establish the security provisions for shipping category 1 quantities of radioactive material by rail.

QUESTIONS/ANSWERS:

Q1: What are the physical protection requirements for rail shipments of category 1 quantities of radioactive material?

A1: Under § 37.79(b)(1)(i), licensees must ensure that rail shipments are monitored either by a telemetric position monitoring system or an alternative tracking system meeting certain criteria for reporting to a licensee, third-party, or railroad communications center. The communications center must provide positive confirmation of the shipment's status and location. Each center must also be prepared to implement preplanned procedures to respond to deviations from the authorized route to a notification of an actual or attempted theft or diversion of a shipment, or to any suspicious activity near the shipment. The procedures must also identify and provide contact information for the appropriate LLEA in each jurisdiction along the shipment route. Rail shipment tracking provides the means for a communications center to immediately report an unusual occurrence that could lead to the theft or diversion of the material.

Under § 37.79(b)(1)(ii), the shipping licensee must ensure that the communications center makes periodic reports at preset intervals.

Q2: What is a telemetric position monitoring system?

A2: A telemetric position monitoring system is a data transfer system that captures, by instrumentation and/or other measuring devices, information about the location and status of a transport vehicle or package between the departure and destination locations. The gathering of this information permits remote monitoring and reporting of the location of a transport vehicle or package. Systems that use radiofrequency identification (RFID) or satellite-based global positioning technologies are examples of telemetric position monitoring systems.

Q3: What's the difference between a railroad communication center and a movement control center for transport by road?

A3: The two types of centers fulfill equivalent communications functions. The NRC refers to "railroad communication center" because that's the accepted railroad industry term for the railroad-related entity that carries out the functions corresponding to those of a movement control center.

Q4: Also under § 37.79(b)(1)(i), the communications center must implement preplanned procedures in response to "deviations" from the authorized route. What constitutes a "deviation"?

A4: A deviation from the authorized route would be any redirection to another rail spur or rail line when the railroad communications center was not aware that the switch was to be made. This could include a relocation of a train within a rail yard if the relocation could adversely affect the ability of the railroad to locate the shipment or provide required security.

Q5: Section 37.79(b)(1)(ii) requires licensees to ensure that periodic reports to the communications center are made at preset intervals. What must I do if one of these reports is late? How long should I wait before taking action?

A5: Your shipment contract with the highway carrier or railroad should require its movement control or communications center to notify you immediately if a call from its transport crew is delayed by more than half the pre-arranged reporting interval. You should contact the LLEA immediately if the movement control or communications center cannot establish communications with the transport crew.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment (cont'd)

§ 37.79(b) Shipments by rail. (cont'd)

§ 37.79(b)(2)

Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 2 quantity of radioactive material shall:

§ 37.79(b)(2)(i)

Use carriers that have established package tracking systems. An established package tracking system is a documented, proven, and reliable system routinely used to transport objects of value. In order for a package tracking system to maintain constant control and/or surveillance, the package tracking system 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.

§ 37.79(b)(2)(ii)

Use carriers that maintain constant control and/or surveillance during transit and have the capability for immediate communication to summon appropriate response or assistance; and

§ 37.79(b)(2)(iii)

Use carriers that have established tracking systems that require an authorized signature prior to releasing the package for delivery or return.

EXPLANATION:

Establishes the security provisions for shipping category 2 quantities of radioactive material by rail.

QUESTIONS/ANSWERS:

Q1: What are the physical protection requirements for rail shipments of category 2 quantities of radioactive material?

A1: Under § 37.79(b)(2)(i), a licensee shipping category 2 quantities of radioactive material by rail must at minimum have the capability to contact the shipping carrier and determine the approximate location of the shipment. Such licensees must also use a carrier that has a documented, proven, and reliable package tracking system that allows the shipping licensee or carrier to identify when and where the package was when the train last reported, and when it should arrive at the next point of control. Under § 37.79(b)(2)(ii), the carrier must maintain constant control and surveillance during transit and have the capability for immediate communication to summon an appropriate response or assistance. Under § 37.79(b)(2)(iii), the carrier must also require an authorized signature prior to releasing the package for delivery or return.

Q2: What must a package control system for a category 2 shipment be able to do to “maintain constant control and/or surveillance?” Would I be in violation if there are any lapses or interruptions?

A2: The performance requirements for “constant control and/or surveillance” are clarified in § 37.79(b)(2)(i), which says that to maintain these capabilities, the package tracking system must allow the shipping licensee or carrier “to identify when and where the package was last and when it should arrive at the next point of control.” Thus, although the shipping licensee should take all reasonable measures to prevent or minimize tracking system malfunctions, the licensee will not be in violation if it is unable to pinpoint the location of the shipment moment by moment in real time.

Q3: Section 37.79(b)(2)(ii) requires me to maintain constant control and/or surveillance “during transit.” When does “transit” begin and end for the purposes of this requirement?

