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

June 2010

Draft for Comment

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

Table of Contents

Acronyms and Abbreviations

AEA	Atomic Energy Act of 1954, as amended
AIS	Automated Information System
ALARA	as low as reasonably achievable
Am	americium
Bq	Becquerel
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
Ci	Curie
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
FCRA	Fair Credit Reporting Act
ft	feet
g	grams
HR	Human Resources
IAEA	International Atomic Energy Agency
lb	pound
LLEA	local law enforcement agency
M&D	Manufacturing and Distribution
MOU	Memorandum of Understanding
NAC	National Agency Check
NRC	U.S. Nuclear Regulatory Commission
PII	Personally Identifiable Information
RAMCQ	radioactive materials in quantities of concern
RSO	radiation safety officer
SAVE	Systematic Alien Verification for Entitlements
SGI	Safeguards Information
SGI-M	Safeguards Information – Modified Handling

Sv	Sievert
T&R	trustworthiness and reliability
TBq	Terabecquerels
TWIC	Transportation Worker Identification Credentials
UPS	United Parcel Service

DRAFT GUIDANCE FOR IMPLEMENTATION OF 10 CFR PART 37 – PHYSICAL PROTECTION OF BYPRODUCT MATERIAL - CATEGORY 1 AND CATEGORY 2 QUANTITIES OF RADIOACTIVE MATERIAL

Introduction

This document provides guidance to a licensee or applicant for implementation of Part 37, "Physical Protection of Byproduct material." specifically category 1 and category 2 quantities of radioactive material. It is intended for use by applicants, licensees, Agreement States, and U.S. Nuclear regulatory Commission (NRC) staff. This document describes methods acceptable to the NRC staff for implementing Part 37. The approaches and methods described in this document are provided for information only. Methods and solutions different from those described in this document are acceptable if they meet the requirements in Part 37. The definitions contained in § 37.5 are not included in this guidance document. Key terms are addressed under the sections pertinent to the definition.

The guidance in this document is provided in the form of questions and answers. The format within this document for each section of the regulation is as follows:

- The rule section is provided in the box at the top of the page.
- Actual rule text is provided in the 2nd box.
- A brief explanation of the rule text is provided below the rule text box.
- Questions and answers are proved after the explanation. The questions and answers are designed to provide guidance on implementation of the rule language in the 2nd box.
- The bottom of the page indicates which subpart or appendix the rule text is from.

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

§ 37.1

This part has been established to provide the requirements for the physical protection program for any licensee that is authorized to possess category 1 or category 2 quantities 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 set the security requirements for category 1 and category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: What is the purpose of Part 37?

A1: These regulations impose security requirements for the 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 increase the protection of the public against the unauthorized use of category 1 or category 2 quantities 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 radioactive material and specifically refer 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: Do Part 37 requirements apply to unsealed radioactive material as well as material sealed in a device? For example, do the requirements apply to materials possessed by a nuclear laundry or radioactive waste processor?

A3: 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 must implement these requirements if it possesses radioactive material in quantities that meet or exceed a category 2 threshold.

Q4: How does a licensee determine if Part 37 applies to them?

A4: The sum of fractions methodology, also known as the unity rule, is used to determine if Part 37 applies to a licensee because it is authorized to possess a category 1 or category 2 quantity of radioactive material. A licensee may need to implement the requirements in 10 CFR Part 37 even if it is not authorized to possess any single source or single radionuclide in excess of the category 2 thresholds. For combinations of materials (to include 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 would be required to consider all of the radioactive material authorized on the license. The following formula for the unity rule would be used to determine if a licensee is required to implement the Part 37 requirements: [(total amount of radionuclide A) ÷ (category 2 threshold of radionuclide A)] + [(total amount of radionuclide B) ÷ (category 2 threshold of radionuclide B)] + etc.....≥ 1. If the sum is greater than or equal to 1, the licensee would be authorized to possess at least a category 2 quantity of radioactive material, and the 10 CFR Part 37 requirements would apply for that license.
The Terabecquerels (TBq) thresholds need to be used in this calculation because they are the regulatory standard, therefore Curie (Ci) values for sources and material should be converted to TBq as follows: n (TBq) = N (Ci) x 0.037 TBq/Ci.

Below are several examples.

Example 1: The licensee is authorized to possess:

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

(5TBq Co-60 + 5TBq Co-60)/0.3 TBq + (20 TBq Ir-192/0.80 TBq) = 58
The sum of fractions is greater than 1, therefore, the Part 37 requirements apply to this licensee.

Example 2: The licensee is authorized to possess:

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

(3 TBq Sr-90/10 TBq) + (0.5 TBq Cs-137/1 TBq) + (0.1 TBq Am-241/0.6 TBq) = 0.97
The sum of fractions is less than 1, therefore, the Part 37 requirements do not apply to this licensee.

Example 3: The licensee is authorized to possess:

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

(3 TBq Sr-90/10 TBq) + (0.55 TBq Cs-137/1 TBq) + (0.1 TBq Am-241/0.6 TBq) = 1.02
The sum of fractions is greater than 1, therefore, the Part 37 requirements apply to this licensee.

Example 4: The licensee is authorized to possess:

- 0.5 TBq Cs-137 (unsealed source)
- 0.3 TBq Co-60 (sealed source)

(0.5 TBq Cs-137/1 TBq) + (0.3 TBq Co-60/0.6 TBq) = 1
The sum of fractions equals 1, therefore, the Part 37 requirements apply to this licensee.

For examples 1, 3, and 4, the extent to which the Part 37 requirements apply depends on the licensee's circumstances and whether an individual has unescorted access to the material and whether the material is aggregated.

The same type of calculation can be conducted to determine if a licensee actually possess a category 1 or category 2 quantity of radioactive material.

§ 37.3 Scope

§ 37.3(a)

Subpart B to this part applies to any person who, under the regulations in this chapter, is authorized to possess or use at any site or contiguous sites subject to the control by the licensee, category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section establishes which licensees are subject to Subpart B.

QUESTIONS/ANSWERS:

Q1*:* Who is covered by Subpart B?

A1: Subpart B requirements apply to any licensee authorized to possess category 1 or category 2 quantities of radioactive material. This includes a wide range of licensees, including pool-type irradiator licensees; manufacturer and distributor licensees; medical facilities with gamma knife devices; self-shielded irradiator licensees (including blood irradiators); teletherapy unit licensees; radiographers; well loggers; broad scope users; radioisotope thermoelectric generator licensees; some fixed gauge licensees; and licensees that ship or prepare for shipment category 1 or category 2 quantities of radioactive material. Depending on the quantity of radioactive material actually possessed by a licensee, it may not be necessary for a licensee to fully implement the Part 37 requirements; for additional questions on applicability see the questions on § 37.21.

§ 37.3 Scope

§ 37.3(b)

Subpart C to this part applies to any person who, under the regulations in this chapter, is authorized to possess or use at any site or contiguous sites subject to the control by the licensee, category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section establishes which licensees are subject to Subpart C.

QUESTIONS/ANSWERS:

Q1*:* Who is covered by Subpart C?

A1: Subpart C requirements apply to any licensee authorized to possess category 1 or category 2 quantities of radioactive material. This includes a wide range of licensees, including pool-type irradiator licensees; manufacturer and distributor licensees; medical facilities with gamma knife devices; self-shielded irradiator licensees (including blood irradiators); teletherapy unit licensees; radiographers; well loggers; broad scope users; radioisotope thermoelectric generator licensees; some fixed gauge licensees; and licensees that ship or prepare for shipment category 1 or category 2 quantities of radioactive material. Depending on the quantity of radioactive material actually possessed by a licensee and where it is located, it may not be necessary for a licensee to fully implement the Part 37 requirements; for additional questions on applicability see the questions on § 37.41(a).

§ 37.3 Scope

§ 37.3(c)

Subpart D applies to any person who, under the regulations of this chapter, imports, exports, transports, or delivers to a carrier for transport in a single shipment, category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section establishes which licensees are subject to Subpart D.

QUESTIONS/ANSWERS:

Q1*:* Who is covered by Subpart D?

A1: Subpart D requirements apply to any licensee that transports or delivers to a carrier for transport category 1 or category 2 quantities of radioactive material.

Q2: What transport is not covered by Part 37?

A2: 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 are originated in a foreign country, pass through the United States, and then continue on to another foreign country.

The rule does not address transport of spent fuel, except irradiated reactor fuel weighing 100 g (0.22 lb) or less in net weight of irradiated fuel, exclusive of cladding or other structural or packaging material, and that has a total external radiation dose rate in excess of 1 Sv (100 rem) per hour at a distance of 3 ft from any accessible surface without intervening shielding.

§ 37.7 Communications

§ 37.7

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 Nuclear Security, 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;

§ 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 Web site 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.

§ 37.9

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:

None for this section.

§ 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 some requirement in the regulations or the NRC can unilaterally decide to exempt a licensee from a requirement. The NRC can do so provided it is legal and there would be no hazard to people or property or harm to the common defense and security.

QUESTIONS/ANSWERS:

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

A1: The licensee needs to submit an amendment request that explains exactly what regulatory requirement from which the licensee is requesting an exemption. The licensee needs to: (1) explain why the requirement cannot be met; (2) propose compensatory measures to reduce the probability or mitigate the consequences of not meeting the specified requirement that the licensee will do as an alternative (if an alternative is proposed) or an alternative that meets the intent of the requirement and how/why the alternative will meet the intent of the regulatory requirement or why an alternative is not necessary; and (3) explain why public health and safety or the security of the material would not be undermined.

The NRC will evaluate the request and determine whether to grant the exemption. NRC cannot grant exemptions that are not authorized 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 Safeguards Information (SGI) as these are required by the Energy Policy Act of 2005 (EPAct).

§ 37.11 Specific exemptions

§ 37.11(b)

Any licensee's activities are exempt from the requirements of this part to the extent that its activities are covered under the physical protection requirements of part 73 of this chapter.

EXPLANATION:

Licensees that protect category 1 or category 2 quantities of radioactive material under a Part 73 security plan are exempt from the Part 37 requirements.

QUESTIONS/ANSWERS:

Q1: If a materials 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 reactor or fuel cycle facility.

In addition to the requirements of the materials licensee's security plan, the fuel cycle or reactor licensee may impose additional requirements to meet its security plan provisions. For example, a contract radiographer licensee who brought a source onto a reactor site to conduct radiography activities at the site may be subject to such 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 Part 50 or 70 license to possess an individual source that is at or above the category 2 threshold, such as a radiography source, 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, including access authorization, then the licensee would be exempt from the security provisions of Part 37. If the source is in an area not covered by the 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, including access authorization, then the licensee would be exempt from the Part 37 requirements.

Q3: Is irradiated fuel subject to Part 37?

A3: Irradiated fuel is not considered to be a category 1 or category 2 quantity of radioactive material even if it contains byproduct material at or above the category 2 threshold. This includes the fuel rod, fuel assembly, the cladding, etc.

However, shipments of small quantities (100 grams or less) of irradiated fuel under § 73.35 would be subject to the transportation security provisions contained in Subpart D.

Q4: Are activation products contained in or part of the reactor structure subject to Part 37?

A4: No. Activation products contained in the structure (stainless steel lining of a reactor vessel, stainless steel bolts, reactor hull, walls, etc) would not be subject to Part 37 as long as they remain an integral component of a reactor. Upon decommissioning of the reactor, the waste generated from decommissioning may be subject to Part 37 if it meets or exceeds the category 2 threshold. Shipment of components would be subject to Subpart D if the total activity met or exceeded the category 2 threshold.

Q5: Is mixed oxide fuel subject to Part 37?

A5: Mixed oxide fuel is not considered to be a category 1 or category 2 quantitiy of radioactive material.

However, shipments of small quantities (100 grams or less) of irradiated mixed oxide fuel under § 73.35 would be subject to the transportation security provisions contained in Subpart D.

§ 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.

EXPLANATION:

Self explanatory.

QUESTIONS/ANSWERS:

None for this section.

§ 37.13 Information collection requirements: OMB approval

§ 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.

Subpart B – Background Investigations and Access Control 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.

(1) Each licensee that is authorized to possess category 1 or category 2 quantities of radioactive material at a facility shall comply with the requirements of this subpart, as appropriate.

(2) Each licensee shall establish, implement, and maintain its access authorization program in accordance with the requirements of this subpart.

(3) By (**Insert date - 30 days - after the final rule is published in the *Federal Register***), each licensee that is authorized to possess a category 1 or category 2 quantity of radioactive material on (**insert the effective date of this rule**) shall submit information concerning the licensee's compliance with the requirements of this subpart to the appropriate NRC regional office specified in § 30.6.

(4) 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 category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section establishes the requirement to have an access authorization program. Licensees must provide the NRC with information on the compliance with the requirements of Subpart B within 30 days of the effective date of the final rule. Licensees newly subject to Part 37 must implement an access authorization program before taking possession of category 1 or category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: Who would be required to have an access authorization program?

A1: Any licensee that is authorized to possess category 1 or category 2 quantities of radioactive materials at a facility would need to determine whether it needs to have an access authorization program. Only those licensees that permit unescorted access to category 1 or category 2 quantities of radioactive material would be required to establish and implement an access authorization program. If a licensee implements a security plan under Subpart C or implements the provisions of Subpart D of Part 37, it will need to have an access authorization

program. This means that the access authorization program must be in place before the licensee can possess aggregated quantities of radioactive material that equal or exceed Category 2.

Q2: What does unescorted access mean?

A2: Unescorted access is defined as solitary access to category 1 or category 2 quantities of radioactive material granted to an approved individual, and includes solitary access to sufficient quantities of radioactive material such that an individual could successfully accumulate lesser quantities of material into a category 1 or category 2 quantity. This refers to an individual at the licensee's facility who has access to various locations within the licensee's facility(ies) and does not refer to the situation where a contractor might have access to the facilities of multiple licensees.

Q3: I do not currently possess category 1 or category 2 quantities of radioactive material but I am authorized to possess them. Do I need to implement an access authorization program?

A3: No. If you do not actually possess category 1 or category 2 quantities of radioactive material, you do not need to implement an access authorization program. However, you need to submit information on compliance in accordance with § 37.21(a)(3).

Q4: I plan to obtain additional radioactive material that will bring my possession quantity at or above the category 2 threshold. I am already authorized to possess a category 2 quantity of radioactive material. When do I need to implement an access authorization program?

A4: If any individual will now have unescorted access to a category 2 quantity of radioactive material, you will need to implement an access authorization program in advance of actually receiving the additional radioactive material that will cause your possession quantity to be at or above the category 2 threshold. You will need to conduct the background investigation, including fingerprinting, for anyone that will have unescorted access to a category 2 quantity of radioactive material. These individuals will need to be approved for access before the material is delivered to the facility. The licensee should also notify the NRC (appropriate NRC Region) that you will be implementing an access authorization program.

Q5: Can the access authorization program requirements be avoided if there are alternative physical controls or alternative administrative controls and training?

A5: No. The Part 37 requirements are designed to provide a defense in depth strategy for the security of radioactive material in quantities of concern. No single measure can provide the same level of protection as all security measures, in total. Therefore, each of the Part 37 requirements must be implemented.

Q6: What do I need to submit under § 37.21(a)(3)?

A6: The licensee would be required to submit information to the NRC concerning its compliance with the access authorization program requirements. The information should state whether the licensee is implementing an access authorization program. If the licensee is not implementing the access authorization program, the licensee should provide a brief statement explaining why it does not need to implement the program. For example, the licensee does not actually possess category 1 or category 2 quantities of radioactive material or that no individual at the site has unescorted access to category 1 or category 2 quantities of radioactive material.

The statement should not include details of the licensee's access authorization program or implementing procedures.

Q7: How should large companies that are licensed in multiple jurisdictions respond to the § 37.21(a)(3) requirements**?**

A7: The § 37.21(a)(3) requirements are imposed based on the license, not the company. If a company holds multiple licenses subject to the Part 37 requirements, it must respond for each license. For example, if a company holds two NRC licenses, it must respond for both licenses. If convenient, the company may submit a combined response covering both licenses, but the response must address each of the licenses. A company licensed in multiple jurisdictions must respond to each jurisdiction in which it holds a license subject to the access authorization requirements.

Q8: What should I do if I amend my license to increase the possession limit?

A8: Any applicant for a license or license amendment to possess category 1 or category 2 quantities of radioactive material at a facility would be required to establish and 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

§ 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 such that they do not constitute an unreasonable risk to public health and safety or the common defense and security.

EXPLANATION:

This section established 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 category 1 or category 2 quantities of radioactive material are trustworthy and reliable and do not constitute an unreasonable risk to the public health and safety or common defense and security.

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

§ 37.21(c)

Applicability.

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

(i) Any individual whose assigned duties require unescorted access to category 1 or category 2 quantities of radioactive material;

(ii) Vehicle drivers and accompanying individuals for road shipments of category 1 quantities of radioactive material;

(iii) Movement control center personnel for shipments of category 1 quantities of radioactive material;

(iv) Any individual whose assigned duties provide access to shipment information that is considered to be Safeguards Information-Modified Handling related to category 1 quantities of radioactive material; and

(v) Reviewing officials.

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

(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.

EXPLANATION:

This section establishes which individuals are subject to the access authorization program.

QUESTIONS/ANSWERS:

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

A1: Individuals subject to a licensee's access authorization program include anyone permitted to have unescorted access to category 1 or category 2 quantities of radioactive material. Unescorted access is defined as solitary access to category 1 or category 2 quantities of radioactive material granted to an approved individual, and includes solitary access to sufficient quantities of radioactive material such that an individual could successfully accumulate lesser quantities of material into a category 1 or category 2 quantity or the individual could exert some physical control over the material or device while he/she are alone. This refers to an

individual at the licensee's facility who has access to various locations within the licensee's facility and does not refer to the situation where a contractor might have access to the facilities of several licensees.

The access authorization program must also include reviewing officials, vehicle drivers and accompanying individuals for road shipments of category 1 quantities of radioactive material, movement control center personnel for shipments of category 1 quantities of radioactive material, and any individual whose assigned duties provide access to shipment information on category 1 quantities of radioactive material.

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

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

Q3: Can other individuals (e.g., contract physicians, physicists, laboratory staff, house-keeping, security staff, or other staff not actually using the device or material) be authorized unescorted access to a device or radioactive material in category or category 2 quantities of radioactive material?

A3: Yes. Other personnel (both licensee and non-licensee) that have job duties that require access to the room where the device or radioactive material is used or stored may have unescorted access to the material or device if the licensee has determined there is a need for them to have access to the material or device and they undergo a background investigation that meets the requirements of Subpart B.

Q4: Our radioactive material is in a room where several people have unescorted access, even though they do not work directly with the radioactive material (.e.g. custodial staff), do these individuals need to be fingerprinted?

A4: Yes. Other personnel (both licensee and non-licensee) that have job duties that require unescorted access to the room where the materials are used or stored must be fingerprinted and undergo a background investigation.

Q5: During a source disconnect, would the individual coming in to provide source retrieval services be subject to the access authorization program? What about an individual who works for another company that provides source retrieval services and the company has performed background investigations, are those checks adequate for my company?

A5: Yes, to both questions. Individuals without a trustworthiness and reliability determination would need to be escorted during source retrieval operations. A service provider licensee implementing the Part 37 requirements can provide written verification of its employee's trustworthiness and reliability to its customers. The written verification is required from the service provider licensee, which includes the name of the 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 10 CFR Part 37.

Q6: Would individuals transporting radioactive material be subject to the background investigation requirements?

A6: Individuals involved in the shipment, in particular those employed by carriers or other organizations handling shipments, may have unescorted access to the material during the shipment process. These persons may not be employees of the licensee and thus may not be under the licensee's direct control. Section 37.21(c) requires licensees subject certain classes of individuals to the access authorization program. Specifically, vehicle drivers and accompanying individuals for road shipments of category 1 quantities of radioactive material, movement control center personnel for shipments of category 1 quantities of radioactive material, and any individual whose assigned duties provide access to the SGI-M shipment information on category 1 quantities of radioactive material must be fingerprinted and undergo background investigations. Commercial drivers for category 2 quantities of radioactive material are not subject to the access authorization program.

Q7: If a licensee transports its own category 2 quantity of radioactive material, are its drivers subject to the access authorization program?

A7: Yes. If a licensee transports its own material, its employees transporting the material would be subject to the access authorization program.

Q8: Is the reviewing official subject to the access authorization program?

A8: Yes, the reviewing official is subject to the access authorization program and must undergo fingerprinting and a background investigation. See the questions on § 37.23(b) for additional information on the reviewing officials.

Q9: Can 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 category 1 or category 2 quantities of radioactive material without undergoing fingerprinting and a background investigation?

A9: 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 can escort these individuals until a background investigation has been completed.

Q10: Who is relieved from the investigation elements of the access authorization program?

A10: Certain categories of individuals would be relieved from the background investigation aspect of the access authorization program (see questions on § 37.29). Licensees do have the option to escort an individual and not make a trustworthiness and reliability determination. The escorts would need to be approved for unescorted access.

Q11: Can service providers not associated with a Manufacturing and Distribution (M&D) license be provided unescorted access to category 1 or category 2 quantities of radioactive material at a customer facility?

A11: Yes. Service provider licensees can make a trustworthiness and reliability determination for individuals that provide service at their customer's facilities. Service providers that have not been determined to be trustworthy and reliable must be escorted by a person, from the customer's facility, who is authorized to have unescorted access to the radioactive material or device containing radioactive material. See questions on § 37.31(c).

Q12: Our industry is subject to three different Federal background check programs: Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Department of Transportation (DOT) and the NRC. All three Federal agencies have different requirements, which can be very cumbersome, confusing and costly. Must licensees establish yet another background investigation program simply to comply with Part 37?

A12: No. If a licensee has a background investigation program for other activities at a site and that program also complies with the requirements of Part 37, the licensee does not need to create a separate program for the radioactive material subject to Part 37. Licensees will, however, need to document how specific elements of existing programs are used to implement each Part 37 requirement and why the licensee expects that these elements will demonstrate compliance with each requirement.

§ 37.23 Access authorization program requirements

§ 37.23(a)

Granting unescorted access authorization.

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

(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 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 being granted the unescorted access.

QUESTIONS/ANSWERS:

Q1: What additional requirements are necessary before granting an individual unescorted access to category 1 or category 2 quantities 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 necessary so the individual will have an understanding of his/her responsibilities.

§ 37.23 Access authorization program requirements

§ 37.23(b)

Reviewing officials.
(1) Each licensee shall nominate one or more individuals to be reviewing officials and shall submit the names of these individuals and their fingerprints to the NRC for a criminal history records check. The nominated individuals shall undergo the background investigation aspects that are required by § 37.25(a)(2) through (a)(9) before their names and fingerprints are submitted to the NRC. The fingerprints of the nominated 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.

(2) Reviewing officials must be required to have unescorted access to category 1 or category 2 quantities of radioactive materials or access to safeguards information, if the licensee possesses safeguards information, as part of their job duties.

EXPLANATION:

After the licensee completes the other elements of a background investigation, it must submit the nominated reviewing official's fingerprints to the NRC for the FBI criminal history records check. The NRC will approve or deny the nominated individual. The fingerprints 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.

QUESTIONS/ANSWERS:

Q1: What is the role of the reviewing official?

A1: The reviewing official makes the trustworthiness and reliability determinations for the licensee and determines who can be granted unescorted access authorization. Note that the Increased Control Fingerprinting Orders referred to a trustworthiness and reliability (T&R) official or T&R Official as the individual that made determinations on an employee's trustworthiness and reliability. Unlike the reviewing official the T&R Official did not have to be fingerprinted and was not approved by the regulator.

Q2: Who can be a reviewing official?

A2: The licensee decides who is nominated as a reviewing official. The reviewing official can be the radiation safety officer (RSO), someone from HR, or any other individual that has unescorted access to category 1 or category 2 quantities of radioactive material or access to SGI or SGI-M as part of their duties. The licensee must conduct the required background

investigation on the nominated person before submitting his or her name and fingerprints to the NRC. If the NRC approves the nominated individual, he/she can act as a reviewing official. Licensees regulated by an Agreement State would have their reviewing official approved by their Agreement State regulator and not the NRC.

Q3: Can the Human Resources (HR) Department be designated to perform the background investigations and be the repository for trustworthiness and reliability determination records? If we have a process in place can we continue to use that process? Does the RSO have to be involved?

A3: The review and/or record storage can be delegated to a licensee's HR or any other appropriate department depending on its organization. Additionally, the process used and the information previously obtained through the hiring process or another background investigation process, may be used to support a trustworthiness and reliability finding without having to re-verify the information. However, the individual responsible for the trustworthiness and reliability determinations must undergo fingerprinting and an Federal Bureau of Investigation (FBI) criminal history check, therefore the individual need to have unescorted access to category 1 or category 2 quantities of radioactive material or access to SGI as part of his or her job duties. The reviewing official must document the basis for concluding that individuals are trustworthy and reliable. The RSO does not have to be involved. However, because safety and security go hand-in-hand, the RSO is likely to be integrally involved in any decisions and implementation.

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

A4: If an individual is nominated to be a reviewing official, he or she must undergo a background investigation and be determined to be trustworthy and reliable. Additionally, the individual responsible for the trustworthiness and reliability determinations must be required to have unescorted access to category 1 or category 2 quantities of radioactive material as part of their job duties. The determination of trustworthiness and reliability may rely on the same or similar information evaluated by human resource personnel in their findings of employability. If the determination of T&R is not made by the HR staff, and the licensee is only relying on the HR staff to provide them with the information for the background check (i.e., employment history, education, and personal references), then the HR staff does not have to undergo a background investigation.

Q5: How does a licensee name an individual to be a reviewing official?

A5: Licensees need to nominate one or more individuals to be a reviewing official and submit their fingerprints to the NRC. Reviewing officials must be permitted either access to safeguards information or unescorted access to category 1 or category 2 quantities of radioactive material. The fingerprints of the nominated individual(s) 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. Before sending the nominated individual's fingerprints to the NRC, the licensee needs to conduct the rest of the elements of the background investigation. The licensee should submit one completed, legible standard fingerprint card (Form FD-258, ORIMDNRCOOOZ) for the individual nominated to be the reviewing official and who requires unescorted access to radioactive materials. The fingerprint card should be submitted to the NRC at:

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

As part of the submittal, the licensee should include a statement that the named individual has been nominated to serve as a reviewing official under § 37.23(b).

Once the NRC receives the fingerprints, the NRC will transmit the nominated reviewing official's fingerprints to the FBI. The NRC will review the individual's criminal history records received from the FBI and, if appropriate, approve the reviewing official.

Q6: How is the initial T&R determination and certification made (based on fingerprints and a criminal history record check) if the individual to be designated as the reviewing official is also the license custodian or applicant, and has unescorted access?

A6: Within the licensing process, there are screening criteria used by the reviewer to assess information regarding the applicant. The purpose of the screening criteria is to provide reasonable assurance that radioactive material will be used as intended.
Where the licensee or applicant requires unescorted access and intends to designate himself or herself as the reviewing official, the licensee or applicant shall submit fingerprints to the NRC. Once the NRC receives the fingerprints, the NRC will transmit the nominated reviewing official's fingerprints to the FBI. The NRC will review the individual's criminal history records received from the FBI and, if appropriate, approve the reviewing official. After the reviewing official is approved by the NRC, the reviewing official can then make T&R determinations for other employees who require unescorted access subject to the fingerprinting requirements.

Q7: If a licensee already has a reviewing official, can this individual serve as the reviewing official under Part 37?

A7: If the reviewing official has undergone a background investigation, including fingerprinting and approval by the NRC, he or she can serve as the reviewing official without further action. If the individual serving as the reviewing official has not undergone fingerprinting and background investigation, he or she cannot continue to serve as the reviewing official until after the background investigation has been completed and approval has been received from the NRC.

For certain licensees, the NRC may have already approved reviewing officials, either under the October 17, 2006, Orders [(EA-06-248, 71 FR 63043; October 27, 2006), (EA-06-250, 71 FR 53046; October 27, 2006), and (EA-06-249; 71 FR 62303; October 24, 2006)], under the August 21, 2006, SGI-M Orders, or under other regulatory requirements. In those cases, the reviewing official may continue to act in that capacity for an expanded set of persons. If the reviewing (or T&R) official has not had an FBI criminal records history check, he or she must be fingerprinted and receive NRC approval before making additional trustworthiness and reliability determinations.

Q8: Why must reviewing officials have unescorted access to category 1 or category 2 quantities of radioactive materials or access to safeguards information**?**

A8 The NRC believes that it is important that the individual who is making the final determination of trustworthiness and reliability for others be trustworthy and reliable themselves and have undergone the same background investigation as individuals who would be granted unescorted access, including fingerprinting and the FBI criminal records check. If the reviewing official is not fingerprinted, a gap could be created in the security program that could potentially be exploited. The NRC's Atomic Energy Act authority to collect fingerprints only applies to individuals that have unescorted access to radioactive material or access to SGI. The reviewing official must therefore have access to radioactive material or SGI for the NRC or the Agreement State to be able to require the collection of their fingerprints for submittal to NRC for processing.

§ 37.23 Access authorization program requirements

§ 37.23(b)

Reviewing officials.
(3) Reviewing officials cannot approve other individuals to act as reviewing officials.

(4) Reviewing officials nominated by the licensee and approved by the NRC are the only individuals who may make trustworthiness and reliability determinations and permit unescorted access to category 1 or category 2 quantities of radioactive materials possessed by the licensee.

(5) Reviewing officials may not make any trustworthiness and reliability determinations or permit any individual to have unescorted access until they have been approved as a reviewing official by the NRC.

EXPLANATION:

Only an NRC or Agreement State approved reviewing official may make the trustworthiness and reliability determinations that permit unescorted access to category 1 or category 2 quantities of radioactive material. Reviewing officials cannot approve other reviewing officials.

QUESTIONS/ANSWERS:

Q1: When can a reviewing official make trustworthiness and reliability determinations to permit unescorted access by employees?

A1: Only after the reviewing official has been approved by NRC or an Agreement State can he or she make trustworthiness and reliability determinations for any employee who requires unescorted access.

Q2: Can a licensee appoint multiple reviewing officials?

A2: Yes, a licensee can designate multiple individuals as reviewing officials but each reviewing official must undergo a background investigation, be nominated by the licensee, and be approved by the regulator.

Q3: Can a reviewing official approve other individuals to act as reviewing officials?

A3: No, a reviewing official cannot approve other individuals to act as a reviewing official. An approved reviewing official can conduct the other aspects of the background investigation (37.25(a)(2) – (a)(9)) for an individual that is to be nominated as a reviewing official.

§ 37.23 Access authorization program requirements

§ 37.23(b)

Reviewing officials.
(6) Individuals nominated as reviewing officials who receive a preliminary denial from the NRC have the right to complete, correct, and explain information obtained through the background investigation prior to a final adverse determination.

EXPLANATION:

A reviewing official that receives a preliminary denial has the right to complete, correct, and explain any information before a final adverse determination is made.

QUESTIONS/ANSWERS:

Q1: If the nominated reviewing official receives a preliminary denial from the NRC, what can he or she do to challenge the decision?

A1: The individual has the right to receive an explanation for the preliminary denial from NRC and to respond by providing additional information to NRC with a request to approve the nomination. See the detailed process in Annex A at the end of the Subpart B discussion

§ 37.23 Access authorization program requirements

§ 37.23(c)

Informed consent.

(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 have undergone a background investigation under the Fingerprint Orders. A signed consent must be obtained prior to any reinvestigation.

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

(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

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

EXPLANATION:

Each licensee must inform individuals that a background investigation is going to be conducted and must obtain a signed consent from the individual. The individual has the right to withdraw his or her consent.

QUESTIONS/ANSWERS:

Q1: What is informed consent?

A1: Informed consent is the authorization provided by an individual 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 the potential consequences if the individual does not agree to the background investigation. The signed consent shows that the individual understands 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.

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, licensees do not need to obtain informed consent from individuals who have already undergone a background investigation that included fingerprinting and an FBI criminal history records check, been determined to be trustworthy and reliable, and permitted unescorted access to category 1 or category 2 quantities of radioactive material under the NRC orders or the legally binding requirements issued by the Agreement States. An informed consent is necessary before starting any new background investigation. Before a reinvestigation of any currently approved individual, the licensee must obtain an informed consent.

Q3: How does a licensee obtain informed consent from an individual?

A3: The licensee should first explain the 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 would read and then sign and date.

Q4: What should a licensee do if an individual withdraws their consent?

A4: An individual may withdraw his or her consent at any time. If consent is withdrawn, the licensee cannot initiate any elements of the background investigation that were not in process at the time of the withdrawal of consent. The licensee is required to inform the individual that withdrawal of consent for the background investigation is sufficient cause for denial or termination of unescorted access authorization.

Q5: If an individual withdraws their consent and the licensee terminates the background investigation, can the individual be granted unescorted access to the material.

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

Q6: Can an individual who initially withdraws their permission and later gives permission again, be granted unescorted access.

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

§ 37.23 Access authorization program requirements

§ 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:

Each individual seeking unescorted access to category 1 or category 2 quantities of radioactive material must disclose 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. The information includes items such as employment history, education, credit history (including bankruptcies), and any arrest record. This information provides the reviewing official with a starting point for the background investigation.

Q2: The information sounds like information provided for employment. Can 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 can be used for this purpose.

Q3: What if an individual refuses to provide information or provides false information?

A3: Failure to provide the information or falsification of any information could be grounds for denial of the individual's request for unescorted access authorization or termination of access if the individual already has access. If the individual provides false information, it could be an indication that he or she is not trustworthy or reliable.

§ 37.23 Access authorization program requirements

§ 37.23(e)

Determination basis.

(1) The reviewing official shall determine whether to grant, deny, unfavorably terminate, maintain, or administratively withdraw an individual's unescorted access authorization based on an evaluation of all of the information required by this subpart. 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.

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

(3) The licensee shall document the basis for concluding whether or not there is reasonable assurance that an individual granted unescorted access to category 1 or category 2 quantities of radioactive material is trustworthy and reliable. Licensees shall maintain a list of persons currently approved for unescorted access authorization and a list of those individuals that have been denied unescorted access authorization. When a licensee determines that a person no longer requires unescorted access, the licensee shall immediately remove the person from the approved list and take measures to ensure that the individual is unable to obtain unescorted access.

EXPLANATION:

Each licensee is responsible for determining whether to grant an individual unescorted access to certain radioactive materials. The licensee shall allow only trustworthy and reliable individuals, approved in writing by the licensee, to have unescorted access to category 1 or category 2 quantities of radioactive material and devices containing that radioactive material. The T&R determination to grant an individual unescorted access to certain radioactive materials is made by the licensee's reviewing official after evaluating information gathered from all elements of the background investigation.

When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and be trusted to exercise the responsibility necessary to work 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.

QUESTIONS/ANSWERS:

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

A1: The reviewing official shall use all of the information gathered during the background investigation (see § 37.25) to make a determination that an individual is trustworthy and reliable. The reviewing official may not determine that an individual is trustworthy and reliable and grant him or her unescorted access until all of the information for the background investigation has been obtained and evaluated. The reviewing official may deny unescorted access to any individual based on any information obtained at any time during the background investigation. However, the licensee must 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 (See § 37.27(b)). 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 for what may be trustworthiness and reliability concern can be found in Annex B located at the end of the Subpart B discussion.

Q2: How will we get 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, the licensee will need to rely more on other aspects of the background investigation. 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 can be escorted until the background investigation has been completed and the individual granted 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: It is the licensee's responsibility to make trustworthiness and reliability determinations for all employees granted unescorted access. The trustworthiness and reliability determination is designed to identify past actions to help verify one's character and reputation; these past actions can provide reasonable assurance of an individual's future reliability. Some indicators that licensees should consider for what may be trustworthiness and reliability concerns can be found in Annex B.

Q5: Are you attempting to determine if employees are telling the truth? If someone has a drug and alcohol problem, does that make them unreliable?

A5: The process has been developed to provide a way for licensees to have reasonable assurance of a person's true identity and trustworthiness and reliability. Being untruthful and the abuse of alcohol or drugs are indicators that may be used to question a person's trustworthiness or reliability, but are not necessarily determinative.

Q6: How should the trustworthiness and reliability determination process for my employees be documented?

A6: The process documentation must include the basis used to develop the determination for each individual (including the criteria and supporting documentation), and the individual's name. The documentation should also include the date of the determination, and the name and signature of the person responsible for making the determination.

Q7: Please provide further clarification regarding the trustworthiness and reliability requirements in Part 37, including suggested procedures for trustworthiness and reliability determinations.

A7: To authorize an employee unescorted access to category 1 or category 2 quantities of radioactive material, a licensee must satisfy the requirements of §§ 37.25 and 37.27. It is the licensee's responsibility to make a trustworthiness and reliability determination of an employee, contractor, or other individual who would be granted unescorted access to the radioactive material or the device containing the radioactive material, and it is expected that licensees will use their best efforts to obtain the information required to conduct a background investigation to determine individuals' trustworthiness and reliability. The determination of trustworthiness and reliability may rely on the same or similar information evaluated by the licensee's human resource personnel for their findings of employability by employers. Information previously obtained during the hiring process may be used to support the determination, without having to re-verify that information.

Q8: If a licensee cannot obtain all of the information required in 37.25, can the individual be granted unescorted access?

A8: Yes. If a licensee concludes the individual should still be authorized for unescorted access based on other background check information, then the licensee can grant the individual unescorted access. However, the licensee should be prepared to provide a supporting explanation, in writing, of their efforts to obtain the necessary information and must document the determination basis for granting unescorted access. The licensee also has the option of escorting the individual and not making a trustworthiness and reliability determination.

Q9: If a licensee has determined someone to be trustworthy and reliable, and the individual later takes the material for malevolent use, what actions are expected of the licensee? What liability does the licensee assume because of their determination?

A9: The licensee is required to provide reasonable assurance that persons granted access are trustworthy and reliable, and if the licensee fails to provide that assurance, the licensee would be in violation of the Part 37 requirements, and enforcement action will be considered. Providing assurance means that the licensee has taken reasonable efforts as required by Part 37 to ascertain trustworthiness and reliability and documented those actions. If there was nothing in the background investigation that would have caused the licensee to deny access

and everything was properly documented, the licensee would not be in violation of the access authorization requirements.

If an incident occurs, the licensee is expected to implement the other elements of their documented program required by Part 37

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

A10:
A denial of unescorted access authorization is not 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 Category 1 and Category 2 quantities of material.

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

A11: Determination of the trustworthiness and reliability of foreign nationals, including students, poses special challenges. An evaluation of academic and other references (e.g., transcripts, college applications, financial aid applications, etc.), can form the basis for a trustworthiness and reliability 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 trustworthiness and reliability determination. Licensees must obtain independent corroborating information to the extent possible. The Part 37 requirements incorporate the phrase “to the extent possible” as opposed to “to the extent practical” to communicate the expectation that licensees will use their best efforts to obtain the information required. However, if obtaining such corroborative information becomes impossible, and the licensee concludes the individual should still be authorized for unescorted access based on other background investigation information, then the licensee should be prepared to provide a supporting explanation, in writing, of its efforts to obtain the necessary information.

Q12: If I decide that based on a federal criminal records history check one of my employees previously granted unescorted access should not have unescorted access to radioactive material what actions can I take?

A12: The licensee should immediately take steps to revoke the individual’s unescorted access. The licensee is ultimately responsible to determine 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 the licensee’s list of individuals who have been denied unescorted access authorization need to include all employees and contractors that have not been granted unescorted access?

A13: No. The list only needs to include those individuals for whom the licensee has made a determination to deny the individual unescorted access. The licensee should consider maintaining a list of individuals whose job duties require access to security zones, but not unescorted access. These individuals would include, for example, janitorial employees or maintenance contractors whose duties do not require unescorted access and employees or

contractors who the licensee has determined no longer require unescorted access to perform their duties.

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

A14: The licensee should check the NRC's list of escalated enforcement actions issued to individuals. The list includes individuals that 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/.

§ 37.23 Access authorization program requirements

§ 37.23(f)

Procedures.

(1) Licensees shall develop, implement, and maintain written procedures for conducting background investigations for persons who are applying for unescorted access authorization to category 1 or category 2 quantities of radioactive material.

(2) Licensees shall develop, implement, and maintain written procedures for updating background investigations for persons who are applying for reinstatement of unescorted access authorization.

(3) Licensees shall develop, implement, and maintain written procedures to ensure that persons who have been denied unescorted access authorization are not allowed unescorted access to category 1 or category 2 quantities of radioactive material.

(4) Licensees shall develop, implement, and maintain written procedures 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 procedure 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:

This section establishes the requirement to have procedures for the access authorization program. This includes procedures to conduct the initial background investigation and the reinvestigation or update of the background investigation, procedures on the method to ensure that those denied unescorted access are not allowed unescorted access, and procedures for notification of individuals denied unescorted access.

QUESTIONS/ANSWERS:

Q1: Is a licensee required to have procedures for conducting background investigations?

A1: Yes, licensees are required to develop, implement, and maintain written procedures for conducting the background investigations. Procedures must address notification of individuals denied unescorted access authorization. These procedures must also ensure that individuals who have been denied unescorted access authorization are not allowed

unescorted access to category 1 or category 2 quantities of radioactive material. (These individuals may, however, be escorted by an approved individual at the licensee's discretion.)

§ 37.23 Access authorization program requirements

§ 37.23(g)

Right to correct and complete information.

(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.

(2) If after reviewing their 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:

Licensees must provide an individual with the right to complete, correct, update, or explain anything in the record of the background investigation before the licensee makes an adverse determination that would deny the individual the right to have unescorted access to category 1 or category 2 quantities of radioactive material. This section contains information on how an individual can challenge the FBI criminal records history check.

QUESTIONS/ANSWERS:

Q1: Why must a licensee provide an individual the right to complete, correct, and explain information obtained during a background investigation before the licensee makes 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 it is necessary that the information is complete and correct. Sometimes information can be incomplete or wrong. The adverse information could be the result of identity theft or misidentification of another individual with the same or similar name. For example, an individual may have been charged with an offense of some type but the charges were later dropped, or the individual was determined to be innocent and the record was never updated to reflect this additional information.

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

A2: Yes, the individual can request clarification of any information that they believe is incorrect. For some of the information, the individual can simply provide what they believe to be the correct information to the licensee. The licensee can then consider the new information in their determination process. The licensee should verify the corrected information, if possible.

Q3: What if the incorrect information is part of a credit history?

A3: If there are errors in the credit history, the individual can provide the information to the licensee. The individual should consider contacting the appropriate credit bureaus and follow their procedures for correcting credit history records. The licensee can consider the information provided by the individual in making its final decision and would not need to wait for a corrected credit report.

Q4: What is the process for challenging criminal history records?

A4: If the individual believes that his or her criminal history records are incorrect or incomplete in any respect, he or she can initiate challenge procedures. These procedures would include direct application by the individual challenging the criminal history records to the law enforcement agency that contributed the questioned information. Or an individual may 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 through 16.34. 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 Identification Division makes any necessary changes to the individual's criminal history record.

The licensee cannot make a final adverse determination based only upon the criminal history records until the licensee receives the FBI's confirmation or correction of the record.

Q5: How long must a licensee allow for an individual to challenge the findings before making its final determination on granting unescorted access?

A5: The licensee must provide at least 10 days for an individual to initiate action to challenge the results of an FBI criminal history records check, although the licensee may allow more time. The licensee may use its own judgment for other elements of the background investigation.

§ 37.23 Access authorization program requirements

§ 37.23(h)

Records.

(1) The licensee shall retain documentation regarding the trustworthiness and reliability of individual employees for 5 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

(2) The licensee shall retain a copy of the current access authorization program procedures as a record for 5 years after the procedure is no longer needed or until the Commission terminates the license, if the license is terminated before the end of the retention period. If any portion of the procedure is superseded, the licensee shall retain the superseded material for 5 years after the record is superseded.

(3) The licensee shall retain the list of persons approved for unescorted access authorization and the list of those individuals that have been denied unescorted access authorization for 5 years after the list is superseded or replaced.

EXPLANATION:

The licensee must retain records that document the determination basis for granting an individual unescorted access. The records must be maintained for 5 years from the date the individual no longer requires unescorted access.

Licensees must retain copies of procedures for 5 years after the procedure is no longer used. The licensee must also maintain the list of individuals that have been granted unescorted access and a list of those that have been denied unescorted access. The records must be maintained for 5 years after it is no longer in use.

QUESTIONS/ANSWERS:

Q1: What access authorization records are required to be maintained?

A1: Licensees are required to retain all fingerprint and criminal history records received from the FBI, or a copy if the individual's file has been transferred. Licensees are also required to retain the written confirmation received from entities concerning a security clearance or favorably adjudicated criminal history records check and any written verifications received from service providers. The licensee must also retain a record of the determination basis (reason for granting unescorted access or denying it). The determination documentation must include the basis used to develop the determination for each individual (including the criteria and supporting documentation), the individual's name, the date of the determination, and the name and

signature of the person responsible for making the determination. The licensee must keep a copy of the information used to verify identity.

Q2: What procedures does a licensee need to keep for the access authorization program?

A2: A licensee needs to retain copies of all the procedures required to implement the access authorization program. This includes procedures for obtaining written consent, conducting the investigation and reinvestigation, correcting the record, and documenting the determination.

Q3: What type of record is necessary for the lists of individuals for unescorted access?

A3: The licensee is required to have a copy of the list of current individuals who have unescorted access to the material. The licensee is also required to keep a list of those individuals who are denied unescorted access to the material. When a list is updated, the previous list must be kept as a record for 5 years.

Q4: How long must the records be maintained?

A4: Background investigation records must be maintained for 5 years after the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material. Licensees are required to keep the list of persons approved for unescorted access authorization and the list of those individuals that have been denied unescorted access authorization for 5 years after the list is superseded or replaced. Procedures are retained for 5 years after the procedure has been replaced with a new or revised version.

Q5: If a facility closes and the license is terminated does the licensee need to keep records for an additional 5 years?

A5: Once a license is terminated for any reason, the licensee is no longer required to maintain its records for the access authorization program. The records may be destroyed. The background investigation records will likely contain personal information that would be considered to be personally identifiable information (PII). Records containing PII should be destroyed to prevent an unauthorized individual gaining access and not just tossed in the trash.

§ 37.25 Background investigations

§ 37.25(a)

Initial Investigation. Before granting an individual unescorted access to category 1 or category 2 quantities of radioactive material, licensees shall complete a background investigation of the individual seeking unescorted access authorization. The scope of the investigation must encompass at least the 10 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:

A licensee must conduct a background investigation on any individual before granting unescorted access to category 1 or category 2 quantities of radioactive material. The background investigation must go back to the individual's eighteenth birthday or at least 10 years, whichever is shorter.

QUESTIONS/ANSWERS:

Q1: How far back in time must a licensee look into a potential employee's historical information as part of the background investigation?

A1: The scope of the investigation must encompass at least the 10 years preceding the date of the background investigation or since the individual's eighteenth birthday, whichever is shorter. Licensees should look into a potential employee's history as far back, to the extent possible, as is necessary to satisfy themselves that sufficient information is available to meet their own criteria for the trustworthiness and reliability determination.

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; verification of true identity; employment history evaluation; verification of education; verification of military history, credit history evaluation; criminal history review; and character and reputation determination.

It is the licensee's responsibility to make a trustworthiness and reliability determination of an employee, contractor, or other individual who would be granted unescorted access to category 1 or category 2 quantities of radioactive material or a device containing such radioactive material. It is expected that licensees will use their best efforts to obtain the information required to conduct a background investigation to determine an individual's trustworthiness and reliability.

The background investigation is a tool to determine whether individuals are trustworthy and reliable and could be permitted unescorted access to category 1 or category 2 quantities of radioactive material. It is essential to ensure that individuals seeking unescorted access to radioactive material are 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 common defense and security.

Q3: Why is a trustworthiness and reliability determination necessary?

A3: A trustworthiness and reliability determination provides the licensee with reasonable assurance that the individual allowed unescorted access will not use the material for malicious purposes. The determination provides a basis upon which access cards and other such security access devices could be issued. This requirement goes beyond access control for radiation protection purposes, and further limits access to those individuals who have a legitimate need to access the licensed material or device.

Q4: Are these trustworthiness and reliability requirements equivalent to those used in nuclear power plants?

A4: No. Nuclear power plants have additional requirements such as 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 access will not use the material for malicious purposes, but the required investigation does provide reasonable assurance that the individual is who he or she purports to be. It also provides the licensee with tools to determine if the individual's character, reputation, and behavior are not adverse to the safe and secure operation of the licensee's facility. A background investigation can provide the licensee with a reasonable basis to determine that allowing an individual to have unescorted access to the licensed material would not constitute an unreasonable risk that the individual would commit or aid a malevolent use of radioactive materials.