A3: Transit begins when the carrier accepts the consignment of radioactive material for shipment electronically or in writing and begins movement of the loaded transport vehicle. Transit ends when the receiving licensee accepts the shipment from the carrier electronically or in writing and unloads or allows the radioactive material to be unloaded at the agreed-upon destination.

Q4: What kind of equipment must a carrier have to “have the capability for immediate communication” to summon help? Satellite phones? Cell phones? Laptops for e-mails? Text messaging? Two-way radios? How “immediate” must this communication be?

A4: The rule does not require any particular communications technology. The carrier has the discretion to choose the type of communication equipment used to summon help under § 37.79(b)(2). The chosen technology must, however, permit communication without delay. Cell or satellite phones and two-way radios meet this requirement. E-mailing or text messaging does not, because you cannot always be certain that the message has been received, and it could remain unopened too long to enable an immediate response.

Q5: Does my carrier have to have a backup communications system to maintain the capability for “immediate communication?”

A5: A backup system is not required, but it could provide a greater degree of assurance that the carrier will be able to maintain its capability for immediate communication in the event of a malfunction or damage to the primary communications system.

Q6: What’s the difference between “response” and “assistance?”

A6: The word “response” is generally used in Part 37 to denote a response by law enforcement personnel to an apparent or actual security event, and/or a response by trained emergency services personnel to prevent or mitigate any collateral safety impacts of a security event. “Assistance” is used in Part 37 to denote a response to other kinds of emergency or urgent conditions under which the transport crew requires outside help, such as towing or on-location repair service, to avoid or minimize an unplanned delay in the shipment. NRC has used both words in § 37.79(b)(2) to signify that the licensee or carrier must have the capability for immediate communications for both security-related and non-security-related incidents.

Q7: Under § 37.79(b)(2)(iii), licensees must use carriers with tracking systems that require “an authorized signature” before the package can be released for delivery or return. How will I know that an individual who signs the shipping papers for a package is “authorized?”

A7: The individual should be an employee or contractor of the receiving licensee. Since that individual is subject to reassignment and may be unknown to you, it is a good practice to ask the carrier or railroad to ask for government- or licensee-issued photo identification to verify the individual’s identity, and company-issued documentation that the individual works for the receiving licensee or its contractor.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment (cont'd)

§ 37.79(c)

Investigations. Each licensee who makes arrangements for the shipment of category 1 quantities of radioactive material shall immediately conduct an investigation upon the discovery that a category 1 shipment is lost or missing. Each licensee who makes arrangements for the shipment of category 2 quantities of radioactive material shall immediately conduct an investigation, in coordination with the receiving licensee, of any shipment that has not arrived by the designated no-later-than arrival time.

EXPLANATION:

The shipping licensee must investigate immediately if a category 1 quantity shipment is lost or missing, or if a category 2 quantity shipment does not arrive by the NLT arrival time.

QUESTIONS/ANSWERS:

Q1: How should I decide that a shipment of my category 1 quantity of radioactive material is lost or missing?

A1: If your carrier's telemetric position monitoring system or the railroad's communications center can't tell you where your shipment is within a few minutes after you ask, and you're confident that the tracking and communications systems are functioning normally, you should consider the shipment lost or missing. Additionally, if you are unable to reach the transport crew after a missed check in, you should assume that the shipment is missing.

Q2: What should an investigation of a lost or missing category 1 quantity shipment include?

A2: The scope of an investigation will depend on the circumstances of the lost or unaccounted-for material, the shipment's transportation mode, and the contingency procedures. You should coordinate your investigation with the carrier. Items for the investigation include but are not limited to:

- Determine the time and location of the last transport crew check in;
- Determine where communication was lost;
- Determine where tracking was lost;
- Confirm equipment is working properly; and
- Contact the escort if one was being used.

Q3: What should I do if my category 2 shipment does not arrive by the NLT arrival time?

A3: If you are a receiving licensee, you must notify the shipping licensee in accordance with § 37.75(c). You should also cooperate in the investigation that the shipping licensee is required to conduct.

If you are the shipping licensee, you must immediately begin an investigation to determine what happened to the shipment.

Q4: What should an investigation of a lost or missing category 2 quantity shipment include?

A4: The shipping licensee should contact the carrier to determine the shipment's last known location. The shipping licensee should work with the carrier to determine the shipment's current location. If the carrier cannot determine where the shipment is located, the shipping licensee should contact the NRC Operations Center that a category 2 shipment is lost or missing. The shipper should continue to work with the carrier to locate the shipment, but if the shipment is still missing after 24 hours of the initial notification, the licensee must again contact the NRC Operations Center.

§ 37.81 Reporting of events

§ 37.81(a)

The shipping licensee shall notify the appropriate LLEA and the NRC Operations Center ((301) 816-5100), within 1 hour of its determination that a shipment of category 1 quantities of radioactive material is lost or missing. The appropriate LLEA would be the law enforcement agency in the area of the shipment's last confirmed location. During the investigation required by § 37.79(c), the shipping licensee will provide agreed upon updates to the NRC Operations Center on the status of the investigation.