§ 37.25 Background investigations

§ 37.25(a)(1)

Fingerprinting and an FBI identification and criminal history records check in accordance with § 37.27 or part 73 of this chapter;

EXPLANATION:

The licensee must ensure that fingerprints are obtained and submitted for the FBI identification and criminal history records checks of individuals that are being considered for unescorted access to category 1 or category 2 quantities of radioactive material.

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 652 of the EPAct amended Section 149 of the AEA to require fingerprinting and a 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."

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 questions for § 37.27 for more detail.

§ 37.25 Background investigations

§ 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:

The licensee must verify the identity of individuals that are being considered for unescorted access to category 1 or category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: How does a licensee verify true identity?

A1: To verify the identity of an applicant for access authorization, the employer must examine at least two identification documents presented by an applicant 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 recorded and maintained.

To satisfy this requirement, licensees can use the e-Verify tool provided by the U.S Customs and Immigration Service (CIS) at the website:

http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=6a0988e60a405110VgnVCM1000004718190aRCRD&vgnextchannel=6a0988e60a405110VgnVCM1000004718190aRCRD

or the CIS paper-based process using the I-9 form at:

http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=31b3ab0a43b5d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=db029c7755cb9010VgnVCM10000045f3d6a1RCRD

Both of these alternatives are available at no cost.

Licensees can use the CIS Systematic Alien Verification for Entitlements (SAVE) Program to verify the immigration status of employees. NRC licensees can use the system without cost on the basis of a Memorandum of Understanding (MOU) between NRC and the DHS. Agreement State licensees would have to pay a fee, normally $0.50 to $2.00 per transaction, unless the State has entered into a MOU with DHS.

Q2: What documents can be used to verify identity?

A2: Identity documents issued by a State or local government or by the Federal government, provided they contain a photograph or information such as name, date of birth, gender, height, eye color, and address. These documents include passports, drivers' licenses, ID cards issued by government entities, birth certificates, Social Security cards, and voter registration cards. For the complete list of allowable documents, see p. 4 of the I-9 form. Note that Items B 10-12 are not acceptable.

§ 37.25 Background investigations

§ 37.25(a)(3)

Employment history evaluation. Licensees shall complete an employment history evaluation. Licensees shall verify the individual's employment with each previous employer for the most recent 10 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;

§ 37.25(a)(5)

Military history verification. Licensees shall verify that the individual was in the military during the claimed period;

EXPLANATION:

The licensee must conduct an employment history evaluation on individuals that are being considered for unescorted access to category 1 or category 2 quantities of radioactive material. The evaluation would include time served in the military and time spent at an education institution such as a college or trade school.

QUESTIONS/ANSWERS:

Q1: Are you defining 10 years of employment as "uninterrupted" service, or can there be breaks in service?

A1: The licensee must go back a minimum of 10 years, unless the individual is younger than 28. For an individual younger than 28, the licensee only goes 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 10 years or more? Does the education and military history verification need to be performed for a long term employee?

A2: The licensee can use its own records of employment for an individual that has been employed with the company for over 10 years and would not need to check any previous employers. The education and military history verifications do not need to be performed, if they occurred over 10 years ago. If the education and military history verifications were performed as a part of the employment process, these checks do not need to be performed again.

§ 37.25 Background investigations

§ 37.25(a)(6)

Credit history evaluation. Licensees shall evaluate the full credit history of the individual who is applying for unescorted access authorization. A full credit history evaluation must include, but is not limited to, a review and evaluation of all of the information that is provided by a national credit-reporting agency about the individual's credit history. For individuals including foreign nationals and United States citizens who have resided outside the United States and do not have established credit history that covers at least the most recent 7 years in the United States, the licensee must document all attempts to obtain information regarding the individual's credit history and financial responsibility from some relevant entity located in that other country or countries;

EXPLANATION:

The licensee must conduct a credit check on individuals that are being considered for unescorted access to category 1 or category 2 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: What is the purpose of the credit history evaluation?

A1: The full credit history evaluation reflects the NRC's intent that all financial information available through credit reporting agencies must be obtained and evaluated as part of the trustworthiness and reliability evaluation. The credit history report provides insight into the financial stability of an individual. An individual with a poor credit history may be coerced into participating in a malicious act.

Q2: How can I evaluate the credit history of an employee who has resided abroad?

A2: The NRC recognizes that some countries may not have routinely accepted credit reporting mechanisms. Therefore, the NRC allows reviewing officials to use multiple sources of credit history to provide information about the financial record and responsibility of a foreign national or U.S. citizen who has resided abroad.

Q3: How can I obtain a credit history report for an employee or job applicant?

A3: Under the Fair Credit Reporting Act (FCRA), you must first notify the individual in writing that you are obtaining a credit report and obtain his or her consent in writing. You can then request a credit report from one or more of the private consumer reporting agencies. Employers may have other obligations under the FCRA, depending on the action taken.

Q4: What information in a credit history report is relevant to the determination of trustworthiness and reliability?

A4: The credit report verifies the name, address, and social security number of the applicant and can provide prior addresses and employment that can be used for more extensive criminal searches as well as cross-referencing employment information. The credit report also includes important information from public records, such as judgments, liens, collections, and bankruptcies. Credit reports provide a detailed history of payments, liabilities, and total debts and financial obligations

Q5: How should this information be evaluated?

A5: A credit report is typically used in addition to application information, references, or skills testing to help employers make the best, most objective decisions. Licensees should consider all other elements of the background investigation in making a decision on whether to grant unescorted access. The decision should not be made solely on the basis of a credit report. If the credit report contains information that concerns the licensee, the licensee should give the applicant an opportunity to clarify the issue.

§ 37.25 Background investigations

§ 37.25(a)(7)

Criminal history review. Reviewing officials shall obtain from local criminal justice resources the criminal history records of the individual who is applying for unescorted access authorization and evaluate the information to determine whether the individual has a record of local criminal activity that may adversely impact his or her trustworthiness and reliability. The scope of the applicant's local criminal history review must cover all residences of record for the 10-year period preceding the date of the application for unescorted access authorization;

EXPLANATION:

The licensee must conduct a local criminal history review for the past 10 years.

QUESTIONS/ANSWERS:

Q1: How far back must the criminal history record checks go? Can the NRC provide guidance on what types of criminal history information should be considered when granting unescorted access?

A1: The local criminal history records check is used to evaluate whether the individual has a record of criminal history that may compromise his or her trustworthiness and reliability. The criminal history records check provides information on all arrests since the individual's 18th birthday. A criminal history found during the local criminal history check would not automatically indicate unreliability or lack of trustworthiness of the employee. The licensee should consider how recent the criminal activity was and the nature of the criminal activity in determining an individual's trustworthiness and reliability.

Q2: It is not legal in my local jurisdiction to perform a local criminal history records check. Can I make a T&R determination without a local criminal background check?

A2: Licensees in some jurisdictions may not have authority to perform local criminal background checks. If local laws do not allow a licensee to perform a local criminal history records check, the licensee may make a T&R determination utilizing criminal history records information available from state or federal sources. The licensee needs to document the local government's prohibition of criminal history records investigations.

§ 37.25 Background investigations

§ 37.25(a)(8)

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. 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:

The licensee must conduct a reference check to obtain information on the character and reputation of the individual.

QUESTIONS/ANSWERS:

Q1: What constitutes a character and reputation determination?

A1: 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 should 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: 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?

A2: Any action, behavior, or conduct that is not dishonest or deceitful, not a conflict of interest or otherwise unethical, or not a violation of any law should not be considered relevant to an individual's trustworthiness or reliability. This category should not include 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.

Q3: This subsection provides that "[r]eference 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?

A3: No. A licensee may contact family members but the information should be limited to verification of other information or obtaining additional contact names.

§ 37.25 Background investigations

§ 37.25(a)(9)

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)(10)

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, the licensee shall:

(i) Document the refusal, unwillingness, or inability in the record of investigation; and

(ii) Obtain a confirmation of employment, educational enrollment and attendance, or other form of engagement claimed by the individual from at least one alternate source that has not been previously used.

EXPLANATION:

Licensees must try to obtain independent information beyond that provided by the individual. If an entity refuses or fails to provide any information, the licensee must document the situation and must obtain confirmation of the information from another source.

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, and family members.

The NRC understands that simple verbal confirmations of past employment and timeframe may be all the information a past 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.

Q2: What should a licensee 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, the licensee would be required to document the refusal, unwillingness, or inability to respond in the record of investigation. The licensee would then need to obtain confirmation from at least one alternate source that has not been previously used.

Often past employers are hesitant to say anything about a past employee for fear of being sued. If the licensee receives any input from a former employer or other reference (or even if they refuse comment), the licensee should document the conversation and take notes about what the former employer said. If attempts to contact the reference fail after several tries, the licensee 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. If the entity refusing to confirm the individual's information is an educational institution, it may indicate that further review is necessary for the individual.

§ 37.25 Background investigations

§ 37.25(b)

Grandfathering. Individuals who have been determined trustworthy and reliable for unescorted access to category 1 or category 2 quantities of radioactive material under the Fingerprint Orders do not need to meet the background investigation elements in this subpart until the 10-year re-investigation.

EXPLANATION:

Individuals that have been granted unescorted access to category 1 or category 2 quantities of radioactive material under the Fingerprint orders are grandfathered and do no need to be investigated until their 10-year reinvestigation.

QUESTIONS/ANSWERS:

Q1: If a licensee has approved individuals for unescorted access under a Fingerprinting Order, does the licensee need to conduct a new background investigation?

A1: No. The licensee does not need to conduct a new background investigation for those employees who were determined to be trustworthy and reliable and were granted unescorted access to category 1 or category 2 quantities of radioactive material or access to SGI under the Fingerprint Orders issued by the NRC or by the legally binding requirements issued by the Agreement States. These individuals are considered to be grandfathered and do not need to meet the new requirements. However, the individuals will need to undergo a reinvestigation 10 years after the initial determination and that background investigation would need to meet the requirements for the reinvestigation.

Q2: If a licensee currently has employees who have unescorted access to materials that have not been determined to be trustworthy and reliable, can the employee continue to have unescorted access until they are approved or denied based on the results of their fingerprints and background investigation elements?

A2: No. Once Part 37 is effective, no one may have unescorted access until fingerprinted and approved by the reviewing official based upon a review of the background investigation information required in § 37.25

Q3: Do you have grandfather provisions for those who are long-term employees regarding trustworthiness and reliability?

A3: No. Long-term employees are not automatically grandfathered unless they have previously undergone a background investigation as discussed in Q&A1 above or fall under one of the categories of individuals granted relief from elements of the background investigation. See questions on § 37.29 for additional information on who can be relieved from fingerprinting.

§ 37.25 Background investigations.

§ 37.25(c)

Reinvestigations. Licensees shall conduct a criminal history update and credit history reevaluation every 10 years for any individual with unescorted access to category 1 or category 2 quantities of radioactive material. The reinvestigations must be completed within 10 years of the date on which these elements were last completed and must address the 10 years following the previous investigation.

EXPLANATION:

Every 10 years, a licensee shall reinvestigate individuals that have been granted unescorted access to category 1 or category 2 quantities of radioactive material. The reinvestigation, at a minimum shall consist of the criminal history check and credit history check.

QUESTIONS/ANSWERS:

Q1: How frequently is a reinvestigation required?

A1: A reinvestigation is required every 10 years to help maintain the integrity of the access authorization program. This is necessary because an individual's financial situation or 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 includes the local criminal history review and credit history check, but need not include identification through fingerprinting, 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 or credit history, 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.

§ 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)(1)

General performance objective and requirements.

(1) Except for those individuals listed in § 37.29, 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:

This section establishes that the licensee shall fingerprint everyone that is considered for unescorted access to category 1 or category 2 quantities of radioactive material and that the fingerprints shall be transmitted to the Commission. The information received from the FBI is to be used in making the decision to grant or deny unescorted access.

QUESTIONS/ANSWERS:

Q1: Can the licensee 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 states 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.”

§ 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)(2)

General performance objective and requirements.

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

(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:

(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

(ii) The previous access was terminated under favorable conditions.

(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 or access to safeguards information 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).

(5) Licensees shall review the criminal history records as part of the trustworthiness and reliability evaluation for each individual seeking unescorted access authorization to category 1 or category 2 quantities of radioactive material.

(6) 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 or access to Safeguards Information.

EXPLANATION:

This section establishes the general performance objective for criminal history records. Licensees are required to inform individuals what the fingerprints will be used for and how the individual can revise or explain the record. Licensees would not be required to refingerprint an individual who is being reinstated after an absence of less than a year, if the individual's previous access was terminated under favorable conditions. Fingerprints are not necessary if the individual has been granted unescorted access by another licensee and the file is transferred.

Licensees are to only use the criminal history records as part of the determination for unescorted access ort access to SGI.

QUESTIONS/ANSWERS:

Q1: Is a licensee obligated to tell an individual why they are being fingerprinted?

A1: Yes. A licensee must inform the individual that their fingerprints will be used to conduct a criminal history record check.

Q2: How should a licensee inform the individual?

A2: The licensee may inform the individual verbally or in writing. The licensee can have the individual sign an acknowledgement form. See also questions on § 37.23(c).

Q3: Should a licensee inform the individual of the procedure for revising the record or adding explanations to the record?

A3: Yes. The licensee must inform the individual of the right to correct the record. See also questions on § 37.23(c).

Q4: If an employee that had unescorted access quits their job and then returns, does the licensee need to fingerprint the individual again?

A4: If the employee has been gone for 365 days or less and left under favorable conditions and had previously undergone fingerprinting and an FBI criminal history records check, the individual would not need to be fingerprinted again. If the individual's unescorted access had been terminated for cause, then the individual would need to be fingerprinted again.

Q5: Does a licensee need to obtain fingerprints of service providers and other individuals that have been granted unescorted access by the service provider or other licensee?

A5: No. A licensee does not need to obtain fingerprints of individuals employed by a service provider or other company, if the service provider meets the requirements of Part 37. Individuals from these service provider licensees, who are providing service 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 may already have made its own determination of trustworthiness and reliability for its service personnel, the service provider licensee can provide its customers with certification of an individual's trustworthiness and reliability for being granted unescorted access. The service provider's program must meet the requirements of Subpart B of Part 37.

Q6: Can I use information obtained as part of a criminal history records check for other purposes?

A6: No. The licensee can only use the information to determine suitability for either access to SGI or unescorted access to category 1 or category 2 quantities of radioactive material.

§ 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(b)

Prohibitions.

(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:

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

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

(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:

This section prohibits the licensee from using information from the FBI as the sole justification for a denial when that information involves: 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 the dismissal of the change or an acquittal. The licensee is also prohibited from using the information in a manner that would infringe on the individual's rights under the First Amendment to the Constitution or would discriminate on the basis of race, religion, national origin, gender, or age.

QUESTIONS/ANSWERS:

Q1: Why can't a licensee base a final determination to deny an individual unescorted access authorization solely on the information received from the FBI 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.

A1: Taking action on an incomplete record might unfairly penalize the individual. It is possible that the charges may have been dropped or the individual may have been determined to be innocent and the record was never updated to reflect the additional information.

§ 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(c)

Procedures for processing of fingerprint checks.

(1) For the purpose of complying with this subpart, licensees shall use an appropriate method listed in § 37.7 to submit to the Office of Administration, Division of Facilities and Security, Mail Stop TWB-05 B32M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0012, 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 (301) 415-7232, 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.

(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 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.)

(3) The NRC 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:

This section establishes the procedures for submitting fingerprints to the NRC for processing. Data received from the FBI will be forwarded to the licensee.

QUESTIONS/ANSWERS:

Q1: Where does a licensee submit the fingerprints for processing?

A1: Under the EPAct, licensees 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 10 CFR 37.29, the licensee would not need to submit the individual's fingerprints to the NRC. A completed fingerprint card (form FD-258) should be sent to:

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

Q2: I was only provided a few fingerprint cards, where can I get more?

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 (301) 415-7232, or by e-mail to forms@nrc.gov.

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

A3: Licensees need to include the following information on each card:
a. Last name, first name, middle name
b. Signature of person being fingerprinted
c. Residence of person being fingerprinted (i.e., State)
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 (Only SSN, no passport numbers etc.)
k. Date of birth
l. Place of birth
m. Sex
n. Race (e.g., A – Asian or Pacific Islander, B – Black, I – American Indian or Alaskan Native, U – Unknown, 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, XXX - Unknown)
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 (e.g. CA-123456).

Incomplete fingerprint cards will not be processed and will be returned to the licensee.

Q4: I was able to get more fingerprint cards from my local law enforcement agency, can I use those instead?

A4: No. Cards from other sources cannot be used because of problems that have been experienced with some of the cards in the past.

Q5: How can I make sure that my fingerprints are classifiable (readable)?

A5: There are instructions on the back of each fingerprint card on how to achieve classifiable fingerprints. Individuals that submit fingerprint cards that are not classifiable will have to submit new cards.

Q6: Who can fingerprint my employees?

A6: Licensees should have their fingerprints taken by an authorized official, such as a representative from a local law enforcement agency. An authorized official, for the purposes of taking fingerprints, could be available through private entities, contractors, or an established on-site fingerprinting program. Note that the fingerprints of the nominated 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.

With the exception of the reviewing official there is no limitation on who can take the fingerprints. However, if a licensee has fingerprints taken at a facility other than that of a recognized Federal, State, or local law enforcement agency, the licensee 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 that the name on the card matches the government issued identification.

3. Sign the block on the fingerprint card labeled "SIGNATURE OF OFFICIAL TAKING THE FINGERPRINTS."

Q7: Is there a fee associated with the NRC processing the fingerprints?

A7: The current fee to process each fingerprint card is $26.00. Additional fees may be charged by the entity taking the fingerprints. Fees for the processing of fingerprints 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) 415-7404). Combined payment for multiple applications is acceptable. 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.)

Q8: Can the NRC waive the fee for processing the fingerprints?

A8: No. The NRC cannot waive the fee for processing the fingerprints or reduce the fee. 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.

Q9: When completing the fingerprint cards, NRC Licensees should use their NRC docket number in the field "YOUR NO. OCA." Since Agreement State Licensees do not have NRC docket numbers, what should they use to complete the field?

A9: Agreement State Licensees should use their two letter State abbreviation followed by a dash and the Licensee's license number (e.g. CA-123456).

Q10: What method of payment does the NRC accept?

A10: 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 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) 415-7404. 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 Facility and Security
Mail Stop TWB-05 B32M
Attn: Criminal History Program
U.S. Nuclear Regulatory Commission
Rockville, MD. 20852

Q11: 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?

A11: The TCN number is not used for pay.gov processing. Since that field is on the pay.gov form, it was decided to use the field for individuals' names or any other identifying information. A TCN number stands for "Transaction Control Number." The TCN 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 can include the names of one or more individuals for whom payment is being made, the licensee's name and date of submittal.

Q12: Can I submit my fingerprints electronically to the NRC?

A12: Yes. Some licensees may choose to make arrangements to submit fingerprints electronically to the NRC. However, for many licensees this option may be prohibitive, due to the cost associated with the purchase of electronic fingerprinting equipment. To establish an electronic fingerprinting program with the NRC, please contact NRC's Facility Security Branch at

301-492-3531. Please note that electronic submission of fingerprints to the NRC must come directly from the licensee. Any fingerprint equipment to be used for the purposes of complying with the fingerprinting requirements must 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: http://www.fbibiospecs.org/iafis/ .

Q13: What happens to the fingerprint cards after the NRC receives them from the licensee?

A13: The NRC scans the fingerprint cards to transmit to the FBI electronically. The cards are retained and secured for approximately a month after which time they are destroyed in accordance with federal guidelines.

Q14: Why might a fingerprint card be unclassifiable?

A14: 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 (smudged, uneven, too dark or light, etc.).
4. Fingers on the card are missing or partially missing without an explanation.

To avoid rejection of fingerprints by the FBI as "unclassifiable," the person taking the prints should ensure they are of good quality and do not include any of these deficiencies, and follow the instructions on the back of the fingerprint card. Also, 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. A checklist to verify that the fingerprint impressions meet the FBI's requirements is also included.

Q15: 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 an individual's fingerprints cannot be classified based on conditions other than poor quality after multiple attempts?

A15: 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 response indicating the fingerprints could not be classified or the FBI Transaction Control Number (TCN). If the FBI is unable to classify the second submission of fingerprints, the licensee can 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 can 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, 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 can 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

Requests may also be faxed to the attention of Doreen Turner at 301-492-3448 with a cover sheet attached, or e-mailed to Doreen.turner@nrc.gov. 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 do not occur often, and should take notice that Step 4 may only occur 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 or other property

§ 37.29

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)

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(b)

A Member of Congress;

§37.29(c)

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(d)

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

§ 37.29(e)

Federal, State, or local law enforcement personnel;

37.29(f)

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

37.29(g)

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(h)

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;

39.29(i)

Emergency response personnel who are responding to an emergency;

§ 37.29(j)

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

§ 37.29(k)

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 (e.g. National Agency Check, Transportation Worker Identification Credentials (TWIC) under 49 CFR 1572, 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, Customs and Border Patrol's Free and Secure Trade (FAST) Program) 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 5 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material;

§ 37.29(l)

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 5 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material; and

§ 37.29(m)

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 5 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

EXPLANATION:

This section lists, by category, those individuals that have been relieved from the fingerprinting criminal history records checks, and other elements of the background investigation before being granted unescorted access to category 1 or category 2 quantities of radioactive materials:

QUESTIONS/ANSWERS:

Q1: Fingerprinting and criminal history records checks are required by the AEA, what is the basis for relieving individuals from these requirements?

A1: Under section 149.b. 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: Has the NRC previously relieved individuals from the fingerprinting and criminal history records checks?

A2: Yes. The NRC has relieved certain categories of individuals from the fingerprinting and criminal history records checks in 2 separate rulemakings. The first rulemaking relieved individuals from fingerprinting and criminal history records check requirements applicable to safeguards information (71 FR 33989; June 13, 2006). The second rulemaking relieved certain individuals who are permitted unescorted access to radioactive materials from the fingerprinting, identification, and criminal history records checks (72 FR 4945; February 2, 2007). The individuals relieved from fingerprinting, identification, and criminal history records checks under that rule include Federal, State, and local officials involved in security planning; Agreement State employees who evaluate licensee compliance with security-related orders; and other government officials who may need unescorted access to radioactive materials or other property subject to regulation by the Commission as part of their oversight function.

Q3: Who is relieved from the fingerprinting and criminal history records checks for unescorted access to category 1 and category 2 quantities of radioactive material in Part 37?

A3: Part 37 provides relief from fingerprinting and criminal history records checks and other elements of the background investigation for 13 categories of individuals. These categories include those provided relief in the rulemakings mentioned in Q&A2 above and a few additional categories. These categories of individuals include the following:

- 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
- members of Congress

- an employee of a member of Congress or Congressional committee who has undergone a prior U.S. Government criminal history records check
- a governor of a State or his/her designated State employee representative
- Federal, State, or local law enforcement personnel
- State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives
- Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i. of the AEA
- 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
- Emergency response personnel who are responding to an emergency
- Commercial vehicle drivers for road shipments of category 2 quantities of radioactive material
- 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 (e.g. National Agency Check, Transportation Worker Identification Credentials (TWIC) under 49 CFR 1572, 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, Customs and Border Patrol's Free and Secure Trade (FAST) Program)
- Any individual who has an active Federal security clearance
- 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.

Q4: How can a licensee determine if an individual has undergone a previous background investigation and falls under one of the categories listed in § 37.29?

A4: For some categories of individuals, it will be obvious. For example, a police officer, NRC employee, or State employee will have identification of some sort that identifies the individual and their employer and no further checking would 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.

Q5: What type of documentation is necessary?

A5: Documentation can consist of written confirmation from the agency or employer that granted a Federal security clearance or reviewed the criminal history records check. Documentation can consist of a copy of the background investigation record.

Q6: How long must a licensee keep documentation records?

A6: A licensee must keep the records for at least 5 years after the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

Q7: Does a National Agency Check (NAC) satisfy the provisions of Part 37?

A7: If the NAC has been conducted within the past 10 calendar years and the employee can provide documentation of favorable results to the licensee's reviewing official, then this would satisfy the provisions of Part 37.