EXPLANATION:

The shipping licensee must notify the LLEA and the NRC Operations center within 1 hour after determining that a shipment of category 1 quantities of radioactive material is lost or missing.

QUESTIONS/ANSWERS:

Q1: When must a licensee make notification that a category 1 shipment is lost or missing?

A1: When a licensee determines that a shipment of a category 1 quantity of radioactive material is lost or missing, the licensee must notify the LLEA in the area of the shipment's last confirmed location within 1 hour and then notify the NRC Operations Center. Notification to the NRC should be as prompt as possible, but not at the expense of causing delay or interference with the LLEA response to the event. Although § 37.81(a) sets one hour as the maximum time for a "lost or missing" notification of a category 1 quantity shipment, the licensee should notify the LLEA as soon as the carrier has completed its first unsuccessful attempt to locate the material and confirmed that the inability to trace it was not a result of human error or a malfunction of the system for monitoring the position of the shipment.

Q2: How can I know when a category 1 shipment is lost or missing?

A2: Under § 37.79(a) and (b), you are required to ensure that shipments are continuously and actively monitored by a telemetric position monitoring system or an alternative tracking system reporting to a movement control center for road shipments or a railroad communication center. Section 37.79(a) and (b) also require you to ensure that both types of centers provide positive confirmation of the location, status, and control over the shipment. Thus, if you comply with these requirements, you should have no trouble in readily ascertaining whether a category 1 shipment is lost or missing.

If the transport crew has not checked in at the required frequency or the tracking system indicates that the shipment is not on the approved route and you have not heard from the transport crew, you should begin an immediate investigation to determine what is happening. If your attempts to contact the transport crew are unsuccessful (using both the primary and backup communication systems), you should assume that something is wrong and report to the LLEA and the NRC.

If you're shipping a category 1 quantity of material by road, and want to enhance the speed and authenticity of your carrier's confirmation of a lost or missing shipment, you could also consider requesting that your carrier adopt one or more of the Transportation Security Administration's (TSA's) voluntary [Security Action Items \(SAIs\) for Highway Security Sensitive Materials \(HSSM\)](#). Appendix B on TSA's web page lists category 1 and category 2 quantities of radioactive materials from the IAEA's Code of Conduct list as Tier I HSSM, which the TSA defines as commercial motor vehicle-transported materials "whose potential consequences from an act of terrorism include a highly significant level of adverse effects on human life, environmental damage, transportation system disruption, or economic disruption." Among the voluntary practices for Tier I HSSMs in the TSA's [Appendix A](#) list of SAIs are two below that could facilitate a timely determination that licensed material is lost or missing:

- **Panic Button Capability ...** – Employers should implement means for a driver to transmit an emergency alert notification to dispatch. 'Panic Button' technology enables a driver to remotely send an emergency alert notification message either via Satellite or Terrestrial Communications, and/or utilize the remote Panic Button to disable the vehicle.
- **Tractor and Trailer Tracking Systems ...** – Employers should have the ability of implementing methods of tracking the tractor and trailer throughout the intended route with satellite and/or land-based wireless GPS communications systems. Tracking methods for the tractor and trailer should provide current position by latitude and longitude. Geofencing and route monitoring capabilities allow authorized users to define and monitor routes and risk areas. If the tractor and/or trailer deviates from a specified route or enters a risk area, an alert notification should be sent to the dispatch center. An employer or an authorized representative should have the ability to remotely monitor trailer "connect" and "disconnect" events. Employers or an authorized representative should have the ability to poll the tractor and trailer tracking units to request a current location and status report. Tractor position reporting frequency should be configured at not more than 15-minute intervals.

These voluntary practices would also facilitate timely notifications under this section.

Q3: How frequently should the licensee provide updates to the NRC Operations Center?

A3: The licensee should provide updates when new information is received. In addition, the licensee should discuss with the NRC, on a case-by-case basis, what the frequency of updates should be as the frequency will depend on the circumstances of the lost or missing shipment.

§ 37.81 Reporting of events (cont'd)

§ 37.81(b)

The shipping licensee shall notify the NRC Operations Center ((301) 816-5100) within 4 hours of its determination that a shipment of category 2 quantities of radioactive material is lost or missing. If, after 24 hours of its determination that the shipment is lost or missing, the radioactive material has not been located and secured, the licensee shall immediately notify the NRC Operations Center.

EXPLANATION:

The shipping licensee must notify the NRC Operations center within 4 hours of the determination that a shipment of category 2 quantities of radioactive material is lost or missing and call after 24 hours if the shipment had not been located.

QUESTIONS/ANSWERS:

Q1: When must a licensee make notification that a category 2 shipment is lost or missing?

A1: The concept of lost or missing licensed material is not new, and not unique to Part 37. In sum, if you don't know where the material is and can't readily locate it, you should consider it lost or missing. You are allowed reasonable time to try and trace a shipment. A licensee is not required to make the notification when a shipment has not arrived by the NLT arrival time. The shipping licensee is required to begin its investigation at the point in time. If the investigation does not discover the location of the material, the licensee must make the notification to the NRC. A licensee can take a reasonable amount of time to conduct the investigation however, the investigation should not last several days. The licensee needs to use some judgment in making the determination that the investigation has taken long enough and that the NRC needs to be notified.

Once you determine that the shipment is lost or missing, you must notify the NRC Operations Center within 4 hours of such determination. The licensee is also required to immediately notify the NRC Operations Center if, after 24 hours from its determination that the shipment was lost or missing, the location of the material still cannot be determined.

§ 37.81 Reporting of events (cont'd)

§ 37.81(c)

The shipping licensee shall notify the designated LLEA along the shipment route, as soon as possible upon discovery of any actual or attempted theft or diversion of a shipment or suspicious activities related to the theft or diversion of a shipment of a category 1 quantity of radioactive material. As soon as possible after notifying the LLEA, the licensee shall notify the NRC Operations Center ((301) 816-5100) upon discovery of any actual or attempted theft or diversion of a shipment, or any suspicious activity related to the shipment of category 1 radioactive material.

EXPLANATION:

The shipping licensee must notify the designated LLEA along the shipment route upon discovery of any actual or attempted theft or diversion of a shipment or suspicious activities related to a shipment of category 1 quantities of radioactive material. After notifying the LLEA, the licensee must notify the NRC Operations Center.

QUESTIONS/ANSWERS:

Q1: This subsection requires me to notify an LLEA along the route as soon as possible “upon discovery” of any actual or attempted theft or diversion of a shipment or suspicious activities. Does this mean I must report whatever a member of the transport crew “discovers” as soon as he or she reports it, without first trying to confirm whether it is what the individual thinks it is?

A1: No. You should, however, immediately assess whether the reported event or activity, or the signal you’ve received from an alarm or monitoring device, requires LLEA assistance without delay. An explosion on or around the transport or escort vehicle, for example, gunshots nearby in an urban or suburban area or other setting where hunting is prohibited, or the image of an armed individual on your or the carrier’s monitoring screen, would indicate the need for an immediate LLEA response and should be reported immediately.

Q2: What would a licensee be required to do if there is an attempt to steal or divert a category 1 shipment?

A2: For shipments of category 1 quantities of radioactive material, under § 37.81(c) a licensee who discovers an actual or attempted theft or diversion of a shipment, or any suspicious activity related to a shipment, must notify the designated LLEA along the shipment route as soon as possible. After notifying the LLEA, the licensee must notify the NRC Operations Center at (301) 816-5100. The NRC Operations Center will notify other affected States and the agency’s Federal partners, as appropriate.

Q3: What types of activities should be considered “suspicious?”

A3: TSA [guidance for private or contract carrier employees](#) lists a number of activities that may be considered suspicious that the licensee could require its carrier to make its employees aware of:

- Discovery of any unknown articles found in, on, or around company vehicles.
- Unauthorized persons photographing company vehicles and/or locations.
- Being followed by other vehicles for extended periods of time.
- Being asked inappropriate questions about your company's business related to security, products, delivery schedules, or any other information that seems suspicious.
- Reports or observations of commercial vehicles parked in unusual locations such as fields, vacant warehouses or other secluded areas.
- Unauthorized persons loitering where company vehicles are loading/unloading, parked, or serviced.

TSA guidance for independent or owner-operated truck drivers offers several related additional examples of suspicious activities:

- Anyone who inquires too much about what you're hauling, where you're going, or your intended route.
- Vehicles following you for extended periods of time.
- Persons observing truck parking areas and automobiles repeatedly cruising through those areas.
- Requests to stop for alleged accidents or breakdowns you cannot see.
- Anyone approaching you seeking a ride for themselves or another person.
- An unattended vehicle parked in or on critical infrastructure (e.g. tunnel, bridge, etc.) or in a location that seems out of place.
- Anyone avoiding a security checkpoint.
- Obviously altered signage on a vehicle.
- Missing license plate(s) or other unique markings on a vehicle.

For example, if the truck driver notices suspicious activity, he or she should proceed in accordance with the employer's established security policies and procedures. If there is any doubt regarding suspicious behavior, the driver should report to his or her supervisor.

The lists above are not exhaustive, but provide examples of actions that could be considered suspicious. The licensee is responsible for evaluating activity to determine if it is suspicious or not.

§ 37.81 Reporting of events (cont'd)

§ 37.81(d)

The shipping licensee shall notify the NRC Operations Center ((301) 816-5100), as soon as possible upon discovery of any actual or attempted theft or diversion of a shipment, or any suspicious activity related to the shipment, of a category 2 quantity of radioactive material.