Q8: Can emergency first responders, such as police and fire department personnel, be deemed trustworthy and reliable without a background check?

A8: Officials of the NRC, state radiation-protection agencies, and local law enforcement authorities are deemed trustworthy and reliable 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.

Q9: Can properly qualified service providers be considered trustworthy and reliable and granted unescorted access to the radioactive material or devices containing the radioactive material?

A9: Yes, provided the service provider meets the requirements of Part 37. Individuals from these service provider licensees, who are providing service 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 may already have made its own determination of trustworthiness and reliability for its service personnel, the service provider licensee can provide its customers with certification of an individual's trustworthiness and reliability for being granted unescorted access. The service provider's program must meet the requirements of subpart B of Part 37.

Q10: What is meant by a commercial driver in § 37.29(j)?

A10: A commercial driver is someone who drives commercial vehicles for a living. For example, someone driving for Fed Ex or UPS would be considered to be a commercial driver. The NRC will rely on the DOT and the Transportation Security Administration 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 category 1 quantities of radioactive material would need to undergo a background investigation. An individual who works for the licensee and drives a company truck between radiography jobs would not be considered to be a commercial driver and would need to undergo a background investigation before having unescorted access to category 1 or category 2 quantities of radioactive material

Q11: If an individual falls under one of the categories listed for relief (§ 37.29), am I required to grant the individual unescorted access to the material?

A11: No. Part 37 does not authorize unescorted access to any radioactive materials or other property subject to regulation by the NRC. Rather, the rule would make clear that a licensee may permit unescorted access to certain categories of individuals otherwise qualified for access without performing a background investigation. Licensees would still need to decide whether to

grant or deny an individual unescorted access independently of this proposed provision. Any required training would need to be conducted before granting unescorted access.

§ 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:

The licensee shall establish a system for the protection of information obtained during a background investigation.

QUESTIONS/ANSWERS:

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

A1: Yes. Licensees are required to protect the information obtained during a background investigation. The collected information will likely contain PII and should only be provided to authorized individuals. Licensees would only be permitted to disclose the information to the subject individual, the individual's representative, those who have a need to know the information to perform their assigned duties to grant or deny unescorted access to category 1 or category 2 quantities of material or safeguards information, or an authorized representative of the NRC or Agreement State agency. The licensee would be required to establish and maintain a system of files and procedures to protect the information from disclosure to any unauthorized person. Background investigation documentation should be stored 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 an individual with a need to know the protected information to perform his or her assigned duties to grant or deny unescorted access to category 1 or category 2 quantities of material or safeguards information.

§ 37.31 Protection of information

§ 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 or Safeguards Information. No individual authorized to have access to the information may redisseminate the information to any other individual who does not have a need to know.

EXPLANATION:

A licensee is prohibited from sharing the personal information obtained during a background investigation to individuals other than those employees involved in the determination process for unescorted access and the subject individual and his or her representative.

QUESTIONS/ANSWERS:

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

A1: A licensee may disclose the information upon receipt of a request by the subject individual, by his or her representative, by a duly authorized representative of NRC or an Agreement State agency, or by an individual with a need for access to the information to perform an assigned duty supporting a decision on unescorted access to Safeguards Information or to the quantities of radioactive material subject to this part. For any request, the request should be in writing, should specify the nature of the information requested, and should document the requestor's need to know. When providing the requested information, the licensee should notify the requestor, in writing, that the information may not be redisseminated to any other individual without the written authorization of the subject individual and a documented need to know.

§ 37.31 Protection of information

§ 37.31(c)

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

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

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

EXPLANATION:

Information from a background investigation may be transferred to another licensee, if the individual requests that the information be transferred to another licensee. The recipient licensee must verify basic information in order to rely on the background information that is transferred.

QUESTIONS/ANSWERS:

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

A1: Yes, a licensee may transfer information from a background investigation of an individual to another licensee if the subject individual makes a written request to the licensee to transfer the information contained in his or her file and the recipient licensee documents a need to know.

Q2: If I receive background investigation information from another licensee, may I rely on that information?

A2: A licensee may rely on background investigation information transferred from another licensee if the recipient licensee documents that it has verified information such as 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.

Q3: Must a licensee re-verify T&R information obtained from another licensee or institution?

A3: No. The process used and the information previously obtained through another background check or the hiring process may be used to support a trustworthy and reliable finding without re-verifying the information, but the licensee official responsible for Part 37 background checks 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. The documentation may reference pre-existing records, but licensees will need to document how these records are used and why they are appropriate to implement each Part 37 requirement.

Q4: What type of written verification attesting to or certifying a service provider employee's trustworthiness and reliability is required from the service provider licensee?

A4: The service provider licensee must provide the service recipient licensee a written communication that at least 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.

Q5: What kinds of information about "other applicable physical characteristics" should a licensee receiving a request for redissemination of an employee's background investigation records ask the requesting licensee to verify?

A5: The licensee recipient of a request for redissemination should ask the requesting licensee to verify any obvious distinguishing characteristics that could not be easily altered and could readily confirm the identity of the subject service provider employee. 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.

§ 37.31 Protection of information

§ 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 5 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

EXPLANATION:

Licensees shall make background investigation records available for NRC inspection. Fingerprint and criminal history records must be maintained for 5 years after the individual no longer requires access to the radioactive material.

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 require a licensee to make available for examination background investigation records obtained under this subpart.

Q2: What records do I need to maintain on the background investigation?

A2: A licensee subject to Part 37 must retain all fingerprint and criminal history records (including data indicating no record) received from the FBI on an individual for the licensee's determination of the trustworthiness and reliability of that individual for unescorted access to category 1 or category 2 quantities of radioactive material. If the individual's file has been transferred to another party, the licensee must retain a copy of these records.

Q3: How long do I need to keep records on an individual?

A3: A licensee must retain records on its determination of an individual's trustworthiness and reliability for 5 years from the date the individual no longer requires unescorted access to category 1 or category 2 quantities of radioactive material.

§ 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 ensure that its entire access program is reviewed at a frequency not to exceed 12 months.

§ 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 5 years.

EXPLANATION:

Licensees need to assess the effectiveness of its access authorization program, take appropriate corrective actions, and maintain the records for 5 years.

QUESTIONS/ANSWERS:

Q 1: How should a licensee define the “effectiveness” of its access authorization program to comply with NRC requirements for program reviews?

A1: A licensee should consider several things when evaluating the continued effectiveness of its access authorization 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. Neither the licensee nor NRC can be assured of the continuing effectiveness of an access authorization program if the licensee cannot find and correct emerging or existing noncompliances. The absence of identified problems does not necessarily demonstrate the continuing effectiveness of the program. To

minimize the potential for false negatives, the licensee's program reviews must address each applicable requirement of this subpart. These reviews should identify adverse conditions, non-compliances, and root causes, and should provide corrective actions. Licensees should also follow up on the implementation of these actions and reassess their affect on the program. This follow up should be transparent and open to security-conscious critical reviews at all levels, from program staff through management. 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 frequently do licensees need to conduct a review?

A2: A review must be conducted at least every 12 months.

Q3: Must a licensee engage an outside contractor to conduct access authorization program reviews? If not, how can a licensee 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 for licensees to demonstrate compliance, the regulation does not require it. To the extent practicable, however, the licensee should avoid the situation where individuals are reviewing their own work. If the licensee has 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 the licensee's access authorization staff. If the licensee conducts activities with category 1 or category 2 quantities of radioactive material 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: Does a licensee need to report to NRC any noncompliance identified during an access authorization 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 access authorization program?"

A5: NRC would 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 length delay of several weeks in the licensee's re-evaluation of an employee's trustworthiness and reliability after receiving information from a local law enforcement agency (LLEA) about a felony arrest, or from a credit rating company of a significant deterioration in the employee's

credit history. Another example might be a licensee's failure to document the basis for determining the need to know of an unfamiliar individual making an initial request for the redissemination of personal information about a licensee or contract 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: The regulation requires the report resulting from a program review to recommend corrective actions "when appropriate." When should a licensee 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 a licensee consider as "review documentation" for the purposes of this subsection?

A7: NRC does not expect a licensee to retain rough drafts of its annual access authorization program reviews, or meeting records, or the notes of each member of a review team, but the licensee should retain its management-approved 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.

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

A8 Records need to be maintained for 5 years.

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

A9: The licensee may keep either a paper copy or an electronic copy as long as the record is legible for the entire period and can be accessed.

Annex A

Process to Challenge NRC Denials or Revocations of Approval to be a Reviewing Official

1. Policy.

This policy establishes a process for individuals whom NRC licensees nominate as reviewing officials to challenge and appeal NRC denials of their nominations or revocations of their authority as reviewing officials. Any individual nominated as a licensee reviewing official whose nomination the NRC has denied shall, to the extent provided below, be afforded an opportunity to challenge and appeal the NRC's determination.

2. Applicability.

This policy applies solely to those employees of licensees who are nominated as a reviewing official, and who are thus to be considered by the NRC for approval as a reviewing official.

3. Determination Criteria.

Determinations for approving a nominated reviewing official will be made by the NRC staff. Authority to be a reviewing official shall be denied or revoked whenever it is determined that an individual does not meet the applicable standards. Any doubt about an individual's eligibility to be a reviewing official shall be resolved in favor of the public health and safety or common defense and security and access will be denied or revoked.

4. Procedures to Challenge the Contents of Records Obtained from the FBI.

Prior to a determination by the NRC [Facilities Security Branch Chief] that an individual nominated as a reviewing official is approved or disapproved, the individual shall:

(i) Be provided the contents of records obtained from the FBI for the purpose of ensuring correct and complete information. If, after reviewing the record, an individual believes that it is incorrect or incomplete in any respect and wishes to change, correct, or update the alleged deficiency, or to explain any matter in the record, the individual may initiate challenge procedures. These procedures include either direct application by the individual challenging the record to the agency (i.e., law enforcement agency) that contributed the questioned information, or direct challenge as to the accuracy or completeness of any entry on the criminal history record to the Assistant Director, Federal Bureau of Investigation Identification Division, Washington, DC 20537-9700 (as set forth in 28 C.F.R. § 16.30 through 16.34). In the latter case, the FBI forwards the challenge to the agency that submitted the data and requests that agency to 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.

(ii) Be afforded 10 days to initiate an action challenging the results of an FBI criminal history records check (described in (i), above) after the record is made available for the individual's review. If such a challenge is initiated, the NRC Facilities Security Branch Chief may make a determination based upon the criminal history record only upon receipt of the FBI's ultimate confirmation or correction of the record.

5. Procedures to Provide Additional Information.

Prior to a determination by the NRC Facilities Security Branch Chief that an individual nominated as a reviewing official is denied or revoked, the individual shall: be afforded an opportunity to submit information relevant to the individual's trustworthiness and reliability. The NRC Facilities Security Branch Chief shall, in writing, notify the individual of this opportunity, and any deadlines for submitting this information. The NRC Facilities Security Branch Chief may make a determination whether to approve or deny the individual as a reviewing official only upon receipt of the additional information submitted by the individual, or, if no such information is submitted, when the deadline to submit such information has passed.

6. Procedures to Notify an Individual of the NRC Facilities Security Branch Chief Determination to Deny or Revoke Authority to be a Reviewing Official.

Upon a determination by the NRC Facilities Security Branch Chief that an individual nominated as a reviewing official is denied or revoked authority to be a reviewing official, the individual shall be provided a written explanation of the basis for this determination.

7. Procedures to Appeal an NRC Determination to Deny or Revoke Authority to be a Reviewing Official.

Upon a determination by the NRC Facilities Security Branch Chief that an individual nominated as a reviewing official is denied or revoked authority to be a reviewing official, the individual shall be afforded an opportunity to appeal this determination to the Director, Division of Facilities and Security. The determination must be appealed within 20 days of receipt of the written notice of the determination by the Facilities Security Branch Chief, and may either be in writing or in person. Any appeal made in person shall take place at the NRC's headquarters, and shall be at the individual's own expense. The determination by the Director, Division of Facilities and Security, shall be rendered within 60 days after receipt of the appeal.

8. Procedures to Notify an Individual of the Determination by the Director, Division of Facilities and Security, Upon an Appeal.

A determination by the Director, Division of Facilities and Security, shall be provided to the individual in writing and include an explanation of the basis for this determination. A determination by the Director, Division of Facilities and Security to affirm the Facilities Branch Chief's determination to deny or revoke an individual's authority to be a reviewing official is final and not subject to further administrative appeals.

Annex B

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 trustworthy and reliable individuals, approved in writing by the licensee, to have unescorted access to radioactive material quantities of concern and devices containing that radioactive material. The T&R determination is made by the licensee's reviewing official, based on information gathered from all elements of the background investigation.

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 whether the 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 reviewing official should consider the following factors:

1. The nature, extent, and seriousness of the conduct;
2. The circumstances surrounding the conduct, to include knowledgeable participation;
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 is 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; and
9. The likelihood of continuation or recurrence.

Each case must be judged on its own merits, and final determination remains the responsibility of the licensee. In every case, the reviewing official should 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. The reviewing official should evaluate the information collected for consistency and adequacy.
2. True identity should be evaluated by comparing applicant provided identification and personal history data to pertinent information from the background investigation, and other data sources.
3. The reviewing official should determine whether inconsistencies determined through 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, it will receive an FBI identification and criminal history record since the individual's eighteenth birthday the licensee reviewing official should evaluate that information using the guidance below.

The licensee's reviewing official 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 and the local criminal history is used in the determination of 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 determination of T&R for unescorted access to radioactive materials, which includes a review of criminal history information, must be documented to include the basis for the decision made.

Licensees shall not make a final determination solely on the basis of criminal history checks information involving an arrest more than 1 year old for which there is not information on the disposition of the case, or an arrest that resulted in dismissal of the charge or an acquittal.

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 local criminal history check does not automatically indicate unreliability or lack of trustworthiness of the employee. The licensee will have to judge the nature of the criminal activity, and recency of the criminal activity. The licensee can authorize individuals with criminal records for unescorted access to radioactive materials, based on a documented evaluation of the basis for determining that the employee was reliable and trustworthy notwithstanding his or her criminal history. Each evaluation conducted in review of criminal history and other background checks information, should be documented to include the decision making basis. At a minimum, the licensee should consider the following elements when evaluating the results of the criminal history records check:

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 revolutionist, 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 unlawfully 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 can 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 unescorted access suitability. Unescorted access suitability is not a hiring decision, and the NRC does not intend for licensees to use this guidance as such. Because a particular individual may not be suitable for unescorted access does not necessarily mean that he is not suitable for escorted access or some other position that does not involve NRC-regulated activities.

All information collected is to be considered by the licensee 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 a 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 positive finding.

It is the licensee's responsibility to make the trustworthiness and reliability determination for an employee seeking unescorted access. The trustworthiness and reliability determination is designed to identify past actions that provide reasonable assurance of an individual's future reliability. The following are some indicators in addition to the criminal history records check that licensees may want to consider for what may be a trustworthiness and reliability concern:

1. Impaired performance attributable to psychological or other disorders.
2. Conduct that warrants referral for criminal investigation or results in arrest or conviction.
3. Indication of deceitful or delinquent behavior.
4. Attempted or threatened destruction of property or life.
5. Suicidal tendencies or 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.
14. Significant behavioral changes, moodiness or depression.

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

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, testing, and calibration.

37.53 Requirements for mobile devices.

37.55 Security program review.

37.57 Reporting of events.

§ 37.41 Security program

§ 37.41(a)

Applicability.
(1) Each licensee that possesses an aggregated quantity of category 1 or category 2 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 isolate category 1 or 2 quantities of radioactive material and limit access to them in order to minimize the risk of theft, sabotage, or diversion for unauthorized use. To "isolate" this material means to keep it within licensee-established security zones, and allow access to these zones only through established access control points. In an operational sense, to have "access" is to have an ability to exercise some physical control over the material or the device containing it by entering a security zone. If access to the radioactive material is required by an individual who has not been approved for unescorted access, the non-approved individual must be escorted by an approved individual.

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

A2: The NRC considers radioactive material to be "aggregated" if an adversary could gain access to a category 2 or greater quantity by breaching a common physical barrier. "Aggregated" thus has the same meaning as "collocated" in the guidance for Increased Controls. Part 37 uses the term "aggregated" 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: How should a licensee determine whether it has an aggregated quantity of radioactive materials large enough to trigger the security requirements of Part 37?

A3: To illustrate how aggregation might work, several examples are provided.

Example 1

An oil and gas well logger is authorized to possess a total 0.4 TBq of Americium-241 (Am-241) sources in down-hole measuring devices. The company has two 0.2-TBq sources at its base of operations. The company also does logging work using Cesium-137 (Cs-137) sources. It is authorized to possess 0.6 TBq of Cs-137 in the form of two logging tools, each with a 0.3 TBq source. Even though each of these logging tools has only a category 3 quantity of Cs-137, the licensee would have to develop a security plan, because, under the sum-of-the-fractions rule, the total quantity of both Am-241 sources and Cs-137 sources equals more than one equivalent category 2 quantity of radioactive materials. In this case, the quantity of Am-241 the licensee is authorized to possess, 0.4 TBq, is two-thirds of a category 2 quantity, and the quantity of Cs-137 the licensee is authorized to possess, 0.6 TBq, is six-tenths of a category 2 quantity. The sum of these fractions, 1 and four-fifteenths, exceeds 1, and therefore requires the licensee to develop a security program. The licensee would not have to implement the security program, however, unless all the sources are aggregated–i.e., accessible to any intruder who could defeat the one physical barrier, such as a perimeter fence or locked door, controlling access to the materials. In such a case, the licensee would have three alternatives: (1) add another physical barrier, such as a locked cage or container, to isolate the aggregated material; (2) separate the material into category 3 or smaller quantities and place each behind at least one independent physical barrier; or (3) implement the security program.

If a licensee is authorized to possess a category 2 or greater quantity of radioactive materials, but doesn't possess an aggregated quantity, the security plan should indicate how the licensee keeps its materials apart. It could do this by adding a physical barrier where each quantity of material is used or stored, or moving some of the material to another location.

Example 2

A hospital system has a license to possess materials at different sites. Hospital A is authorized to possess a total of 2 TBq (54 Ci) of cesium-137, and keeps 0.4 TBq (11 Ci) at location 1, 0.7 TBq (19 Ci) at location 2, and 0.9 TBq (24 Ci) at location 3, each several miles apart. Hospital A would be required to develop a security program because its total authorization of 2 TBq (54 Ci) is more than the category 2 threshold. Hospital A would not be required to implement the security program, however, because no single location is possesses a quantity that could be aggregated to the category 2 threshold of 1TBq (27 Ci).

Example 3

Hospital B is authorized to possess 0.4 TBq (10.8 Ci) of cesium-137 at location 1, 0.5 TBq (13.5 Ci) at location 2, and 1.1 TBq (29.7 Ci) at location 3. Hospital B's total authorization is 2 TBq (54 Ci); Hospital B would be required to develop a security program for all of its locations, and implement it for location 3 if all the material at that location is aggregated within a single physical barrier, because the total quantity possessed is above the category 2 threshold of 1 TBq (27 Ci) for cesium-137. Hospital B would therefore have to add another physical barrier to isolate the aggregated material; separate the material into quantities less than category 2 quantities and place each behind at least one independent physical barrier; or implement the security program at location 3.

Q4: Must a licensee have a security program for temporary job sites?

A4: Yes. If a licensee has category 1 or category 2 quantities 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 site, however. It only means that the licensee's security plan must address the security of the licensee's category 1 or category 2 quantities of radioactive material regardless of their location, even at temporary job sites.

Additionally, when transporting radioactive material in such quantities to and from a temporary job site, the licensee must maintain access control when the transport vehicle is stopped at a hotel, restaurant, gas station, or other location.

Q5: Does Part 37 apply if a licensee has two or more sources located in the same area that, when added together, meet or exceed a category 2 threshold quantity?

A5: Yes, Part 37 applies. If there is no additional physical barrier between the sources or devices, so that an intruder would only have to defeat one barrier to gain access to a category 2 or greater quantity of radioactive material, the licensee would have to develop and implement a security program. With only one common barrier, the sources or devices would be considered aggregated. An example would be a high dose afterloader with a back up source. If the two sources were stored in the same area behind a single barrier, they would be aggregated.

Using this same example of a high-dose afterloader and backup source, the licensee would not be required to implement the security program, if the backup source is stored in a separate locked room, or in a locked device that could not be removed, such as a safe. These could be considered additional barriers.

§ 37.41 Security program

§ 37.41(a)(2)

A licensee that is authorized to possess at least a category 2 quantity of radioactive material but does not possess an aggregated quantity that equals or exceeds the category 2 threshold shall develop a security program in accordance with the requirements of this subpart. At least 90 days before a licensee aggregates radioactive material to a quantity that equals or exceeds the category 2 threshold, the licensee shall implement its security program. The licensee shall provide written notification to the NRC regional office specified in § 30.6 of this chapter that the licensee is now implementing its security program as follows:

(i) If the aggregated quantity of radioactive material fluctuates above and below the category 2 threshold more than once in a 90-day period and will continue to do so indefinitely, the licensee need only notify the NRC the first time the security program is to be implemented. This notification must inform the NRC that the licensee aggregates material at or above the category 2 threshold from time to time and that the licensee will implement the security program whenever the material is aggregated at or above the category 2 threshold. If the security program is discontinued for more than 90 days, then the licensee shall notify the NRC the next time the security program is to be implemented.

(ii) If the aggregated quantity of radioactive material does not fluctuate above and below the category 2 threshold more than once in a 90-day period, the licensee shall notify the NRC each time a previously discontinued or new security program is to be implemented.

EXPLANATION:

Each licensee that is authorized to possess a category 1 or category 2 quantity of radioactive material must develop a security program but does not need to implement the program unless the licensee has aggregated quantities that equal or exceed the category 2 threshold. A licensee must notify the NRC at least 90 days before implementing the program.

QUESTIONS/ANSWERS:

Q1: Why is the requirement for program development based on the quantity a licensee is authorized to possess, rather than the quantity actually possessed?

A1: The NRC has several reasons for basing the requirement to develop a security program on possession limits. First, a licensee authorized to possess category 2 or greater quantities of radioactive material may not have sufficient time to develop, establish, and implement a security program before being faced with an operational need to take possession of such quantities. Requiring such licensees to develop a security program in advance relieves them of some of the

time pressures- and attendant risk of error or delay–in establishing the program. Requiring program development beforehand also provides more time for identifying and training staff to prepare for the problems that can often occur during the initial implementation of any new and unfamiliar program.

Conversely, the cost of program development may also prompt licensees to consider whether they actually need to possess as much material as their licenses allow. Licensees should not be authorized to possess a greater quantity of radioactive material than they could foreseeably use without good reason. Having a possession limit greater than needed could allow insiders or other actors to covertly accumulate a sufficient quantity of radioactive materials for a malevolent purpose.

Still another reason for requiring licensees to develop security programs based on licensed possession limits is operational. For regulators and licensees, developing a new or modified security program every time a threshold quantity of radioactive material is actually possessed would make it more difficult for licensees to maintain, and regulators to enforce, a consistent and adequate level of security over time and across licensees.

Q2: What about licensees that need to possess a threshold quantity of radioactive material intermittently for short periods that are routine but not always predictable?

A2: The NRC recognizes that some licensees may not always have quantities of radioactive material that equal or exceed category 2, and may not always have a 90-day notice of the need to cross the threshold for implementing the security program. Accordingly, the requirements also include provisions to cover situations where a licensee may routinely, but not continuously, possess aggregated quantities of radioactive material at or above the category 2 threshold.

A licensee whose aggregated quantity of radioactive material fluctuates above and below the category 2 threshold more than once in a 90-day period need only notify the NRC the first time that the security program is implemented. This notice then serves to inform the NRC that the licensee will be periodically implementing the security provisions.

If the fluctuation in aggregated quantity does not reach the category 2 threshold more than once in a 90-day period, the licensee must notify the NRC each time a previously discontinued or new security program is to be implemented.