EXPLANATION:

The shipping licensee must notify the NRC upon discovery of any actual or attempted theft or diversion of a shipment or suspicious activities related to a shipment of a category 2 quantity of radioactive material.

QUESTIONS/ANSWERS:

Q1: This subsection requires me to notify the NRC as soon as possible “upon discovery” of any actual or attempted theft or diversion, or suspicious activities related to a shipment of a category 2 quantity. Does this mean I must report whatever my carrier has “discovered” as soon as the carrier reports it, without first trying to confirm whether it is what the carrier thinks it is?

A1: No. Under § 37.81(b), you must notify the NRC Operations Center ((301) 816-5100) within 4 hours of your determination that a shipment of category 2 quantities of radioactive material is lost or missing. This should allow you time to gather sufficient information to decide whether there actually have been suspicious activities or an actual or attempted theft or diversion.

Q2: What would a licensee be required to do if there is an attempt to steal or divert a category 2 shipment?

A2: Under § 37.81(d), a licensee who discovers an actual or attempted theft or diversion of a category 2 quantity shipment, or any suspicious activity related to a shipment, must notify the NRC Operations Center at (301) 816-5100 as soon as possible.

Q3: What types of activities should be considered “suspicious?”

A3: See Q&A 3 for § 37.81(c).

§ 37.81 Reporting of events (cont'd)

§ 37.81(e)

The shipping licensee shall notify the NRC Operations Center ((301) 816-5100) and the LLEA as soon as possible upon recovery of any lost or missing category 1 quantities of radioactive material.

EXPLANATION:

The shipping licensee must notify the NRC and the LLEA upon recovery of any lost or missing category 1 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: What constitutes “recovery” for purposes of this notification?

A1: Lost or missing licensed material can be considered recovered only when it is again in the physical possession of, or in a location otherwise under the control of, an authorized employee of the carrier, the shipping or recipient licensee, an authorized state or federal agency, or an LLEA who is able to prevent or deter unauthorized access to the material.

Q2: How can I know that the individual reporting the recovery of a lost or missing category 1 shipment is the person he or she says she is, and not an adversary trying to trick me into calling off my search?

A2: To frustrate any attempt by an unauthorized individual to call off an ongoing recovery effort prematurely, you should try to confirm the true identity of the employee, regulatory agency representative, or law enforcement officer reporting from an offsite location. If there is a video camera on the vehicle, this confirmation may be accomplished by asking the caller to appear before the camera and display a photo identification badge.

If there is no on-board video camera, a licensee could confirm the identity of an employee by using its pre-established authentication code, by asking the employee to use an agreed-upon separate radio frequency or alternative communication method, by asking for the correct answer to one or more agreed-upon identifying questions, or by a combination of these. If you use questions, they should require specific responses that are either of a personally-distinguishing nature (e.g., the name of a first pet) or otherwise not so intuitively obvious that an adversary could infer the correct response.

To confirm the true identity of a regulatory agency representative or law enforcement officer claiming to have recovered the lost or missing material when there is no on-board video camera, you could ask the individual to describe the location and wait with the material until additional law enforcement assistance arrives. If the individual says that his or her current location is unsafe, you may ask for the address or distinguishing landmarks of the alternate location and tell the individual to wait for assistance there while you direct the nearest operating LLEA to the new location. If the individual claims

to be a law enforcement officer, you could ask the responding LLEA to verify the individual's employment or refer you to a number where you can obtain such verification. If the individual claims to be a regulatory agency representative, you could ask for the agency's toll-free number to verify his or her employment. The individual's responses to your requests for more information may not provide the positive identification you need, but incorrect or misleading information may signify that the individual is not the official he or she claims to be. If you suspect a false identity, you should try to keep the individual on the phone and silently alert a colleague if possible (e.g., with a hand-written note) to contact the responding LLEA out of the caller's earshot. This might enable the LLEA to work with the phone service provider to identify more accurately the caller's current location and direction of travel.

The licensee or carrier should also use its pre-established duress code to confirm that an offsite interlocutor is not being forced (e.g., at gunpoint or within lethal range of an explosive) to submit a false report. The code should permit the offsite individual to introduce it on his or her own initiative without prompting, and may involve seemingly mission-related technical questions and answers, apparently offhand remarks, or some other conversational technique to enable the offsite individual to signal without arousing suspicion that he or she is making a false report to licensee or call center personnel under threat by an adversary not visible or obviously malevolent. See also Q&A 3 for § 37.79(a)(1)(v)(B).

§ 37.81 Reporting of events (cont'd)

§ 37.81(f)

The shipping licensee shall notify the NRC Operations Center ((301) 816-5100) as soon as possible upon recovery of any lost or missing category 2 quantities of radioactive material.

EXPLANATION:

The shipping licensee must notify the NRC upon recovery of any lost or missing category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: Should licensees make notification that a lost or missing category 2 shipment has been found?

A1: Yes. The licensee must notify the NRC Operations Center when a lost or missing shipment of category 2 quantities of radioactive material has been located. An Agreement State licensee notifies the Agreement State. This notification would be considered an update of the initial notification.

Q2: Can I notify the NRC Operations Center by any other means than telephoning?

A2: Yes. You can fax a notification to the NRC Operations Center at (301) 816-5151.

§ 37.81 Reporting of events (cont'd)

§ 37.81(g)

The initial telephonic notification required by paragraphs (a) through (d) must be followed within a period of 30 days by a written report submitted to the NRC by an appropriate method listed in § 37.7. A written report is not required for notifications on suspicious activities required by paragraphs (c) and (d) of this section. In addition, the licensee shall provide one copy of the written report addressed to the Director, Division of Security Policy, Office of Nuclear Security and Incident Response. The report must set forth the following information:

§ 37.81(g)(1)

A description of the licensed material involved, including kind, quantity, and chemical and physical form;

§ 37.81(g)(2)

A description of the circumstances under which the loss or theft occurred;

§ 37.81(g)(3)

A statement of disposition, or probable disposition, of the licensed material involved;

§ 37.81(g)(4)

Actions that have been taken, or will be taken to recover the material; and

§ 37.81(g)(5)

Procedures or measures that have been, or will be, adopted to ensure against a recurrence of the loss or theft of licensed material.

EXPLANATION:

The licensee must provide NRC a written report within 30 days of an initial report of lost or missing material or attempted or actual theft or diversion of a shipment of category 1 or category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: What level of detail should I provide in my 30-day written report on an event?

A1: The appropriate level of detail would depend on a number of considerations, including: the nature and severity of the security incident; whether it was a first occurrence or a reoccurrence, and whether it has a significant potential to recur; the adequacy of the licensee's monitoring efforts; the timeliness of the initial detection; the accuracy of the assessment; and the timeliness and potential effectiveness of the measures implemented in response to the incident. In addition to an identification of corrective actions, the report should describe the data and analyses that support the licensee's identification of the root and significant contributing cause(s) of the incident, and how these data and analyses support the licensee's selection of corrective actions identified. If the incident was a recurrence of a similar incident, the report should briefly describe past corrective actions and the findings of past assessments, and identify likely reasons that the past corrective actions did not prevent or mitigate a recurrence of the

condition. The report should then explain the basis for the licensee's determination that the proposed new or revised corrective actions, or changes in the licensee's implementation of these actions, are likely to reduce the probability of a recurrence of the condition or mitigate its effects.

§ 37.81 Reporting of events (cont'd)

§ 37.81(h)

Subsequent to filing the written report, the licensee shall also report any additional substantive information on the loss or theft within 30 days after the licensee learns of such information.

EXPLANATION:

After filing the 30-day report, the licensee must report any additional substantive information on the loss or theft within 30 days after the licensee learns of such information.

QUESTIONS/ANSWERS:

Q1: What would be considered to be “additional substantive information?”

A1: Examples of additional substantive information would include information not previously reported to the NRC that has been gathered since the previous report was made. If you were unable to complete your investigation within 30 days for the initial report, the final findings would need to be provided in the subsequent report.

Q2: Would I have to report as “additional substantive information” something I “learned of” through TV, radio, or print news? Through Wikipedia or some other internet source? From an LLEA representative?

A2: No, you would not necessarily need to report as substantive information something that was learned through TV, radio, print news, or internet sources. The fact that information is available does not mean that the information is correct or would be of interest to the NRC. Depending on the information provided by an LLEA representative, the information might be considered to be substantive. You should use judgment in deciding whether the information obtained from any source would be of interest to the NRC.

Annex D

Template for Advance Notifications to the NRC of Shipments of Category 1 Quantities of Radioactive Material under § 37.77(b)

Notification Date: _____

Shipping ID (Unique Identifier): _____

Notification Revision Number: _____

Shipper (Include Name,* Address* and Name of Point of Contact and Telephone Number*):

Shipper's License Number* (and Import / Export License When Applicable): _____

Type of Shipment (Domestic; Import; Export; Transshipment): _____

Point of Origin* (Include Address and Name of Point of Contact and Telephone Number):

Recipient (Consignee) (Include Name,* Address,* Name of Point of Contact, and Telephone Number

Recipient's License Number*: _____

Radioactive Isotope*: _____

Estimated Activity* (Preferably in TBq): _____

Description of Shipment* (e.g., physical form, number of sources/flasks/containers):

End Use of Shipment:

Carrier(s) (Include Name,* Address,* and Name of Point of Contact, and Telephone Number*):

Planned date* and time* of Shipment Departure (and Confirmation of Shipment Actual Departure date* and time*): _____

Planned date* and time* of Shipment Arrival (and Confirmation of Shipment Actual Arrival date* and time*): _____

Routing Information:

Mode(s) of Transportation: _____

Estimated Time and Date that the shipment is expected to enter each State along the route*:

For Import/ Exports Include Point of US Entry or Departure*: _____

Point of contact, with a telephone number, for current shipment information*:

* indicates that the information is required under § 37.77(b). The other items are voluntary but are requested to enable the NRC to provide more accurate and detailed information for any emergency response.