Q3: Appendix A of the rule says that the Ci values in Table 1 are rounded after conversion from the TBq values, and are provided only for information. Because the TBq values are the international regulatory standard, licensees with licenses still expressed in curie (Ci) values must convert these values to TBq to determine whether their sources are subject to Part 37. When the quantity of radioactive material in a single source closely approaches Category 2 values, and a license's authorization limits are expressed in Ci, how does a licensee use these values to determine whether Part 37 applies? Does a 16 Ci Am-241 source, for example, require development of a security program***?***

A3: The NRC has determined that the TBq, values are to be used to two significant figures. Using the example of Am-241 above, though the Category 2 limit for Am-241 is shown as 0.6 TBq, it should be interpreted as 0.60 TBq to be consistent with two significant figures. For a reported or measured 16 Ci Am-241 source activity, the measured or reported value should be converted to TBq for compliance purposes. Using two significant figures, and the conversion formula of n TBq = N (Ci) x 0.037 TBq/Ci, 16 Ci converts to 0.59 TBq, which is less than 0.60

TBq. Thus, Part 37 requirements would not apply to a single non-aggregated source with this activity.

Q4: How would fixed gauge licensees determine if the sources in their devices are considered aggregated?

A4: Sources and devices containing sources are considered aggregated if breaching a common physical security barrier would allow access to the sources or devices. For example, multiple fixed gauges in a facility where all gauges are accessible after passing through a perimeter security check point, or by breaching a perimeter fence, would be considered aggregated. However, if additional physical security barriers would prevent access to radioactive materials in quantities equal to or greater than Category 2, the sources or devices are not considered aggregated. The licensee would still need to develop a security program but would not need to implement it.

Examples of physical barriers for fixed gauges include locked enclosures such as rooms, cages, and metal lockers that completely encase the gauge and are permanently attached to some other immovable object, such as a large pipe, a storage tank, a steel beam, or a solid floor or ceiling. Examples of non-permanent physical security barriers include robust cables or chains with locks, or tamper-proof (such as one-way threaded or welded-in-place) mounting bolts. Using locks to prevent removal or disassembly of gauge mounting hardware (e.g., by passing them through mounting bolts or both the housing and mounting plates) is another example. A heavy-duty twisted steel wire cable may also be used to secure mobile devices.

§ 37.41 Security program

§ 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 section provides the general performance objective of the security program and references the sections of the regulations that must be addressed in the security program.

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: The licensee must have a security program that would 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 *immediately*. The objectives are to reduce the risk that the material will be stolen and used for unauthorized purposes, and if it is stolen, to improve the likelihood of timely recovery.

Q2: What are the key requirements of a security program?

A2: 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 if so, 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 would 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, calibration, 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.

Q3: What's the difference between "actual" and "attempted" unauthorized access? Wouldn't the same kinds of measures apply to both?

A3: Depending on the types of barriers used to establish a specific security zone, a licensee may have to have additional measures against attempted intrusions. 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, attempts may also include covert actions in preparation for an actual 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.

Q4: Can licensees use measures required for radiation safety to comply with Part 37 security requirements too?

A4: 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.

§ 37.41 Security program

§ 37.41(d)

Information submittal and notification. By (**Insert date - 30 days - after the final rule is published in the *Federal Register***), each licensee that is authorized to possess a category 1 or category 2 quantity of radioactive material on the effective date of this regulation shall submit information concerning the licensee's compliance with the requirements of this subpart to the appropriate Regional Administrator.

EXPLANATION:

Licensees must provide the NRC with information on the compliance with the requirements of subpart C within 30 days of the effective date of the final rule.

QUESTIONS/ANSWERS:

Q1: How much "information concerning compliance" must a licensee submit?

A1: The information should include a statement that the licensee has developed a security plan and that it is or is not implementing a security program, but should not include details of the program, the security plan, or implementing procedures. If the licensee is not implementing the security program, the licensee should provide a brief statement explaining why it does not need to implement the program. For example, the licensee could explain that it does not actually possess category 1 or category 2 quantities of radioactive material or the material is not aggregated.

§ 37.43 General security program requirements

§ 37.43(a)

Security plan.
(1) Each licensee subject to the requirements of this subpart shall develop a written security plan. 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:

(i) Describe the measures and strategies used to implement the requirements of this subpart;

(ii) Identify the security resources, equipment, and technology used to satisfy the requirements of this subpart;

(iii) Describe any site-specific conditions that affect implementation of Commission requirements; and

(iv) Describe the training by which individuals implementing the security program will be informed of their responsibilities and of any changes that may affect their ability to implement the security program.

EXPLANATION:

Each licensee authorized to possess category 1 or category 2 quantities of radioactive material is required to develop a written security plan. The section lists those items that must be included in the security plan.

QUESTIONS/ANSWERS:

Q1: Must licensees submit their written security plans to NRC?

A1: No. Part 37 does not require licensees to submit security plans to NRC for review or approval, and licensees should not submit their security plans to NRC. The security plan will be subject to NRC or Agreement State inspection program.

Licensees are required only to affirm in a general statement that they have developed and they are or are not implementing their security plan. This provides NRC with sufficient notice to plan the necessary inspections of licensee facilities.

Q2: What must a licensee's security plan address?

A2: The purpose of a security plan is to establish, in writing, the licensee's overall security strategy to ensure that all of the required security measures work effectively and in an integrated way for all facilities and operations where category 1 or category 2 quantities of radioactive material will be used or stored. The plan must, among other things, include a description of the measures and strategies to implement the security requirements, and must

describe any site-specific conditions that affect how the licensee will implement the requirements. For those licensees that don't have aggregated quantities, the security plan should indicate how the licensee will ensure that the material remains unaggregated.

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 clearly explain how it will implement its chosen security measures to ensure that they work together to meet the applicable performance objectives.

Under § 37.43(a), each licensee authorized to possess category 1 or category 2 quantities of radioactive material must develop a written security plan to establish the licensee's overall security strategy to ensure the integrated and effective functioning of the licensee's security program. The security plan must at a minimum describe the licensee's implementation measures and strategies, describe any site-specific conditions affecting implementation, and describe the training by which individuals implementing the program will be informed of their responsibilities and made aware of any changes that may affect their ability to implement the program. The security plan must also identify the security resources, equipment, and technology the licensee will use.

To ensure the integrated and effective functioning of the security program, the security plan must also describe a process for identifying and implementing corrective actions or compensatory measures in the event of a failure of 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," the Appendix sets forth the recommended contents of a typical security plan for the radioactive materials subject to this proposed rule. 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: 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?

A3: Part 37 does not specifically require a licensee to develop any contingency plans, but such planning should be done to be 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 develop contingency plans for ensuring the security and accountability of the radioactive material in the event of an evacuation or other emergency situation. These plans should, at a minimum, take into account particular events, such as floods and tornadoes that have an increased probability of occurring in the area where the facility or site is located. Licensees should coordinate with their local law enforcement and emergency responders for developing contingency plans.

Q4: Should the radiation safety office or officer be involved in the development or implementation of security plans and procedures?

A4: Although radiation safety officers and their staff may not be the licensee's experts in security, they should be involved in the development and implementation of security plans and procedures 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.

§ 37.43 General security program requirements

§ 37.43(a)(2)

The security plan must be reviewed and approved by the individual with overall responsibility for the security program.

EXPLANATION:

The security plan must be reviewed and approved by the individual with responsibility for the security program.

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 given the responsibility 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. This does not mean that this individual would not need to keep his or her management informed about the development and approval of the security program. The NRC would expect that the licensee's approving individual will maintain regular communication with company management as part of his or her "overall responsibility" for the security program.

§ 37.43 General security program requirements

§ 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:

(i) The revision has been reviewed and approved by the individual with overall responsibility for the security program and licensee management; and

(ii) The affected individuals are instructed on the revised plan before the changes are implemented.

EXPLANATION:

Each licensee is required to revise its security plan as necessary and to ensure that individuals are trained on the revisions.

QUESTIONS/ANSWERS:

Q1: How frequently should a licensee revise its security plan?

A1: There is no predetermined frequency for revision of the security plan. A licensee may want to revise its security plan after the completion of the annual security program review so that any recommendations are addressed in the revised plan. A licensee may need to revise its security plan if the licensee increases its possession of radioactive material, moves the location of a storage area, or alters the facility.

Q2: Who should approve revisions to the security plan?

A2: The revised security plan should be approved by the individual who has overall responsibility for the security program.

Q3: When should a licensee train its employees on the revised security plan?

A3: Licensees need to train their employees on revisions to the security plan before the revised plan is implemented.

§ 37.43 General security program requirements

§ 37.43(a)(4)

(4) The licensee shall retain a copy of the current security plan as a record until the Commission terminates the license and, if any portion of the plan is superseded, retain the superseded material for 5 years after the record is superseded.

EXPLANATION:

Copies of the current security plan must be maintained for the life of the license. Superseded copies may be discarded after 5 years.

QUESTIONS/ANSWERS:

Q1: When a licensee's possession limits are reduced to less than a Category 2 quantity, may the licensee destroy or transfer to the NRC the security documentation required by Part 37?

A1: No. The licensee is required to maintain documentation until the license is terminated by the NRC. At that time, all security documentation should be appropriately destroyed. No transfer of documentation to the NRC is necessary.

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. The licensee would need to retain a copy of the old security plan for 5 years.

§ 37.43 General security program requirements

§ 37.43(b)

Implementing procedures.
(1) The licensee shall develop and maintain written procedures that document how the requirements of this subpart and the security plan will be met.
(2) The implementing procedures and revisions to these procedures must be approved in writing by the individual with overall responsibility for the security program.
(3) The licensee shall retain a copy of the current procedure as a record until the Commission terminates the license and, if any portion of the procedure is superseded, retain the superseded material for 5 years after the record is superseded.

EXPLANATION:

Each licensee is required to have implementing procedures that are approved by the individual with responsibility for the security program. Copies of the procedures are to be maintained for the life of the license with superseded material being maintained for 5 years.

QUESTIONS/ANSWERS:

Q1: Is a licensee subject to Part 37 required to develop security procedures even if the licensee doesn't actually possess a category 2 quantity of material?

A1: No. A licensee only needs to develop security procedures if it is implementing the security program because it has aggregated quantities that meet or exceed the category 2 threshold. However, a licensee that plans on obtaining additional radioactive material or relocating currently possessed radioactive material such that the aggregated quantity meets or exceeds the category 2 threshold must implement its security program 90 days prior to obtaining or relocating the material. This would include having the procedures in place. The licensee also must notify the NRC 90 days in advance of taking such action. See also Q&A on § 37.41(b).

Q2: What must a licensee's security procedures address?

A2: Security procedures must "document how the requirements of this subpart and the security program will be met." Thus, the procedures must be designed not only to meet the individualized security needs of each site where a category 1 or category 2 quantity of radioactive material is used or stored, but to address operational issues common to all licensees' security plans. Licensees should establish written procedures for responding to events ranging 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 provisions for immediate response, for after-hours notification of LLEAs and licensee management, 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. In fact, under § 37.43(a)(3) a licensee is *required* to revise its security plan to address changing circumstances, which may in turn require conforming revisions in security procedures. Licensees are therefore encouraged to consider the need for different implementation measures and strategies to account for changing security needs. 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. This would be the same individual who approved the security plan.

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, after approval by the individual with overall responsibility for the security program. A procedure can be completely revised or partially revised to be considered superseded.

§ 37.43 General security program requirements

§ 37.43(c)

Training.

(1) Each licensee shall conduct training on the security plan to ensure that those individuals responsible for implementing the security plan possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively. The training must include instruction in:

(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;

(ii) The responsibility to report promptly to the licensee any condition that causes or may cause a violation of Commission requirements;

(iii) The responsibility 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

(iv) The appropriate response to security alarms.

(2) In determining those individuals who shall be trained on the security plan, 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 as detailed in the licensee's security plan.

(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:

(i) Review of the training requirements of paragraph (c) of this section, and any changes made since the last training;

(ii) Reports on any relevant security issues, problems, and lessons learned;

(iii) Relevant results of NRC inspections; and

(iv) Relevant results of the licensee's program review and testing and maintenance.

(4) The licensee shall maintain records of the initial and refresher training for 5 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:

This section requires the licensee to conduct initial training and annual refresher training on the security plan and lists those items that must be included in the training.

QUESTIONS/ANSWERS:

Q1: What is the purpose of the training program?

A1: The purpose of the training program is to ensure that each individual at a subject facility, as appropriate, has the requisite knowledge, skills, and abilities to support, or avoid interfering with, an effective response to any potential security emergency identified in the licensee's security plan.

Q2: What minimum elements must a training program include?

A2: Under § 37.43(c)(1), a training program must include instruction on: the licensee's security program and implementing procedures; the purpose and function of the security measures employed; the responsibility of individual employees to "report promptly" to the licensee "any condition that causes or may cause a violation of Commission requirements;" the responsibility to report promptly to both the LLEA and the licensee any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material; and the appropriate response to alarms.

The quality and comprehensiveness of a licensee's training program will be judged by the performance objective of this subsection. This objective is to "ensure that those individuals responsible for implementation of the [security] plan possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively." Thus, the minimum scope of a training program should identify these individuals, and identify and justify 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 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 to management and the LLEA. 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, calibration, and maintenance activities.

Q3: What "potential situations" involving theft, diversion, or sabotage must a licensee's training program address under § 37.43(c)(2)?

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. Members of the general public who make a one-time visit to the licensee's facility do not have to be trained beforehand. Individuals who may visit more than once but have no responsibilities for security plan implementation may also be excused from training for good cause. In such cases, a licensee would have to show that these individuals visit so infrequently, or visit a part of the facility so remote from any security zone, or from which it would be so difficult to gain access to security-sensitive equipment or operations, that the cost of training would not justify any foreseeable security benefit.

Licensees must, however, provide at least a minimal level of training to all employees and contract personnel with job responsibilities at a facility that could involve them in responding to or assisting a response to a security event. Such individuals need not receive the same level of training as individuals with responsibilities for implementing the site security plan, but the training should be sufficient in scope and depth to effectively assist security personnel to carry out their assigned responsibilities.

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: 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. No individual subject to these 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 involvement. To ensure that each individual has successfully completed the appropriate training, he or she should have passed a test or examination for each training class or course taken, and the licensee should maintain records of the individual's score and attendance. Under § 37.43(c)(4), the licensee must maintain records of the initial and refresher training for 5 years from the date of the training, and the training records must include the dates of the

training, the topics covered, a list of licensee personnel in attendance, and "related information." If tests are administered, copies of the tests administered, the passing score for each test, and the trainee's score should be maintained."

Another measure of the likelihood that a trainee will be able to carry out assigned security responsibilities is evidence that the trainee 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. Licensees are encouraged to train their personnel using such system-wide drills or table top exercises, and to notify affected LLEAs of opportunities to participate in such training.

Q6: How frequently should licensees provide refresher training?

A6: 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. A licensee should consider providing refresher training if there has been a security related event so that the employees can obtain an understanding of what happened and how to avoid the situation from recurring.

Q7: What should be included in refresher training?

A7: Refresher training needs to address reports on any security issues; lessons learned from the program review or any events; and results from any NRC inspections or the program review. In addition the licensee should include an update on the topics covered in the initial training along with any changes since the last training.

§ 37.43 General security program requirements

§ 37.43(d)

Protection of information.

(1) Except as provided in paragraph (d)(8) 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 and implementing procedures.

(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.

(3) Before granting an individual access to the security plan or implementing procedures, licensees shall:

(i) Evaluate an individual's need to know the security plan or implementing procedures; and

(ii) Complete a background investigation to determine the individual's trustworthiness and reliability. A trustworthy 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)(10). The § 37.25(a)(1) fingerprinting and criminal history records check requirements shall not be applied to those individuals who do not require unescorted access to category 1 or category 2 quantities of radioactive material.

(4) Licensees need not subject the following individuals to the background investigation elements for protection of information:

(i) The categories of individuals listed in § 37.29(a) through (m); or

(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)(10) has been provided by the security service provider.

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. 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, the licensee shall immediately remove the person from the approved list and take measures to ensure that the individual is unable to obtain the security plan or implementing procedures.

(6) When not in use, the licensee shall store their security plan and implementing procedures in a manner to prevent removal. Information stored in non-removable electronic form must be password protected.

(7) The licensee shall retain as a record for 5 years after the document is no longer needed:

(i) A copy of the information protection procedures; and

(ii) The list of individuals approved for access to the security plan or implementing procedures

(8) 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:

Licensees are required to protect the security information and only share the information with individuals that have a need to know and have undergone a background investigation (without the fingerprinting and FBI criminal history records check). A licensee must have procedures addressing the protection of information and keep a copy of the procedures for 5 years after it is no longer needed. The licensee must also keep a record of the list of individuals allowed access to the security information.

QUESTIONS/ANSWERS:

Q1: What kinds of information are licensees required to protect?

A1: Licensees are required to limit access to their security plans and implementing procedures to prevent unauthorized disclosure.

A licensee must protect information about its physical protection (security and controls) for category 1 or category 2 quantities of radioactive material. This includes but is not limited to: information describing how the radioactive material is secured from unauthorized removal or access when it is in storage; information describing how the licensee controls and maintains constant surveillance of the radioactive material when not in storage; information describing specific policies and procedures for actions to be taken by the licensee to implement the requirements of this subsection; the security plan, and combination or lock information.

Q2: Who is allowed access to this protected information?

A2: 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) – (10). These elements include: verification of identity; employment history evaluation; verification of education; verification of military history; credit history evaluation;

criminal history review; and a determination on the individual's character and reputation. In addition, the licensee must obtain independent information to corroborate that provided by the individual.

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.

Licensees may not, however, fingerprint individuals or subject them to an FBI background investigation as conditions for permitting them access to security plans or procedures. Information previously obtained during the hiring process may be used to support a licensee's determination of an individual's trustworthiness and reliability without having to re-verify that information. Licensees that have safeguards information (SGI) or safeguards information-modified handling (SGI-M) would remain subject to the more stringent information protection requirements of 10 CFR 73.21, including fingerprinting and an FBI criminal records check.

If there is any indication that the recipient would be unwilling or unable to provide proper protection for the licensee's sensitive information, the recipient should not be authorized to receive it. Licensees must ensure that individuals not authorized to receive such information do not overhear conversations relating to the substantive portions of the sensitive information.

Q3: Is anyone exempt from the background investigation elements?

A3: Yes. The same categories of individuals that have been relieved from the background investigation elements for unescorted access to the radioactive material are also exempt from the background investigation elements for access to security information. See also questions on § 37.29. These categories are as follows:

- 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
- members of Congress
- an employee of a member of Congress or Congressional committee who has undergone a prior U.S. Government criminal history records check
- a governor of a State or his/her designated State employee representative
- Federal, State, or local law enforcement personnel
- State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives
- Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under section 274.i. of the AEA
- 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
- Emergency response personnel who are responding to an emergency
- Commercial vehicle drivers for road shipments of category 2 quantities of radioactive material
- 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 (e.g. National Agency Check, Transportation Worker Identification Credentials

(TWIC) under 49 CFR 1572, 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, Customs and Border Patrol's Free and Secure Trade (FAST) Program)

- Any individual who has an active Federal security clearance
- 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.

Q4: What measures are required for adequate information protection?

A4: 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. 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:

(1) 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;

(2) Address how to protect sensitive information while in use, storage, and transit;

(3) Address the preparation, identification or marking, and transmission of documents or correspondence containing the licensee's security program information;

(4) Address how access to the licensee's security program information is to be controlled;

(5) Include methods for destruction of documents containing security program information;

(6) Include procedures for the use of automatic data processing systems containing security program information; and

(7) Address removing documents from the licensee's protected information category when they become obsolete or no longer sensitive.

Items (2) through (7) of the above list are discussed in more detail in the Qs and As below.

Q5: How should a licensee protect sensitive information while in use, storage, and transit?

A5: 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 the office. 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.

Q6: How should a licensee prepare, identify, mark, and transmit documents or correspondence containing the licensee's security program information?

A6: Licensee-generated security program information should be prepared and marked 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. Transmittals to the NRC 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.

Q7: How should a licensee control access to its security program information?

A7: Dissemination of security program information by licensees must be limited to individuals who have a "need-to-know" the information to perform their job duties, and who have been determined trustworthy and reliable in accordance with the requirements in § 37.25(a)(2) – (10). Access by licensee employees, agents or contractors may not be permitted without both an appropriate need-to-know as determined by the licensee, and an appropriate determination concerning their trustworthiness and reliability. Employees of an organization affiliated with the licensee's company, such as a parent company, may be considered as employees of the licensee for access purposes. Licensees must ensure that individuals not authorized to receive such information do not overhear conversations relating to the substantive portions of the sensitive information

Q8: What methods should a licensee use for destruction of documents containing security program information?

A8: Documents containing this information should be destroyed by 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. (Note: security program information should not be sent to recycling without being destroyed first.)

Q9: What procedures should a licensee have for the use of automatic data processing systems containing security program information?

A9: Such information may be processed or produced on an Automated Information System (AIS) provided that the user is appropriately briefed on the proper procedures while using the computer system. 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 T&R have access to the information.

Q10: When should a licensee remove documents from the licensee's protected information category when they become obsolete or no longer sensitive?

A10: Licensees are required to retain copies of the policies and procedures until the NRC terminates the license, and retain superseded portions for 5 years.

Q11: Will licensees need to handle Safeguards Information?

A11: Some licensees will be required to handle SGI-M. The security information for 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 is considered to be SGI-M and must be protected under the measures for SGI-M specified in § 73.23.

§ 37.45 LLEA coordination and notification

§ 37.45(a)

LLEA coordination.

(1) A licensee subject to this subpart shall provide information to and 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:

(i) A description of the facilities and radioactive materials subject to this subpart;

(ii) A description of the licensee's security measures that have been implemented to comply with this subpart;

(iii) 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;

(iv) A request for information about the LLEA's capabilities to provide a timely armed response taking into consideration the description of the security measures provided in paragraph (a)(1)(ii) of this section;

(v) A request to establish a written agreement with the LLEA that describes the LLEA's commitments to provide a response in accordance with this section;

(vi) A request to establish a means of direct communication with an LLEA-designated point of contact for security emergencies involving actual or attempted theft or sabotage of licensee materials;

(vii) A request that the LLEA notify the licensee whenever the LLEA's contact information changes;

(viii) A request that the LLEA notify the licensee whenever the LLEA's response capabilities become degraded or it becomes incapable of providing a timely armed response; and

(ix) A request for information about the LLEA's willingness to participate in drills and exercises.

EXPLANATION:

Each licensee is required to attempt to coordinate with the LLEA for responding to threats to the licensee's facility. The section lists the information to be provided to the LLEA.

QUESTIONS/ANSWERS:

Q1: What kinds of LLEA coordination activities are required?

A1: The coordination activities principally involve meetings and other communications to request or provide information. As discussed in more detail in the Qs & As below for this section, the licensee must notify the LLEA that it will request an armed response to any such incident, and must provide contact information and information about the facility, its radioactive materials, and the licensee's current security measures. The licensee could also offer LLEA personnel training in radiation protection.

Q2: What is the purpose of the LLEA coordination?

A2: Coordination with an LLEA is essential for ensuring an effective and efficient physical protection program. 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 onsite, but possibly also for offsite coordination to protect public health and safety, and for mitigating the potential consequences of malevolent use 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 would need to be a government entity that has the authority to make arrests and the capability to provide an armed response. In the event of an actual or attempted theft, sabotage, or diversion of radioactive material, an armed response is likely to be necessary. Adversaries could be well armed, and the small unarmed or lightly-armed private security guard service typically at byproduct material licensee sites would not be an adequate substitute for an LLEA. However, the LLEA need not be a municipal or county police force. If a hospital or 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 would also have 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 would 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. An on-site armed force can serve as the initial licensee response, but the licensee must still coordinate with an off-site LLEA. The off-site LLEA must 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: What kinds of information should a licensee provide to an LLEA for effective coordination?

A5: 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. Examples of information which could be discussed with the LLEA and incorporated into a pre-arranged response plan include, but are not limited to:

- Types and quantities of devices and radioactive material;
- 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, 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 must also request information from the LLEA concerning the LLEA's capabilities to provide a timely armed response, request a contact in order to establish a means of direct communication, and request a means of contacting the LLEA in case of an emergency. The licensee would be required to request that the LLEA enter into a written agreement with the licensee that describes the LLEA's commitments to provide a response. The licensee would be required 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.

Q6: Does the NRC require the licensee's responders to have firearms, or will non-lethal weapons suffice? Some security staff do not carry firearms, and an LLEA response might not meet the timeliness requirement.

A6: The rule does not require a licensee's security staff to be armed, nor does it prohibit licensees from arming their security staff. The requirement for an armed response is not to prevent unauthorized access, but to ensure that an LLEA will be able to respond effectively and disrupt an actual or attempted theft, sabotage, or diversion of radioactive material. Adversaries could be well armed individuals. A private security force does not substitute for a LLEA.

Q7: What should a licensee seek as an adequate LLEA response to a threat to a licensee's facility? For example, is a single officer with radio backup sufficient, or is an entire SWAT team necessary?

A7: The LLEA will respond as appropriate to the event based on the agency's understanding of the situation and 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, in the protection of the public health and safety, to mitigate potential consequences of malevolent use of radioactive material.

Q8: Can LLEAs have access to the licensee's physical protection information? What are the LLEAs responsibilities for protecting this sensitive information?

A8: LLEAs can have access to the licensee's physical protection information if the licensee determines that they have a need for the information to conduct official business. State, local, or other law enforcement authorities are members of occupational groups deemed to be trustworthy and reliable by virtue of their employment status, and these authorities handle sensitive law enforcement information routinely in the course of their operations. Thus, licensees may give their physical protection information to the coordinating LLEA without violation of NRC information protection requirements.

Q9: Would it be appropriate for a licensee to give a diagram of its facility to an LLEA?

A9: Depending on the size of the licensee's facility and the location of the at-risk material, providing a facility plan to 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.

Q10: When the licensee requests that the LLEA notify it when the LLEA's response capabilities become degraded, what kinds of degradation should the licensee ask the LLEA to report?

A10: The kind of degradation in LLEA response capabilities that licensees should ask LLEAs to report should be longer-term inadequacies of several months' duration, such as a major budget reduction or severe shortage of law enforcement personnel. Reportable degradations are not intended to cover the possibility of short term inadequacies, such as when the LLEA may have to respond to several emergencies at the same time.

Q11: If a licensee is required to have an emergency plan under 10 CFR Part 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)?

A11: Yes, if the licensee's plan calls for LLEA communication. 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, a licensee authorized to possess a quantity of radioactive material and that has an emergency

plan that complies with 10 CFR 30.32, may be presumed to comply with the requirements under § 37.45(a)(1)(vi)-(viii), if the emergency plan requests that the LLEA:

- "[E]stablish a means of direct communication with an LLEA-designated point of contact for security emergencies involving actual or attempted theft or sabotage of licensee materials;"

- "[N]otify the licensee whenever the LLEA's contact information changes;" and

- "[N]otify the licensee whenever response capabilities become degraded or incapable of providing a timely armed response."

It should be noted, however, that category 2 quantities of the radioactive materials covered by Part 37 may vary from the quantities requiring consideration of the need for an emergency plan under 10 CFR 30.72 Schedule C. If a licensee is authorized to possess no more than a category 2 quantity of cobalt-60, cesium-137, iridium-192, or promethium-147, for example, no emergency plan is required under 10 CFR 30.72 Schedule C. If a licensee is authorized to possess a category 2 quantity of americium-241, curium-244, strontium-90, or thulium-170, however, the licensee could comply with the LLEA coordination requirements of § 37.45(a)(1)(vi)-(viii) by implementing an emergency plan under 10 CFR 30.32(i). All licensees authorized to possess a category 2 quantity of any radioactive material covered by Part 37 would still have to comply with other applicable requirements of this Subpart.

Q12: Is the licensee required to keep LLEA responders trained in radiation protection?

A12: No. However, for the LLEA to know how best to respond, it helps to know something about the potential hazards of radioactive materials, and the LLEA would therefore benefit from having some radiation protection education. Licensees can invite the LLEA to attend their annual health and safety and security training sessions.

Q13: 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?

A13: The level of knowledge, experience and interest of LLEAs will be varied. The Federal government through the DHS is actively working with LLEA organizations to improve their awareness and response across a wide field of threats by providing information, training, and funds. In coordination efforts with the LLEA, the licensee's information should add to, and help reinforce, the LLEA's knowledge regarding radioactive materials, their use, and potential risks associated with their malevolent use. Licensees can invite the LLEA to attend their annual health and safety and security training sessions.

§ 37.45 LLEA coordination and notification

§ 37.45(a)(2)

The licensee shall notify the appropriate NRC regional office listed in § 30.6(a)(2) of this chapter within three business days if:

(i)The LLEA has not responded to the request for coordination within 60 days of the coordination request; or

(ii) The LLEA notifies the licensee that the LLEA does not plan to participate in coordination activities.

EXPLANATION:

If the LLEA indicates that it does not plan to participate in coordination activities or doesn't respond to the request, the licensee must contact the appropriate NRC Regional office.

QUESTIONS/ANSWERS:

Q1: Would an LLEA's decision not to coordinate put a licensee into non-compliance with these coordination requirements?

A1: No, not if the licensee has notified the NRC of the LLEA's decision not to coordinate with the licensee. 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 possibly other coinciding events within its jurisdiction, for not entering into a formal agreement 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. An LLEA's refusal to coordinate with a licensee would not by itself render a licensee's coordination activities inadequate, however. In determining the adequacy of the licensee's coordination efforts, the NRC will recognize that in an actual emergency, State and local government officials will respond to protect the health and safety of the public. Thus, if the LLEA refuses to coordinate beforehand, the licensee could still comply by making and documenting periodic good-faith efforts to elicit the LLEA's participation in planning for a timely and effective response. If the LLEA does not participate in the coordination activities, the licensee must notify the NRC.

Q3: To trigger this notification requirement, must a licensee have a written or oral statement from an LLEA stating that it does not plan to participate in coordination activities?

A3: 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.

§ 37.45 LLEA coordination and notification

§ 37.45(a)(3)

The licensee shall document its efforts to coordinate with the LLEA to provide a response to threats to the licensee's facility. The licensee's documentation must include:

(i) Dates, times, and locations of meetings with the LLEA;

(ii) Licensee personnel present;

(iii) LLEA personnel present; and

(iv) Copies of any correspondence between the licensee and LLEA.

EXPLANATION:

Each licensee must document its LLEA coordination activities.

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.

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: Using certified mail, UPS, or other third-party delivery method to document the licensee's transmittal of a coordination request would be one 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.

§ 37.45 LLEA coordination and notification

§ 37.45(a)(4)

The licensee shall coordinate with the LLEA at a frequency no greater than 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. The coordination activities shall include verification of contact information and response capabilities.

EXPLANATION:

Each licensee must coordinate with the LLEA on, at a minimum, every 12 months.

QUESTIONS/ANSWERS:

Q1: When should licensees coordinate with the LLEA concerning changes made to the facility design or operation?

A1: If possible, the licensee should notify the LLEA prior to making any changes to the facility design or operation that would adversely affect the potential vulnerability of the licensee's material. If prior coordination with the LLEA is not possible, the licensee should notify the LLEA of any such changes as promptly as possible after making them. The licensee should coordinate with the LLEA at least every 12 months even if there are no significant changes to the facility design or operation. The coordination should include a discussion of the potential consequences of any changes, as well as verifying contact information and response capabilities. LLEA response personnel should be afforded the opportunity to familiarize themselves with the facility once any design or operating changes have been made.

§ 37.45 LLEA coordination and notification

§ 37.45(a)(5)

The licensee shall notify the appropriate NRC regional office listed in § 30.6(a)(2) of this chapter within three business days after the licensee becomes aware of any applicable state or local agency requirement that an initial response to an emergency involving radioactive materials must be provided by other than armed LLEA personnel.

EXPLANATION:

A licensee must notify the NRC if it becomes aware that the LLEA initial response would be provided by other than armed personnel.

QUESTIONS/ANSWERS:

Q1: How can a licensee "become aware" of a state or local requirement that an initial response to an emergency involving radioactive materials must be provided by other than armed LLEA personnel?

A1: The licensee should ask the LLEA. A convenient time to ask could be during one of the licensee's required interactions with the LLEA to develop or maintain effective coordination of licensee and LLEA responses to a security incident.

Q2: How should a licensee notify the NRC regional office to meet this requirement?

A1: The licensee should notify the NRC regional office by letter or telephone.

(

§ 37.45 LLEA coordination and notification

§ 37.45(b)

LLEA notification for temporary job sites.

(1) At least three business days prior to beginning work at temporary job sites where the licensee will use or store category 1 or category 2 quantities of radioactive material for more than seven consecutive calendar days, the licensee shall provide advance written notification to the appropriate LLEA. Advance notification must include:

(i) An explanation that the licensee is required to provide this notification to the LLEA in accordance with this section;

(ii) An explanation that the licensee will request an armed response from the LLEA in the event of an actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material at the temporary job site;

(iii) Information on the quantities of radioactive material involved and the potential hazards associated with loss of control of the material;

(iv) Scheduled start date and expected duration of the licensee's work requiring the use or storage of category 1 or category 2 quantities of radioactive materials at the temporary job site for which this notice is provided;

(v) Address of the temporary job site, if available, or sufficient directions to allow the LLEA to determine the location of the temporary job site;

(vi) Names and contact information for licensee personnel expected to be present at the temporary job site and responsible for the security of category 1 or category 2 quantities of radioactive material;

(vii) Names and contact information for other licensee personnel to be contacted in an emergency or for additional information;

(viii) Names and contact information for the NRC Region responsible for oversight of the licensee's activities at the temporary job site that the LLEA may contact for information; and

(ix) A request that the LLEA confirm receipt of the notification.

EXPLANATION:

Each licensee that will be working at a temporary job site for more that 7 days must provide notification to the LLEA at least 3 business days in advance. The section contains the types of information that must be included in the notification.

QUESTIONS/ANSWERS:

Q1: What is the purpose of notifying LLEAs of licensees' plans to work with category 1 or category 2 quantities of radioactive materials at temporary job sites?

A1: This requirement is intended to ensure that local law enforcement officers who might be summoned to such a job site in the event of a security incident will be aware that they might be summoned, will know the potentially affected location, and will be able to reach responsible licensee representatives before the operations begin if the officers want additional information. Notification gives the LLEA essential information about the time, location, and nature of the activity so that the LLEA can be prepared to respond if necessary. Notification would also provide the LLEA an opportunity to request more information if needed. In addition, licensees must know how to request assistance from the LLEA at temporary job sites in the event of a security incident.

Q2: What are the LLEA notification requirements for work at a temporary job site?

A2: For temporary job sites (i.e., locations not specifically identified on the license for possession of radioactive materials), the rule requires licensees to provide advance written notification to the appropriate LLEA(s) at least 3 business days in advance if the licensee plans to use or store category 1 or category 2 quantities of radioactive material at the temporary job site for more than 7 consecutive calendar days. The notification would need to include such things as the purpose of the notification, timeframe and location for the temporary work, information on the quantities of radioactive material to be used or stored at the site, and contact information.

Q3: What should a licensee do if it can't identify an appropriate LLEA for a temporary job site?

A3: The NRC recognizes that may be difficult to identify an appropriate LLEA for a temporary job site, especially in the remote areas where well loggers and many industrial radiographers often have to operate. In geographically large rural counties with only a few small population centers, for example, the closest law enforcement agency may be the state police. There are also areas where several law enforcement agencies may operate, either in coordination or separately, each for different purposes. In such cases, if the licensee's local client cannot identify the appropriate LLEA with certainty, and a 911 number is not available at the temporary job site, the licensee should seek the advice of the state police. Where there are several agencies with overlapping jurisdictions, such as state police and state or federal park rangers, the licensee should seek to coordinate with the LLEA that can provide an armed response in the shortest time.

Q4: If a licensee must conduct radiography work on a pipeline, with a continually shifting location that extends through a series of LLEA jurisdictions, must the licensee notify each of these LLEAs?

A4: The licensee would be required to notify only those LLEAs in jurisdictions within which the licensee will be operating more than 7 consecutive calendar days. Thus, if the licensee spent one day in each of seven LLEA jurisdictions, for example, the licensee would not be required to notify any of them. The 7-days-at-one-site threshold for application of the LLEA notification requirement is intended to balance the need for timely LLEA awareness with the need to avoid licensee notification requirements that may be out of proportion to the security risks. Some temporary job sites may only be in use by a licensee for several days a year on short notice and at unpredictable intervals. Such circumstances make it difficult for a malevolent group to plan and execute theft, sabotage, or diversion.

Q5: What coordination with the LLEA is required for work at temporary job sites?

A5: Unlike for an LLEA with jurisdiction over a permanent job site, a licensee would not be required to coordinate in advance with the LLEA for a temporary job site. Only notification is required, and then only if the licensee expects to be at the temporary job site for more than seven consecutive calendar days. The notification requirement would not preclude a licensee from coordinating with an LLEA at a temporary job site, if the LLEA and licensee believe it would be beneficial to do so. Licensees could also coordinate with their established LLEA point of contact, who may be in the best position to communicate with another LLEA or to advise licensees on best practices.

Q6: 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?

A6: Yes. Licensees need to know how to request assistance from the LLEA at temporary job sites. Procedures following a theft or sabotage at a temporary job site should be documented as part of the licensee's security program.

§ 37.45 LLEA coordination and notification

§ 37.45(b)(2)

If an emergency or other unforeseen circumstance does not allow the licensee to provide three business days written advance notice to the LLEA, the licensee shall notify the LLEA as soon as possible via telephone, facsimile, or e-mail.

§ 37.45(b)(3)

The licensee shall maintain documentation of all temporary job site notifications sent to the LLEA and any confirmations provided by the LLEA.

EXPLANATION:

If an emergency prevents a licensee from providing 3 business day advance notice, the licensee must notify the LLEA as soon as possible.

QUESTIONS/ANSWERS:

Q1: Would a licensee be prohibited from working at a temporary job site if the licensee couldn't notify the affected LLEA(s) 3 business days in advance?

A1: No. The proposed LLEA notification requirement for temporary job site operations provides for unforeseen circumstances under which a licensee might not be able to provide 3 business days written advance notice to the LLEA. If, due to an emergency or other unforeseen circumstances, a licensee is required to work at a temporary job site for more than 7 consecutive calendar days, and is unable to provide the 3 days advance written notice to the LLEA before the licensee's trip to the site, the licensee is required to provide as much advance notice as possible by telephone, facsimile, or e-mail.

Q2: What specific kinds of documentation should a licensee maintain for temporary job site notifications and LLEA confirmations?

A2: The licensee should maintain a record copy of the written information provided in each notification required by § 37.45(b)(1) showing the date the notification was sent by the licensee. For mailed notifications, the licensee should maintain a copy of the dated letter. The licensee may choose to maintain a certified letter receipt or other similar record from the post office indicating the date each notification was mailed. For notifications delivered by a service such as FedEx or UPS, the licensee should maintain a similar record from the service provider showing the date it received the written notification document from the licensee. If the notification had to be faxed because the licensee was not notified in time to send the written notification by mail or delivery service, the licensee should maintain a copy of the fax cover sheet indicating the date and time that the licensee completed the fax transmission. For e-mailed notifications, the licensee should maintain a record copy of the e-mail showing either the text of the notification

document or that the document was attached as a file. For each notification provided by telephone, the licensee should maintain written documentation of the date, time, and name of the employee who made the call. If the licensee's notifying employee was able to speak with an LLEA official, the licensee's telephone record should also document the name of the LLEA representative who received the call. The written documentation of this representative may be used as a confirmation of the LLEA's receipt of the notification. To confirm the LLEA's receipt of each notification by other delivery methods, the licensee should maintain a copy of the fax confirmation document if provided by the fax machine, the dated delivery confirmation document provided by the delivery service, or the dated post office document confirming the LLEA's receipt of the notification by registered mail or special delivery.

§ 37.45 LLEA coordination and notification

§ 37.45(c)

Records. The licensee shall maintain records of its coordination activities with any LLEA in the development of the licensee's security plan, and copies of all documents and correspondence provided to or received from any LLEA in accordance with this section. Records of coordination activities at a temporary job site must be maintained for a period of 5 years.

EXPLANATION:

Documentation regarding coordination activities must be maintained for 5 years.

QUESTIONS/ANSWERS:

Q1: How long should a licensee maintain records of its LLEA coordination activities for licensee facilities, as opposed to temporary job sites?

A1: Consistent with the retention requirements for other types of documentation in this rule, a licensee must maintain records of LLEA coordination activities for a period of 5 years.

Q2: 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?

A2: No. Records do not need to be maintained in paper. As long as the record is legible, the licensee can keep a reproduced copy, microform copy, or electronic copy.

§ 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:

Aggregated category 1 and category 2 quantities of radioactive material must be used or stored within security zones.

QUESTIONS/ANSWERS:

Q1: What is 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 unauthorized access. "Isolation" means deterring persons, material, or vehicles from entering or leaving through other than established access control points. "Access control" means allowing only approved individuals into the security zone, and ensuring that other individuals with a need for access are escorted by approved individuals. A security zone effectively defines where the licensee will apply these isolation and access control measures. Together, they must enable the licensee to demonstrate, for the defined area, a means to detect any unauthorized access to licensed material, deliberate or inadvertent. All category 1 and category 2 quantities of radioactive material must be used or stored only within a security zone.

Q2: What is the purpose of a security zone?

A2: The purpose of security zones is to isolate and control access to category 1 or category 2 quantities of radioactive material to protect it more effectively, and to deter theft, sabotage, or diversion by providing, among other things, more time for the licensee and the LLEA to respond.

Q3: How does a security zone differ from an area established for radiation safety? Can they be the same?

A3: 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, the security zone does not have to be the same as either of these areas.

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. 10 CFR 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.

Thus, for a temporary well-logging operation within which the licensee is required by 10 CFR 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.”

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.”)

Since materials licensees are differently configured 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 a facility-by-facility basis and can change based on each facility’s operating status and security needs. The security zone may be as small as a locked cabinet, or as large as a warehouse area.

Q4: How does a permanent security zone differ from a temporary one?

A4: A permanent security zone provides isolation for the material with permanent barriers. These barriers may consist of: fences; gates; free standing walls for exterior areas; exterior or interior building walls; locked doors; locked windows; bars; or grillwork. The barriers or walls deter and delay penetration by unauthorized persons and aid detection by providing an indication of forced penetration.

Temporary security zones need not have permanent barriers at their boundaries. Isolation of the material and the people using the material 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.

§ 37.47 Security zones

§ 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:

Temporary security zones must be established as necessary.

QUESTIONS/ANSWERS:

Q1: When should a licensee establish a temporary security zone, and how?

A1: Temporary security zones would need to be established to meet transitory or intermittent operating requirements such as periods of maintenance, source delivery, source replacement, temporary storage, or the need to work at a temporary job site. A licensee could establish a security zone at a temporary job site simply by keeping the area under "direct supervision" by an approved individual(s). Similarly, when work is being done inside a temporary security zone, a licensee could meet the requirements for controlling unescorted access by having the material, people, and area within the zone under direct control of an approved individual(s) at all times.

§ 37.47 Security zones

§ 37.47(c)

Security zones must, at a minimum, allow unescorted access only to approved individuals through:

(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; or

EXPLANATION:

This section establishes the requirements for a security zone.

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 an established access control point. The continuous barrier should have no openings, other than access control points, 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.

As a best practice to provide additional delay, hinges on doors to the security zone should also be moved inside, or if the external hinges are an integral part of a metal doorframe, at least one hinge should be pinned or peened to delay removal of the door. Exposed hinge hardware such as common screws or bolts should be replaced with tamper-resistant hardware to make quick removal of the hinge difficult.

Q3: Does Part 37 require that locks for different rooms be re-keyed to different keys or combinations?

A3: 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. If the licensee uses a key based system to control access, the keys must be distributed only to approved individuals.

A best security practice is to avoid relying on keys to control access to the security zone. Key control becomes more difficult as time passes (especially for large institutions) as more duplicate keys are made for 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: Shouldn't the features of a device containing a category 1 or category 2 quantity of radioactive material be considered or given credit for providing some isolation for purposes of access control?

A4: 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 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 all the Part 37 requirements. Therefore, each of these new requirements must be implemented.

Q5: 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?

A5: 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.

Q6: Can the requirements for controlling access be waived if compliance is overly burdensome?

A6: The NRC is unlikely to grant relief from an access control requirement simply because the removal of the material would require a trained individual. The NRC has engaged the expertise of national laboratories that have shown that these devices may be vulnerable to theft, sabotage, or diversion in a short time period under certain scenarios. For this reason, and the possibility that the necessary trained individual could be a malevolent 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: 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 does not

allow licensee personnel into the repair bay to keep the on-board security zone under continuous surveillance?

A7: 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.

Q8: 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?

A8: No. Section 37.53 is not intended to provide 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 to provide delay, a portable or mobile device could be removed from a facility before the licensee can assess and respond to the initial unauthorized access.

Q9: To what extent is a licensee required to secure a room or area from unauthorized access where radioactive material is being stored behind locked doors with entry alarms?

A9: A licensee must have a security program to monitor and immediately detect, assess, and respond to unauthorized access to category 1 or category 2 quantities of radioactive material, even if the material is stored behind locked doors with entry alarms. The key to a successful security program is the integration of people, procedures, and equipment into a system that protects radioactive material. Licensees must therefore take into account and protect against situations where existing alarms, locks, walls, or other barriers could be defeated. To protect against unauthorized access to and removal of material behind conventional door locks with entry alarms, licensees may use such additional means as guards, closed circuit television, or motion detectors.

The specific system and means to protect material is the choice of the licensee, but to meet Part 37 requirements, the licensee should consider reasonably foreseeable actions by adversaries and 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.

§ 37.47 Security zones

§ 37.47(c)

Security zones must, at a minimum, allow unescorted access only to approved individuals through:

(2) Direct control of the security zone by approved individuals at all times; or

EXPLANATION:

This section establishes the requirements for a security zone.

QUESTIONS/ANSWERS:

Q1: 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?

A1: 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 and try to prevent 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 amount of interest in the system, equipment, and procedures used to protect the security zone.

Q2: How should a licensee 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. An approved individual must be determined to be trustworthy and reliable through a background investigation that includes fingerprinting and an FBI criminal history records check. In addition, the licensee must also provide training to its staff. This training should encourage increased awareness and reporting of unusual or unexpected conditions that could degrade facility security.

Further, 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.

Q3: What is an escort's responsibility?

A3: There are no specific requirements other than maintaining line-of-sight surveillance of the escorted individual(s) and carrying 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. 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.

Q4: Do licensees have to visually distinguish (e.g., with badges) all individuals who have not been granted unescorted access?

A4: 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.

Q5: Can we assume that patients can be granted unescorted access during patient treatments?

A5: No. Patients who are being treated with devices containing category 1 or category 2 quantities of radioactive material are usually escorted, monitored, or frequently observed by an approved individual. Access 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 or confronted by approved individuals.

Q6: Can the requirement for escorted access be waived for hospitals because of the cost and radiation safety concerns involved in accompanying patients at all times? Exceptions are also needed for emergency situations.

A6: Licensees must comply with the Part 37 requirements and ensure that patients who are receiving treatment with devices containing category 1 or category 2 quantities radioactive material do not have unauthorized access to the devices. Escorting is required for all individuals who have not been deemed trustworthy and reliable in accordance with Subpart B of this Part, and patients being treated are usually escorted, monitored, or frequently observed by an approved individual for radiation safety purposes in any case. Licensees should identify those areas and rooms where category 1 or category 2 quantities radioactive material are

located, and may use a variety of methods to escort, monitor, and otherwise limit access by patients. Licensees need to determine which methods would be the most reasonable and practical for their situation. While safety and security are complementary, security should not interfere with safety. Licensees can determine their own best practices or procedures in anticipated emergency situations, provided that they continue to comply with the requirements of Part 37.

Q7: 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?

A7 No, as long as there is an approved individual escorting these individuals.

§ 37.47 Security zones

§ 37.47(c)

Security zones must, at a minimum, allow unescorted access only to approved individuals through:

(3) A combination of continuous physical barriers and direct control.

EXPLANATION:

This section establishes the requirements for a security zone.

QUESTIONS/ANSWERS:

Q1: Can licensees use any combination of continuous physical barriers and direct control?

A1: Yes, as long as the combination can be shown to be effective in allowing only approved individuals to have unescorted access to the licensee's security zone(s). See questions on §§ 37.47(a) and 37.47(b)

§ 37.47 Security zones

§ 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 an approved individual 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:

During certain listed situations involving category 1 quantities of radioactive material, the licensee must provide continuous surveillance through the use of approved individuals.

QUESTIONS/ANSWERS:

Q1: When are special additional measures for category 1 quantities of radioactive material required?