NOTE: The preferred notification method to the NRC is via the Operations Center by e-mail or facsimile at least four days before the scheduled shipping date. The notification to the NRC may be made by e-mail to RAMQC_SHIPMENTS@nrc.gov or by fax to (301) 816-5151. Shippers should coordinate with States as indicated in § 37.77(a). The Shipper is requested to also notify the NRC with a confirmation of the departure date within one day after the actual shipment departure and arrival date within one day after the actual arrival.

Revisions: Under § 37.77(c)(1), any change in the shipment information supplied above must be provided to the States and NRC as soon as the information becomes available, but no later than commencement of the shipment. Under § 37.77(c)(2), notification of shipment schedule changes while in transit must be made immediately to the NRC Operations Center and the appropriate States.

Subpart E – Reserved

Subpart F – Records

37.101 Form of records.

37.103 Record retention.

§ 37.101 Form of records

§ 37.101

Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform, provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, and specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records.

EXPLANATION:

Licensees are required to keep records that are legible for the length of the retention period.

QUESTIONS/ANSWERS:

These provisions are not unique to part 37, therefore no questions and answers are provided.

§ 37.103 Record retention**§ 37.103**

Licenses shall maintain the records that are required by the regulations in this part for the period specified by the appropriate regulation. If a retention period is not otherwise specified, these records must be retained until the Commission terminates the facility's license. All records related to this part may be destroyed upon Commission termination of the facility license.

EXPLANATION:

Licenses are required to maintain records required by the regulations until the Commission terminates the license, unless the regulations specify a retention period.

QUESTIONS/ANSWERS:

Q1: If Part 37 does not specify how long to keep a record, is the licensee required to keep it? If so, for how long?

A1: If the regulations in Part 37 do not specify the length of record retention for a particular record, the record must be retained under this section until the Commission terminates the facility license.

Subpart G – Enforcement

37.105 Inspections.

37.107 Violations.

37.109 Criminal penalties.

§ 37.105 Inspections

§ 37.105(a)

Each licensee shall afford to the Commission at all reasonable times opportunity to inspect category 1 or category 2 quantities of radioactive material and the premises and facilities wherein the nuclear material is used, produced, or stored.

§ 37.105(b)

Each licensee shall make available to the Commission for inspection, upon reasonable notice, records kept by the licensee pertaining to its receipt, possession, use, acquisition, import, export, or transfer of category 1 or category 2 quantities of radioactive material.

EXPLANATION:

The NRC has the right to inspect licensee facilities, including all records maintained by the licensee pertaining to its receipt, possession, use, acquisition, import, export, or transfer of radioactive material.

QUESTIONS/ANSWERS:

These provisions are not unique to part 37, therefore no questions and answers are provided.

§ 37.107 Violations

§ 37.107(a)

The Commission may obtain an injunction or other court order to prevent a violation of the provisions of --

§ 37.107(a)(1)

The Atomic Energy Act of 1954, as amended;

§ 37.107(a)(2)

Title II of the Energy Reorganization Act of 1974, as amended; or

§ 37.107(a)(3)

A regulation or order issued pursuant to those Acts.

EXPLANATION:

The NRC may obtain a court order to stop someone from violating the regulations.

QUESTIONS/ANSWERS:

None. The NRC [Enforcement Manual](#) is the implementing guidance for the NRC enforcement program. For additional information on the Manual and links to related documents, click on

<http://www.nrc.gov/about-nrc/regulatory/enforcement/guidance.html#manual>.

The Manual provides guidance consistent with the NRC [Enforcement Policy](#), which sets forth the general principles governing the enforcement program. For additional information on the Enforcement Policy and links to related documents, click on

<http://www.nrc.gov/about-nrc/regulatory/enforcement/enforce-pol.html>.

§ 37.107 Violations (cont'd)

§ 37.107(b)

The Commission may obtain a court order for the payment of a civil penalty imposed under section 234 of the Atomic Energy Act:

§ 37.107(b)(1)

For violations of --

§ 37.107(b)(1)(i)

Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended:

§ 37.107(b)(1)(ii)

Section 206 of the Energy Reorganization Act;

§ 37.107(b)(1)(iii)

Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;

§ 37.107(b)(1)(iv)

Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

§ 37.107(b)(2)

For any violation for which a license may be revoked under Section 186 of the Atomic Energy Act of 1954, as amended.

EXPLANATION:

The NRC may obtain a court order to force someone to pay a civil penalty for violating the regulations.