A1: The requirements of 37.47(d) apply to category 1 quantities of radioactive material during periods of maintenance, source receipt, preparation for shipment, installation, or source removal or exchange. Licensees are required to provide, at a minimum, an approved individual 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 the specified activities.

During source replacement or equipment maintenance, 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 it does not need to be the same individual for the duration of the work. The second observer must begin surveillance before the original observer departs.

§ 37.49 Monitoring, detection, and assessment

§ 37.49(a)

Monitoring and detection.

(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 have the ability to continuously monitor and detect unauthorized entries into security zones.

QUESTIONS/ANSWERS:

Q1: Is there a need to provide security monitoring for locations other than windows, doors, and access ways?

A1: Yes, if necessary for immediate detection. 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 objectives are to reduce the risk that the material will be stolen and used for unauthorized purposes, and if it is stolen, to improve the likelihood of timely recovery. The licensee's actions to achieve these objectives must ensure that the licensee will remain continuously able to detect, assess, and respond to unauthorized activities without delay. 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?

A2: 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. An alarm system for a power source impairment should therefore be calibrated to trip for power surges, brownouts, and other anomalies that would cause a loss of the monitoring or detection system’s functionality. If the licensee chooses instead to use an alternate or auxiliary power source, such as a gasoline-fueled generator, the alternate power source should also be set to begin generating at the lowest level needed to continuously power the monitoring and detection system with no degradation in the security system’s performance.

§ 37.49 Monitoring, detection, and assessment

§ 37.49(a)(2)

Monitoring and detection.

Monitoring and detection must be performed by:

(i) A monitored intrusion detection system that is linked to an on-site or off-site central monitoring facility;

(ii) Electronic devices for intrusion detection alarms that will alert nearby facility personnel;

(iii) Visual monitoring by video surveillance cameras; or

(iv) Visual inspection by approved individuals.

EXPLANATION:

This section lists the methods to be used for monitoring and detection.

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 adequacy of a licensee's methods to comply with Part 37 requirements can only be determined by an on-site inspection. The regulation was designed to allow licensees flexibility to choose methods that work best in each licensee's specific circumstances. It is not sufficient just to choose effective methods to monitor, detect, and assess, however. The licensee's choices must also ensure that there is a 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: Can a less rigorous monitoring system be put in place during the routine workday? Can the licensee rely on visual inspection by approved individuals during the normal workday, and a system depending on an off-site monitoring facility at night?

A2: Effective detection and monitoring can be accomplished in different ways tailored to different facility-specific operating conditions. Detection and monitoring requirements can be met using trained guards, 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. Visual monitoring must also be capable of alerting trained assessment and response personnel without delay.

Q3: If a licensee uses electronic intrusion detection alarms, what minimum performance should these devices be capable of?

A3: If a licensee decides to use alarms that will alert nearby facility personnel of 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.

If a licensee decides to use magnetic switches on doors and windows as part of an intrusion alarm system, NRC considers it a best practice to use balanced magnetic switches, which are more difficult for an adversary to defeat. If a licensee uses motion detectors, it must use enough detectors to cover all potential egress points for radioactive material from the security zone. 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.

Q4: May a licensee use radiation safety monitoring and detection systems for material security purposes?

A4: Yes, if their use does not adversely affect radiation safety. Monitored motion detection systems or alarms used to control access to high radiation areas as required by 10 CFR Part 20, or equivalent Agreement State Regulations, for example, or other alerting systems used for radiation protection, may be used or modified, provided that 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. Conversely, a radiation sensor calibrated to detect a larger quantity of radioactive material to prevent or mitigate occupational exposures for Part 20 compliance may have to be recalibrated for more sensitivity to monitor for the security of a category 2 quantity of material. The licensee's security plan should describe how any radiation safety systems used for security purposes will provide the required intrusion detection without impairing these systems' performance or functionality for radiation protection.

§ 37.49 Monitoring, detection, and assessment

§ 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:

(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:

(A) Electronic sensors linked to an alarm;

(B) Continuous monitored video surveillance; or

(C) Direct visual surveillance.

(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:

This section establishes the requirement for a licensee to have a means to detect unauthorized removal of radioactive material from a security zone and establishes how a licensee can provide the detection capability.

QUESTIONS/ANSWERS:

Q1: 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?

A1: No, this requirement is in addition to the requirement to detect, assess, and respond to access to the security zone. Methods that the licensee may use to meet this requirement include, but are not limited, to the following:

- Alarming electronic tamper indicating device;
- Alarming radiation detector; or
- 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.

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.

Q2: Do the requirements for immediate detection of a removal of protected radioactive material apply at temporary job sites?

A2: Yes. Additionally, when a licensee is transporting protected radioactive material to and from a temporary job site, detection and assessment capability must be maintained when the transport vehicle is stopped at a hotel, restaurant, gas station, or other location.

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 would 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 who can challenge 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 response to unauthorized removal of radioactive material.

Q4: What about a medical facility using personnel for monitoring the removal of category 1 material where the personnel are moving about constantly and may not always be watching the area under access controls? How must this area be monitored?

A4: The licensee may use any of a number of methods to detect a removal of a category 1 quantity of material, but the method selected must meet the Part 37 requirements to immediately respond to any actual or attempted theft, sabotage, or diversion of protected radioactive material. Thus, if the licensee relies on trained personnel to detect removal, at least one individual should 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? Is there any way to monitor without an alarm system?

A5: Part 37 is designed allow a licensee flexibility to choose methods best adapted to its specific circumstances. While trained individuals can be used to monitor and immediately detect, assess, and respond as required, periodic checks would not meet the immediate detection requirement, nor would checks at 15-minute intervals. 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, even if the adversary is able to remove it from its authorized location.

Trained individuals can be used to fulfill some requirements of Part 37, but a licensee must meet the applicable Part 37 requirements 24 hours per day, 7 days per week. An appropriate method of monitoring, detection, and assessment that 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.

Q6: 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?

A6: The NRC is unlikely to grant an exemption solely on a basis of remoteness. Remoteness may allow an intruder to gain undetected and unauthorized access more readily than in more populated environments. An additional lag in communications about a detected intrusion may also provide advantages to an intruder planning to steal or sabotage material. Therefore, licensees must meet all applicable Part 37 requirements.

If a licensee believes it cannot meet a Part 37 requirement because of remoteness or the difficulty of timely communication, the licensee must request an exemption and provide compensatory measures to reduce the probability or mitigate the consequences of not meeting the specified requirement. Exemption requests will be evaluated on a case-by-case basis. See Qs&As for § 37.11

Q7: Could radiation detection meters connected to a silent alarm be used to alert local law enforcement of an attempted theft of radioactive material?

A7: Yes, radiation meters could be a means to detect theft of radioactive material depending on the configuration of shielding surrounding the radioactive source. However, the Part 37 requirements were designed to provide a defense-in-depth strategy for the control of protected radioactive material, and the NRC expects licensees to consider all credible scenarios when developing and implementing a security program to implement the requirements of Part 37.

Q8: 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?

A8: Licensees may use any method to detect the removal of a category 2 quantity of radioactive material that is acceptable for detecting the removal of a category 1 quantity. Although the electronic sensors used for detecting removal of a category 1 quantity of material are not required for category 2 quantities, NRC encourages licensees to consider the application of these devices where feasible for immediate detection capability.

If a licensee decides to use an electronic tamper indicating alarm for detecting removal, the NRC recommends that the system be designed to alarm if an attempt is made to remove a device, or a source from its device. The tamper indicating alarm should be armed at all times (except during periods of maintenance).
The licensee’s security plan should 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

§ 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:

Licensees must assess every actual or attempted unauthorized entry into a security zone.

QUESTIONS/ANSWERS:

Q1: Can a licensee use automated devices to assess an intrusion and alert an LLEA?

A1: Licensee may use automated devices to assess an intrusion and alert the LLEA 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 immediately request assistance and promptly begin any other mitigating measures. Depending on the security system, the layout of controlled areas, and the design capabilities of the sensors, automated devices or systems may be programmed to automatically summon LLEA assistance 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: What does it mean to perform assessments by automated devices?

A2: Depending on the security system, layout of control areas, and sensors, automated devices or systems may be programmed to automatically summon LLEA assistance in response to an intrusion alarm. In effect, the licensee has performed the assessment in advance and preset the security system to respond to alarms from one or more detectors without real-time human analysis.

Q3: Can licensees perform their own vulnerability assessment and change Part 37 time requirements for detection and response?

A3: No. Part 37 requires licensees to detect, assess, and respond to any unauthorized access to the security zone “without delay.” Notification of the LLEA must be made as soon as possible. If for some reason a licensee cannot comply with a specific requirement, the licensee should inform the NRC or its Agreement State licensing authority, as appropriate, and request an exemption. The exemption request should propose compensatory measures to reduce the probability or mitigate the consequences of not meeting the specified requirement.

§ 37.49 Monitoring, detection, and assessment

§ 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:

(1) Maintain continuous capability for personnel communication and electronic data transmission and processing among site security systems; and

(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 the capability for personnel communication and electronic data transmission and processing between site security systems for systems supporting the monitoring, detection, and assessment systems.

QUESTIONS/ANSWERS:

Q1: What are the requirements for a licensee's primary personnel communications and data transmission?

A1: Licensees are required to maintain continuous capability for personnel communication and electronic data transmission and processing between site security systems for any personnel and automated or electronic systems used to support the site security systems. The licensee 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. Land line phones, auto dialers, cellular phones, pagers, radios, and other similar modes of communication may be used to fulfill this requirement. When more than one person is used for detection and assessment, a means of communicating between the various monitoring personnel must be provided.

Q2: What personnel communications and data transmission systems are subject to the requirement for an alternative capability?

A2: Licensees would be required to have alternative capability for any system of communication or data transmission and processing in the event of loss of the primary means. 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.

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 would 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

§ 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 immediately respond to any actual or attempted unauthorized access to the security zones and to any attempted theft, sabotage, or diversion of category 1 or category 2 quantity of radioactive material. The licensee's response must include requesting an armed response from the LLEA for actual or attempted theft, sabotage, or diversion of the material.

QUESTIONS/ANSWERS:

Q1: What would a licensee need to do when it detects an intrusion into its security zone?

A1: A licensee's response to an intrusion would depend on the licensee's assessment of the purpose of the intrusion, but a response would be required without delay. If the unauthorized access appeared to be an actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material, the licensee would have to immediately notify and request an armed response from the appropriate LLEA, followed soon thereafter 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 risk that the material could be used for malevolent purposes. Immediate notification would also allow for early warning to other possible targets of a simultaneous attempt to divert material from multiple locations.

A licensee's decision to call the LLEA and the NRC would depend not only on the licensee's assessment of the intent of the unauthorized access, but also on whether the area where the breach occurred is an area the licensee had previously determined needed to be monitored in order to meet NRC physical protection requirements. Thus, a licensee's assessment and response to an intrusion alarm in the business office section of its facility could be entirely different from its assessment and response to an intrusion alarm in a radioactive material storage area.

Q2: Does the NRC intend to require the responder to have firearms, or will non-lethal weapons suffice? As an example, some security staff do not carry firearms and an LLEA response might not meet the need for timeliness.

A2: The NRC does not require licensee responders to be armed. The requirement for armed response capability applies only to the LLEA from which the licensee is required to request assistance. The purpose of requiring such an LLEA to be capable of an armed response is not to prevent unauthorized access, but to respond to and disrupt an actual or attempted theft, sabotage, or diversion of radioactive material. Adversaries could be well armed individuals. A private security force, even if armed, does not substitute for an LLEA. The LLEA will respond to the event as it deems appropriate, considering its available resources and concurrent needs for response elsewhere within its jurisdiction.

Q3: Could radiation detection meters connected to a silent alarm be used to alert local law enforcement of an attempted theft of radioactive material?

A3: Yes, radiation meters could be used as a means to alert an affected LLEA of an actual or attempted theft of radioactive material, if this method is acceptable to the LLEA under the terms of the coordination agreement. The rule is designed to provide a defense-in-depth strategy for the control of the radioactive material protected under this Part, however, and the NRC expects licensees to consider other measures for requesting LLEA assistance if they would also be appropriate.

Q4: Since licensed facilities are also broken into to obtain equipment other than radioactive materials, would coordination require licensees to summon the LLEA every time there is a break in?

A4: 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 the business office section of its facility could be entirely different from its assessment and response to an intrusion alarm in a radioactive materials storage area.

§ 37.51 Maintenance, testing, and calibration

§ 37.51(a)

Each licensee subject to this subpart shall implement a maintenance, testing, and calibration 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, and are inspected and tested for operability and performance at intervals not to exceed 3 months.

EXPLANATION:

Each licensee shall have a maintenance, testing, and calibration program for any security-related systems.

QUESTIONS/ANSWERS:

Q1: What minimum measures should a licensee implement for a maintenance, testing, and calibration program?

A1: A licensee should

- Identify all alarms, communication systems, and other physical components used to secure or detect unauthorized access to radioactive material;
- 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 and calibration 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 and calibration 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;

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

Q2: Would inspection and testing be required every 3 months for every component of every system to secure radioactive materials or detect unauthorized access to them?

A2: No. The operability and performance of some components, such as personnel and data communications systems, may be confirmed by regular daily or weekly use. For further discussion of testing and the components and systems to be tested, see Qs&As below.

Q3: What's the difference between "maintain[ing 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?

A3: The need for different tests would depend on the intended function of the system or component, and whether that function 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.

Q4: What kinds of tests for intrusion alarms would be acceptable for demonstrating compliance?

A4: Acceptable tests for intrusion alarms should be identified on the basis of the functions each alarm is expected to perform. An alarm used with a tamper-indicating device to provide immediate detection of any attempted unauthorized removal of a category 1 quantity of radioactive material from the security zone under §37.49(a)(3)(i), for example, should not only detect the tampering and trigger an audible alarm, but may also need to transmit notification of the tampering to onsite or offsite monitors or responders. At a minimum, an alarm expected to fulfill these functions should be tested for its ability to fulfill all of them. But each function does not need to be tested independently. The detection, sound production, and communications capabilities of an intrusion alarm, for example, could all conceivably be tested by producing a motion of a specified magnitude at a specified elevation and distance designed to test the alarm's detection sensitivity. Such tests would also be useful to confirm that the subcomponents of the intrusion alarm system work as expected.

Q5: What does NRC mean by "associated" communications systems–associated with the intrusion alarm or associated with the whole system for security or detection?

A5: 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.

Q6: What should a licensee consider to be a "communication system" subject to testing, calibration, 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: For the purposes of this section, the NRC would consider 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 would include such things as a land-line phone, a walkie-talkie system, a cell phone, or a megaphone. 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 calibration, and maintenance requirements of this section would apply, because § 37.51 would apply 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.

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 maintenance, testing and calibration? 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 thus 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.

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 as low as reasonably achievable (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: Would testing, calibration, and maintenance have to be performed by approved individuals meeting the access authorization requirements of Subpart B?

A8: No. Individuals not approved for unescorted access would, however, need to be escorted when performing maintenance, testing, or calibration activities within a security zone.

Q9: Would testing or calibration equipment need to be secured within a security zone?

A9: No. If the testing or calibration equipment was 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 and calibration 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 controlled key or combination lock.

§ 37.51 Maintenance, testing, and calibration

§ 37.51(b)

The licensee shall maintain records on the maintenance, testing, and calibration activities for 5 years.

EXPLANATION:

Maintenance records must be maintained for 5 years.

QUESTIONS/ANSWERS:

Q1: What kinds of records of maintenance, testing, and calibration 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; and
- The purpose of the maintenance, identifying as appropriate the deficiencies in operability or performance.

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 or calibration activities needed to remove any deficiency in the operability or performance of the component or system.

For each calibration activity, a record should identify:

- The name(s) of the person(s) who performed the calibration(s);
- The date of the calibration(s);
- The component(s) or system(s) calibrated; and
- The purpose of the calibration(s), identifying as appropriate the deficiencies in operability or performance.

§ 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:
(a) Have two independent physical controls 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 that contain category 1 or category 2 quantities of radioactive material must have two independent physical controls to secure the device from unauthorized removal.

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 is not under direct control and constant surveillance by the licensee?

A1: Due to ease of movement, mobile devices are particularly vulnerable to attempted theft or diversion; it may be possible for a mobile device to be removed before the licensee has an opportunity to respond to an intrusion. The objective of this requirement, therefore, is to delay an unauthorized entity long enough to provide additional time for the licensee and the LLEA to respond.

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 direct control and constant surveillance by the licensee. Such a physical control should provide an additional redundant 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 (e.g., construction trailer, sea container, etc.), or in a locked garage, with the device physically secured by a locked chain or steel cable to a non-portable structure in such a manner that the device could not be removed without removing the chain or cable. A device should be inside a locked, non-portable cabinet or locked container that is secured to a non-portable structure.

- Storage of the device in a locked garage within a locked vehicle, or physically secured by a locked chain or steel cable to the vehicle in such a manner that the device could not be removed without removing the chain or cable.

Q3: If mobile devices are stored in one room, does that mean the licensee has an aggregated quantity of radioactive materials?

A3: 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 methodology. (See questions on § 37.1); 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.

§ 37.53 Requirements for mobile devices.

§ 37.53(b)

For devices in or on a vehicle or trailer, 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:

For any device containing category 1 or category 2 quantities of radioactive material that is in or on a vehicle or trailer, the licensee must use a method to disable the vehicle or trailer when the radioactive material is not under direct control and constant surveillance.

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: Consistent with the objective of the requirement for two independent physical controls on stationary equipment containing category 1 or 2 quantities of radioactive material, the objective of the vehicle disabling requirement is to delay unauthorized removal of a device containing this material long enough to provide additional time for the licensee and the LLEA to respond. Examples of acceptable vehicle disabling methods would include: trailer hitch locks, wheel locks ("boots"), or methods to disable the vehicle's engine.

For vehicles used to transport mobile devices inside a facility, additional delay may be accomplished by a variety of other independent physical controls, including:

- Speed bumps too large for the vehicle to traverse on the facility floor;
- Elevated doorway thresholds;
- Protective storage enclosures;
- Channels in a floor large enough to catch the device wheels;
- 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.

Q2: Does the requirement to secure mobile devices mean that all trucks will need an alarm system?

A2: If the truck is left unattended with a device containing a category 1 or category 2 quantity of radioactive material, licensees should have a way to monitor and immediately detect, assess, and respond to actual or attempted theft, sabotage, or diversion of the radioactive material or device(s). An alarm system is an acceptable method.

Q3: When a licensee 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 a licensee is 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 should the licensee assess whether the security satisfies Part 37?

A3: Licensees who possess the radioactive material are responsible for the security and control of their own material and need to meet the security requirements whether at their own or a customer's facility. If a licensee chooses to store devices at its customers' facilities, it may consider the customer's physical protection program to comply with one or more of the requirements of this section. There should, however, be a clear understanding of the roles and responsibilities of the licensee and its customer, and what features of the customer's security and control program are to be relied on to meet the security requirements for the radioactive material. Licensees should assess the customer's security and control features being relied upon against its own program for implementing these requirements.

Particular attention should be given to limiting unescorted access to as few as possible of the customer's personnel, and to whether the customer has a process for determining whether individuals are trustworthy and reliable. The licensee and customer will also need to determine who will be responsible for satisfying the requirements to monitor and immediately detect, assess, and respond to any actual or attempted theft, sabotage, or diversion of radioactive material. If the customer is to implement these requirements, clear roles, responsibilities and methods need to be defined for communicating with the licensee, assessing the incident, and summoning the appropriate responder, including requesting assistance from the responsible LLEA.

Q4: Can a licensee put an intrusion alarm system on a radiography truck? At field stations, who must meet the requirements for security and immediate detection?

A4: Yes, an intrusion alarm system can be put on a radiography truck or any vehicle. The licensee and its authorized users would have to meet the requirements of the new security regulations at field stations and all off-site locations.

Q5: 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?

A5: Yes. A heavy-duty twisted steel wire cable may be used 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 that a No. 10 wire - 1/8 inch or 2 mm). Any system is only as effective as its weakest component; therefore other components of the securing mechanism

need to have similar strength such that it 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 Department of Energy (DOE) M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests.

Q6: If a licensee locks a radiographic camera in a trailer at a job site, and the source is locked inside the trailer, how should the licensee secure the trailer?

A6: How a trailer could be immobilized or secured to add a delay factor would depend on the size of the trailer and its location. Immobilization may be accomplished by a variety of physical controls including: protective storage enclosures, trailer hitch locks, wheel locks, a hardened chain and hardened lock, removing the wheels, or deflating the tires.

Q7: If disengaging a standard key from a vehicle's ignition must not be considered a means to "disable" a vehicle when a vehicle or trailer is not under direct control and constant surveillance by the licensee, what methods would be acceptable?

A7: 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 a key, such as using a duplicated key or hot-wiring techniques. There are currently many advances in ignition and key technology that provide for additional barriers that would cause delay in accessing radioactive material quantities of concern. An example is a key implanted with an electronic chip that is only recognizable to the computer in the vehicle. Only this key, and not a duplicated key, would be able to start the vehicle. These technologies, and others that allow operation of a vehicle only by a means that is not easily defeated, would be considered an appropriate means to disable a vehicle.

Q8: 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?

A8: 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 how the licensee will control 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—especially if they are in control of combinations or keys that secure material--understand the importance of their roles and responsibilities for controlling access.

§ 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 ensure that the security program is reviewed at a frequency not to exceed 12 months.

§ 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 5 years.

EXPLANATION:

Licensees need to assess the effectiveness of its security program, take appropriate corrective actions, and maintain the records for 5 years.

QUESTIONS/ANSWERS:

Q 1: How should a licensee define 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. Neither the licensee nor NRC can be assured of the continuing effectiveness of a security program if the licensee cannot find and correct emerging or existing noncompliances. The absence of identified problems does not necessarily demonstrate the continuing effectiveness of the 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; these actions should be transparent, open to security-conscious critical reviews at all levels. The hallmark of an effective program is not, therefore, the absence of recorded adverse conditions or noncompliances. 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: Must a licensee engage an outside contractor to conduct security program reviews? If not, how can a licensee ensure that the review isn't conducted by the same people carrying out the activities being reviewed?

A2: 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 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. Licensees may also choose to set up a review team through an industry association, with participants from several independent member organizations available to conduct program reviews.

Q3: Does a licensee need to report to NRC any noncompliance identified during a security program review?

A3: 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.

Q4: What would NRC consider a "condition adverse to the proper performance of the security program?"

A4: NRC would consider as an adverse condition any occurrence or continuing state that, if not corrected, could degrade the ability of the physical security system to secure against or detect an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. A condition would be deemed adverse if it degraded or was reasonably likely to degrade the licensee's ability to monitor, detect without delay, assess, or respond to an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. 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.

Q5: The regulation requires the report resulting from a program review to recommend corrective actions "when appropriate." When should a licensee recommend corrective actions?

A5: 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 security program" identified as a result of the review.

Q6: What should a licensee consider as "review documentation" for the purposes of this subsection?

A6: 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, but the licensee should retain its management-approved 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.

§ 37.57 Reporting of events

§ 37.57(a)

The licensee shall immediately notify the LLEA after initiating an appropriate response to any 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:

Licensees must immediately notify the LLEA when responding to any actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. After notifying the LLEA, the licensee must notify the NRC.

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 would probably 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 in turn 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, 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. If one or more members of the licensee's security staff are authorized and qualified to use firearms, however, an appropriate response need not rule out the use of these weapons if, for example, the intruding party is armed and violent. The NRC recognizes that in

such cases, licensee security staff may need to use firearms in self-defense, or to subdue the intruders until the LLEA can take them into custody.

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 or available to help the security staff respond to the event, NRC would expect that employee to notify his or her management and 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. In sum, other than a situation requiring a licensee to devote all available resources to restoring its facility to a safe condition or protecting individuals from physical harm, the NRC would consider a postponed notification to be justified only if the LLEA required all available licensee resources to assist it, and a temporary diversion of those resources to call the NRC could reasonably be expected to delay or otherwise interfere with a timely or effective LLEA response.

Q3: To avoid an NRC notice of violation after the event, would the licensee 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 the licensee is not prohibited from seeking the LLEA's endorsement of the licensee's decision to delay NRC notification, and 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 licensee's judgment, not the LLEA's.

Q4: Under what circumstances could a licensee delay notifying the NRC for 4 hours without violating the requirement to notify the NRC "as soon as possible?"