QUESTIONS/ANSWERS:

None. The NRC [Enforcement Manual](#) is the implementing guidance for the NRC enforcement program. For additional information on the Manual and links to related documents, click on

<http://www.nrc.gov/about-nrc/regulatory/enforcement/guidance.html#manual>.

The Manual provides guidance consistent with the NRC [Enforcement Policy](#), which sets forth the general principles governing the enforcement program. For additional information on the Enforcement Policy and links to related documents, click on

<http://www.nrc.gov/about-nrc/regulatory/enforcement/enforce-pol.html>.

§ 37.109 Criminal penalties

§ 37.109(a)

Section 223 of the Atomic Energy Act of 1954, as amended, provides for criminal sanctions for willful violation of, attempted violation of, or conspiracy to violate, any regulation issued under sections 161b, 161i, or 161o of the Act. For purposes of section 223, all the regulations in part 37 are issued under one or more of sections 161b, 161i, or 161o, except for the sections listed in paragraph (b) of this section.

§ 37.109(b)

The regulations in part 37 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§ 37.1, 37.3, 37.5, 37.7, 37.9, 37.11, 37.13, 37.107, and 37.109.

EXPLANATION:

Anyone who willfully violates, attempts to violate or conspires to violate the regulations can be criminally prosecuted.

QUESTIONS/ANSWERS:

None. The NRC [Enforcement Manual](#) is the implementing guidance for the NRC enforcement program. For additional information on the Manual and links to related documents, click on <http://www.nrc.gov/about-nrc/regulatory/enforcement/guidance.html#manual>.

The Manual provides guidance consistent with the NRC [Enforcement Policy](#), which sets forth the general principles governing the enforcement program. For additional information on the Enforcement Policy and links to related documents, click on <http://www.nrc.gov/about-nrc/regulatory/enforcement/enforce-pol.html>.

Appendix A to Part 37 - Category 1 and Category 2 Radioactive Materials

Table 1 — Category 1 and Category 2 Radioactive Materials Thresholds¹

Radioactive material	Category 1 (TBq)	Category 1 (Ci)	Category 2 (TBq)	Category 2 (Ci)
Americium-241	60	1,620	0.6	16.2
Americium-241/Be	60	1,620	0.6	16.2
Californium-252	20	540	0.2	5.40
Cobalt-60	30	810	0.3	8.10
Curium-244	50	1,350	0.5	13.5
Cesium-137	100	2,700	1	27.0
Gadolinium-153	1,000	27,000	10	270
Iridium-192	80	2,160	0.8	21.6
Plutonium-238	60	1,620	0.6	16.2
Plutonium-239/Be	60	1,620	0.6	16.2
Promethium-147	40,000	1,080,000	400	10,800
Radium-226	40	1,080	0.4	10.8
Selenium-75	200	5,400	2	54.0
Strontium-90	1,000	27,000	10	270
Thulium-170	20,000	540,000	200	5,400
Ytterbium-169	300	8,100	3	81.0

The terabecquerel (TBq) values are the regulatory standard. The curie (Ci) values specified are obtained by converting from the TBq value. The curie values are provided for practical usefulness only.

¹Calculations Concerning Multiple Sources or Multiple Radionuclides

The "sum of fractions" methodology for evaluating combinations of multiple sources or multiple radionuclides is to be used in determining whether a location meets or exceeds the threshold and is thus subject to the requirements of this part.

I. If multiple sources of the same radionuclide and/or multiple radionuclides are aggregated at a location, the sum of the ratios of the total activity of each of the radionuclides must be determined to verify whether the activity at the location is less than the category 1 or category 2 thresholds of Table 1, as appropriate. If the calculated sum of the ratios, using the equation below, is greater than or equal to 1.0, then the applicable requirements of this part apply.

II. First determine the total activity for each radionuclide from Table 1. This is done by adding the activity of each individual source, material in any device, and any loose or bulk material that contains the radionuclide. Then use the equation below to calculate the sum of the ratios by inserting the total activity of the applicable radionuclides from Table 1 in the numerator of the equation and the corresponding threshold activity from Table 1 in the denominator of the equation. Calculations must be performed in metric values (i.e., TBq) and the numerator and denominator values must be in the same units.

R_1 = total activity for radionuclide 1

R_2 = total activity for radionuclide 2

R_N = total activity for radionuclide n

AR_1 = activity threshold for radionuclide 1

AR_2 = activity threshold for radionuclide 2

AR_N = activity threshold for radionuclide n

$$\sum_1^n \left[\frac{R_1}{AR_1} + \frac{R_2}{AR_2} + \frac{R_n}{AR_n} \right] \geq 1.0$$

EXPLANATION:

This appendix establishes the thresholds for category 1 and category 2.

QUESTIONS/ANSWERS:

See Q&As on definition of category 1 and category 2, [§ 37.5](#).