A4: The NRC can envision none but the most extreme and unusual circumstances to justify such a significant delay. One such circumstance would be the total loss of both the LLEA's and the licensee's primary communication capability, such that responders would be forced to rely exclusively on the licensee's alternative communications system. Another scenario would be the incapacitation of all law-abiding individuals at a remote site, unnoticed by the dispatching LLEA or any offsite individual for up to four hours after an attack. Needless to say, such hypothetical circumstances are highly unlikely. One real-world rule of thumb for an effective

limit on the allowable time for the licensee to notify the NRC, however, would be the shortest reasonable time it would take for an off-site individual not directly involved in the emergency to discover it and alert a local news organization.

Q5: When a licensee determines that an actual or attempted theft, sabotage, or diversion of radioactive materials has begun, what information must be reported to what organization (NRC, Agreement State, LLEA)?

A5: Under these circumstances, a licensee would be required to notify the LLEA first and without delay, and the notification would at minimum have to contain a request for the LLEA's assistance. Depending on the frequency and quality of the licensee's coordination activities under § 37.45 of the regulation and the LLEA's familiarity with the licensee's operations, the licensee's initial emergency contact may not need to provide much additional information. If the licensee's coordination efforts with the LLEA have not been recent, however, or the LLEA's expected point of contact is not available, the licensee should provide additional information to facilitate a timely and effective LLEA response. Such information could include, for example: the affected facility's location and quickest route from the nearest LLEA station; 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).

The licensee's notifications to the NRC or Agreement State regulatory agency, as appropriate, would depend in part on the agency's applicable regulations and guidance. If no such regulations or guidance are available, the licensee should be prepared to provide at minimum an estimate of the kinds and quantities of radioactive material that could be affected by an unauthorized access, and how the material is contained, such as whether it is in a stationary or a mobile device, or another type of container. Depending on the regulatory agency's need for additional information, the licensee could also provide some of the information already provided to the LLEA, such as, 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 LLEA responders.

For both kinds of notification, the licensee should consider the known and potential needs of the recipient agency for mission-related information and address these issues in its security plan and procedures. The licensee should also consider that compliance with these notification requirements does not relieve it 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 or the Agreement State regulatory agency every time there is a break in?

A6: No. The regulation does not require a licensee to request LLEA assistance and notify the affected Agreement State or 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 NRC or Agreement State regulators would depend on an assessment of whether the detected break-in was intended 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 the business office section of its facility 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.

Q7: If someone reports lost or missing category 1 or category 2 quantities of radioactive material, what would be the response of the NRC or Agreement State?

A7: If such an incident occurs, the NRC or Agreement State would expect the licensee to implement the appropriate elements of its security plan. The NRC or Agreement State would 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 Plan, the NRC would notify and coordinate with other Federal Agencies as needed. Similarly, Agreement States would notify NRC and other state agencies, and coordinate State resources as needed.

Q8: What must a licensee do when it determines that a detected intrusion into a security zone is not a false alarm?

A8: In the event of any actual or attempted theft, sabotage, or diversion of radioactive material protected under Part 37, the licensee 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 or a responsible Agreement State regulatory agency should be as prompt as possible, but not at the expense of causing delay or interfering with the LLEA's response to the event.

§ 37.57 Reporting of events

§ 37.57(b)

The licensee shall notify the LLEA upon discovery of any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material. 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:

Licensees must notify the LLEA upon discovery of any suspicious activity related to possible theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material. After notifying the LLEA, the licensee must notify the NRC.

QUESTIONS/ANSWERS:

Q1: Why am I reporting to the suspicious activities to the NRC?

A1: The reporting of suspicious activities is an important component of 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 the 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 NRC licensed activities?

A2: No, licensees are not required to report activities they deem to be "routine and non-threatening." The NRC notes that what is considered "routine and non-threatening" may evolve over time, may change as the threat levels change, and may vary by geographical area. Because this requirement is intended to assist the NRC's threat assessment missions, rather than implement physical security requirements, or report more specific events (e.g., discovery of contraband inside a controlled area) both the regulations and guidance in this area are worded broadly to provide licensees with flexibility.

Q3: Is there 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.

§ 37.57 Reporting of events

§ 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 of such unauthorized access.

EXPLANATION:

The licensee must submit a written report within 30 days of reporting an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material.

QUESTIONS/ANSWERS:

Q1: The regulations specify that the licensee's written report on the security incident "must include sufficient information for NRC analysis and evaluation, including identification of any necessary corrective actions to prevent future instances of such unauthorized access." Other than an identification of necessary corrective actions, what, at a minimum, should the report 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 indicative of 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 Nation's enemies 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 the "current threat assessment." The prompt reporting of actual or imminent hostile actions permits the NRC to execute its strategic missions of communicating hostile action against the facilities and activities it regulates to senior Federal officials and other licensees; thereby protecting public health and safety, the common defense and security, and the environment.

The 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 and should be reported under § 37.57(b):

a. 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.

b. Individual(s) conducting unapproved photographing or videotaping of licensed facilities on owner controlled property.

c. Individual(s) conducting unapproved photographing or videotaping of licensed facilities from public property or non-owner controlled property when combined with other suspicious information gathered by security personnel challenges to, or interviews of, the individuals.

d. 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.

e. Loitering for no apparent purpose in areas where intelligence could be gathered or preoperational reconnaissance could be performed.

f. Suspicious behavior (e.g., fleeing, moving quickly away from licensee or certificate holder personnel, unexpected vehicular movement).

g. Secretive sketching, making maps, or taking notes on the owner controlled area.

h. Eliciting information from security or other site personnel regarding security systems or vulnerabilities.

i. Unusual challenges to security systems that could represent attempts to gather information on system performance or personnel or equipment response actions.

j. 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).

k. Theft or suspicious loss of official company identification documents, uniforms, or vehicles necessary for accessing plant facilities.

l. Use of forged, stolen, or fabricated documents to support access control or authorization activities.

m. Boating activities conducted in unauthorized locations or attempts to loiter near facility restricted areas.

n. Unusual attempts to obtain information or documents related to site security training, techniques, procedures, or practices.

o. Discovery of Internet site postings that make violent threats related to specific licensed facilities or activities.

p. 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.

q. Stated threat(s) against the licensee's facility or staff, unless they are determined to be unsubstantiated.

r. 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.

s. Fires or explosions of suspicious or unknown origin.

t. 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.

u. The intentional cutting of wires that does not affect the facility or security operations.

v. The modification of security equipment that renders the equipment inoperable.

w. The overt changing of equipment or controls to settings that do not affect their intended function.

The NRC does not consider this list to be exclusive. Additionally, licensees should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 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

§ 37.71(a)

Notwithstanding the requirements of any other regulation in this chapter, 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 address requested for delivery. The transferor shall document the verification.

§ 37.71(b)

Notwithstanding the requirements of any other regulation in this chapter, 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. The transferor shall document the verification.

§ 37.71(c)

The transferor shall keep a copy of the verification documentation as a record for 5 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 5 years.

QUESTIONS/ANSWERS:

Q1: Is verification of the transferee's license necessary?

A1: Yes. Licensees are required to verify that the licensee that is being sent category 1 or category 2 quantities of radioactive material is authorized to receive the radioactive material. The verification is required to occur before the radioactive material is actually transferred.

Q2: How does a licensee make the verification?

A2: These verifications would be conducted with the license issuing authority, i.e., the NRC or the appropriate Agreement State or by using the NRC's license verification system.

Q3: What is the license verification system?

A3: The license verification system is a new web-based system that NRC is developing that may be used to verify the validity of a license issued by either NRC or an Agreement State. Although this system is in the early stages of development, it should be available before the effective date of the final rule. If the system is not available, licensees would need to contact the appropriate licensing 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. More information will be available once the system is fully developed and operational.

Q4: 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., exports), does it still need to verify the transfer?

A4: No, the verification of license is only applicable if the licensee is transferring category 1 and category 2 quantities of radioactive material to a licensee of the NRC or an Agreement State. If the licensee is transferring material to DOE, verification is not required. Licensees exporting material 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.

Q5: What information needs to be verified?

A5: The licensee must verify that the transferee's license authorizes the receipt of the type, form, and quantity of radioactive material to be transferred. For transfers of category 1 quantities of radioactive material, the transferring licensee would also be required to verify that the transferee licensee is authorized to receive radioactive material at the address requested for delivery.

Q6: Why are there differences between the category 1 and category 2 verification requirements?

A6: Because category 1 quantities of radioactive material are considered to be of greater concern than those of category 2, the licensee transferring category 1 quantities is subjected to the additional requirement of verifying that the transferee licensee is authorized to receive radioactive material at the address requested for delivery.

Q7: How should a licensee document the verification?

A7: If the licensee checks with the licensing agency, the licensee should document the conversation with a note to file or an e-mail confirming the information provided by the licensing agency. The documentation should include the date of the conversation, the name of the individuals participating in the call, and basic information on the shipment. If the licensee uses the license verification system, the system will save the record and the licensee would not need to keep further documentation. The licensee may print a copy of the record and keep a paper copy. The record must be maintained for 5 years.

Q8: What should a licensee do if it receives an unusual order?

A8: The shipping licensee should pay particular attention to orders that appear unusual, as compared to previous shipments to the transferee licensee, with respect to the type, form, location of shipment destination, and/or quantity of material to be shipped. Unusual orders raise heightened security concerns, including an attempt by terrorists to obtain radioactive materials, and as such, the transferring licensee must take appropriate precautions, including contacting the requisite regulatory authority."

§ 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 (c) through (e); 37.77; 37.79(a)(1), (b)(1), (c) and (d); 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 (d); 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 category 1 quantities of radioactive material shall comply with the requirements for physical protection contained in §§ 37.75(a)(2) and (c) through (e); 37.77; 37.79(a)(1), (b)(1), (c), and (d); and 37.81(a), (c), (e), (g), and (h) during the domestic portion of the shipment.

§ 37.73(e)

Each licensee that imports category 2 quantities of radioactive material shall comply with the requirements for physical protection during transit contained in §§ 37.75(c) through (e); 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.

QUESTIONS/ANSWERS:

Q1: Would two or more packages in a shipment from one NRC licensee, each containing less than a category 2 quantity but that in aggregate reach or exceed a category 2 quantity, be required to meet the Subpart D requirements?

A1: 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 of concern regardless of how many individual packages may be in the shipment. In that case, the individual package quantities are said to "roll-up" to a category 2 quantity with the full knowledge of the licensee. Therefore, a licensee cannot avoid meeting the Subpart D requirements by partitioning the total shipping quantity into multiple packages on the same vehicle.

Q2: Can two or more packages, from more than one licensee with separate bill of ladings, and each containing less than a category 2 quantity but that in aggregate reach or exceed a category 2 quantity, be considered as more than one consignment under DOT regulations and, therefore, not be required to meet Subpart D requirements?

A2: Yes. "Consignment," as defined by the DOT in 49 CFR Part 173.403, is a package, group of packages, or load of radioactive material, offered by a person for transport in the same shipment. However, DOT regulations do not consider roll-up quantities from multiple sources. Since each licensee is independently shipping a quantity of radioactive material that is below the category 2 threshold, the licensees have no knowledge of what the total quantity of material might be in the shipment, and they are not responsible if the carrier picks up radioactive material from multiple locations that, in the aggregate, meets or exceeds the category 2 threshold.

Q3: Which licensee is responsible for meeting the requirements of Subpart D?

A3: Generally, the shipping licensee is responsible for meeting the requirements of this subpart. However, the receiving licensee may choose to agree in writing to arrange for the required in-transit physical protection measures. In that case, meeting the physical protection requirements of this subpart is the responsibility of the licensee receiving the shipment.

Q4: During what part of the shipment are the category 1 and category 2 security requirements applicable for imports?

A4: 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).

Q5: For material being exported, is the licensee required to follow the security requirements for the entire trip?

A5: The licensee is responsible for following the security provisions for the domestic portion of the trip up until the time when the shipment comes under the jurisdiction of a U.S. Government agency (e.g., Federal Aviation Administration (FAA), Transportation Security Administration (TSA), Customs, etc.) at a port, a border crossing, or an airport. For example, once a package is delivered to an airport and accepted by an airline carrier, FAA and TSA security provisions apply. In addition, once a shipment arrives into another country, that country's security provisions would then apply.

Q6: Do the security provisions for category 1 and category 2 nuclear material quantities of concern apply during the time when shipments are placed in interim storage, such as in a shipping warehouse or similar situation?

A6: Yes, the security provisions do apply. During planning and coordination, NRC licensees should ensure that any storage incident to transport is minimized and, when it cannot be avoided, appropriate security measures are in place.

Q7: Do the security provisions apply to transshipments?

A7: 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 company in one country, pass through the United States, and then continue on to a company 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:

(1) Preplan and coordinate shipment arrival, including the no-later-than arrival time, and departure times with the receiving licensee;

(2) Preplan and coordinate shipment information with the governor or the governor's designee of any State through which the shipment will pass to:

(i) Ensure minimal delays;

(ii) Discuss the State's intention to provide law enforcement escorts;

(iii) Arrange for positional information sharing when requested;

(iv) Identify Highway Route Control Quantity shipments (as the term "Highway Route Control Quantity" is defined in 49 CFR 173.403); and

(v) Identify safe havens; and

(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. The shipping licensee must coordinate with the receiving licensee to establish a no-later-than arrival time.

QUESTIONS/ANSWERS:

Q1: Is preplanning and coordination of shipments of category 1 quantities of radioactive material necessary?

A1: Yes. Licensees are required to preplan and coordinate shipment information for shipments of category 1 quantities of radioactive material. The shipping licensee (licensee sending the licensed material) is required to coordinate the departure and arrival times, including the no-later than arrival time, with the receiving licensee (licensee receiving the licensed material). The licensee would also need to preplan and coordinate the shipment information with the State(s) through which the shipment will pass. As part of the coordination activities, the licensee would be required to discuss the State's intention to provide law enforcement escorts for the shipments, identify highway route control quantity shipments,

identify safe havens, and arrange for any positional information sharing. The purpose of the information sharing is to ensure minimal delay of the shipment.

Q2: What is meant by no-later-than arrival time?

A2: The term “no-later-than arrival time” is defined as 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 2 hours after the estimated arrival time for category 1 shipments. Requiring verification that the shipment arrived on time provides the licensee, in the event that the shipment fails to arrive by the no-later-than arrival time, with a fixed time to identify and immediately report an unusual occurrence that could lead to the theft or diversion of the material.

Q3: What type of documentation is necessary?

A3: The shipping licensee should document any phone conversations that it has with the receiving licensee to include the names of the individuals participating in the call, the agreed upon no-later-than arrival time, and departure times. The shipping licensee should also document any interactions with the governor’s designee to include names of the individuals participating in the call, decision on escorts, safe havens identified, and any other pertinent information.

Q4: What does the NRC consider to be a safe haven?

A4: 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.” The NRC expects safe havens to be identified and designated by the licensee based on discussions with appropriate State personnel.

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; secure company terminals; State weigh stations; truck stops with secure areas; and LLEA sites, including State police barracks.

Q5: What is a Highway Route Control Quantity?

A5: A Highway Route Control quantity is defined in 49 CFR 173.403 to mean a quantity within a single package which exceeds: (1) 3,000 times the A1 value of the radionuclides as specified in § 173.435 for special form Class 7 (radioactive) material; (2) 3,000 times the A2 value of the radionuclides as specified in § 173.435 for normal form Class 7 (radioactive) material; or (3) 1,000 TBq (27,000 Ci), whichever is least. However, it should be noted that individual States may have specific control quantities that may apply, and 10 CFR Part 37 requirements do not preempt any State requirements that may be applicable.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material

§ 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 verify and document the shipment no-later-than arrival time and the actual shipment arrival with the receiving licensee. Verification may be made by e-mail, fax, or written documentation of a verbal conversation.

EXPLANATION:

Licensees shipping category 2 quantities of radioactive material must coordinate with the receiving licensee the no-later-than arrival time.

QUESTIONS/ANSWERS:

Q1: Is preplanning and coordination of shipments of category 2 quantities of radioactive material necessary?

A1: Yes. For shipments of category 2 quantities of radioactive material, the shipping licensee must verify and document the shipment's no-later-than arrival time and the actual arrival time with the receiving licensee.

Q2: What is meant by no-later-than arrival time?

A2: The term "no-later-than arrival time" is defined as 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 4 hours after the estimated arrival time for category 2 shipments. Requiring verification that the shipment arrived on time provides the licensee, in the event that the shipment fails to arrive by the no-later-than arrival time, with a fixed time to identify and immediately report an unusual occurrence that could lead to the theft or diversion of the material.

Q3: What type of documentation is necessary?

A3: The shipping licensee should document any phone conversations that it has with the receiving licensee to include the names of the individuals participating in the call and the agreed upon no-later-than arrival time. E-mails may be printed or stored electronically. A copy of any fax and the confirmation information should be maintained.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material

§ 37.75(c)

Each licensee who receives a shipment of a category 1 or category 2 quantity of radioactive material shall notify the shipping licensee within 4 hours when the shipment arrives at its destination.

EXPLANATION:

Within 4 hours of receiving a shipment of category 1 or category 2 quantities of radioactive material, the receiving licensee must notify the shipping licensee that the shipment arrived.

QUESTIONS/ANSWERS:

Q1: Are there any requirements for the receiving licensee to notify the shipping licensee when the shipment arrives?

A1: Yes. The receiving licensee must notify the shipping licensee when the shipment of a category 1 or category 2 quantity of radioactive material arrives at its destination. The notification must be no later than 4 hours after the package arrives.

Q2: How should the receiving licensee notify the shipping licensee?

A2: The receiving licensee may contact the shipping licensee by phone, e-mail or facsimile. During the preplanning and coordination activities the licensees should decide what method of notification would be used.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material

§ 37.75(d)

Each licensee, who transports or plans to transport a shipment of a category 1 or category 2 quantity of radioactive material, and determines that the shipment will arrive after the no-later-than arrival time provided pursuant to paragraph (a)(1) 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 of the new no-later-than arrival time.

QUESTIONS/ANSWERS:

Q1: Is the shipping licensee required to notify the receiving licensee if the no-later-than arrival time changes?

A1: Yes. If the no-later-than arrival time will not be met, the shipping licensee must inform the receiving licensee of the new no-later-than arrival time for shipments of category 1 or category 2 quantities of radioactive material. This provision allows licensees the ability to modify departure and arrival time due to unforeseen events.

§ 37.75 Preplanning and coordination of shipment of category 1 or category 2 quantities of radioactive material

§ 37.75(e)

The licensee shall retain a copy of the documentation for preplanning and coordination and any revision thereof, as a record for 5 years.

EXPLANATION:

Preplanning and coordination documentation must be maintained for 5 years.

QUESTIONS/ANSWERS:

Q1: How long must a licensee keep preplanning and coordination records?

A1: Licensees must retain preplanning and coordination records for 5 years. These records include the verification for license authorization for transfers of category 1 or category 2 quantities of quantities of radioactive material transfers, records related to preplanning and coordination, and records related to the advance notification for shipments of category 1 quantities of radioactive material. Licensees should also retain verification records.

§ 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. 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.

EXPLANATION:

Licensees must provide advance notification to the NRC and the governor of any State (or the governor's designee) for which a shipment licensed material in a category 1 quantity that passes through or across the boundary of the State.

QUESTIONS/ANSWERS:

Q1: What is an advance notification?

A1: An advance notification is a notice to the NRC and States that shipment of a category 1 quantity of radioactive material is being made on a set date.

Q2: What advance notifications would be required?

A2: Licensees must provide advance written notifications for shipments containing category 1 quantities of radioactive material. The advance notifications are made to the NRC and to any State through which a shipment will be transported. The State notification would be made to the governor or the governor's designee.

Advance notifications would not be required for shipments of category 2 quantities of radioactive material, unless the shipment falls within the scope of 10 CFR 71.97(b).

Q3: Why is the option of providing notification to a "governor's designee" permitted under the requirements of § 37.77?

A3: Allowing notification in advance of applicable shipments of category 1 quantities of radioactive material to a governor's designee provides flexibility to the governors of each state to determine the appropriate party to receive the information within each state. Since each state may have a unique administrative hierarchy, and public concerns regarding radioactive shipments may vary, each state's governor can determine the appropriate party to be informed in advance of a shipment through or across the boundary of the state.

Q4: What does State refer to in the requirements?

A4: As used in part 37, the term "State" means the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Q5: Where does a licensee obtain contact information for the governor's designee?

A5: A list of the contact information for the governor's designees is published annually in the *Federal Register* most recently on July 14, 2009 (74 FR 34053). 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.

Q6: How reliable, with respect to timely updating, is the contact information that is provided on the NRC website or from the NRC Headquarters' Office?

A6: Contact information provided on the web site, which includes telephone numbers and mailing addresses, can be revised very quickly. In general, however, much of the key information is rather unlikely to change, even if the names of the individuals in those positions to which the information pertains were to change. While the timeliness of information provided by mail from NRC Headquarters is slightly less robust, it is considered very unlikely that any changes which may occur while the information is being mailed to the requester will interfere with the shipper's ability to provide advance notification. The NRC contacts each State on an annual basis to request updated information.

Q7: Is it necessary to provide advance notification to the NRC if the shipment will only pass through Agreement States?

A7: A licensee will notify each state through which a shipment passes, regardless of whether the state is an Agreement State. In addition, the licensee would notify the NRC. An Agreement State licensee would notify the Agreement State.

Q8: What does NRC do when it receives shipment advance notification information?

A8: When NRC receives advance notification information, it shares the information with other relevant Government agencies, such as DOT and DHS.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material

§ 37.77(a)

Procedures for submitting advance notification.

(1) The notification must be made in writing to the office of each appropriate governor or governor's designee and to the NRC's Director, Division of Security Policy, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

(2) A notification delivered by mail must be postmarked at least 7 days before transport of the shipment commences at the shipping facility.

(3) A notification 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 of a shipment within or through the State.

EXPLANATION:

Advance notifications must be made in writing and postmarked 7 days before the shipment begins.

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 in as timely a fashion as other forms of communication. To make this more likely to occur, the mail notification must be sent sufficiently early to allow it to be postmarked at least 7 days before the shipment commences.

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.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material

§ 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:

(1) The name, address, and telephone number of the shipper, carrier, and receiver of the category 1 radioactive material;

(2) The license numbers of the shipper and receiver;

(3) A description of the radioactive material contained in the shipment, including the radionuclides and quantity;

(4) The point of origin of the shipment and the estimated time and date that shipment will commence;

(5) The estimated time and date that the shipment is expected to enter each State along the route;

(6) The estimated time and date of arrival of the shipment at the destination; and

(7) A point of contact, with a telephone number, for current shipment information.

EXPLANATION:

This section establishes the information that must be provided in an advance notification.

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 relevant available information when making an advance notification. As a minimum, licensees must include the following information in an advance notification for a category 1 shipment of radioactive material, if the information is available at the time of notification: (1) the name, address, and telephone number of the shipper, carrier, and receiver of the category 1 radioactive material; (2) the license numbers of the shipper and receiver; (3) a description of the radioactive material contained in the shipment, including the radionuclides and quantity; (4) the point of origin of the shipment and the estimated time and date that shipment will commence; (5) the estimated time and date that the shipment is expected to enter each State along the route; (6) the estimated time and date of arrival of the shipment at the destination; and (7) the contact and telephone number for the point of contact. For the purpose of coordination only, the actual information in the advance notification would not be considered to be SGI-M. Any information that is not available at the time of the initial notification must be provided in a revised notification when the information becomes available.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material

§ 37.77(c)

Revision notice.

(1) The licensee shall provide any information not previously available at the time of the initial notification, as soon as the information becomes available, 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.

(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 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 state in the notice that it is a cancellation and identify the advance notification that is being cancelled.

EXPLANATION:

If the schedule for a shipment is revised or cancelled the shipping licensee must notify each of the previously notified States and the NRC.

QUESTIONS/ANSWERS:

Q1: What should a licensee do if the shipment schedule is revised or the shipment cancelled?

A1: If the shipment schedule is revised or cancelled, the shipping licensee must notify the appropriate States and the NRC or Agreement State.

Q2: What mechanism should a licensee use to notify the States and the NRC?

A2: The rule does not specify a mechanism for revisions; therefore, the licensee can use the method that works best for them, as long as the information is provided before the no-later-than arrival time. For cancellations, the notice should be in writing, so an e-mail, facsimile, or written

correspondence can be used as long as the cancellation is received before the no-later-than arrival time.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material

§ 37.77(e)

Records. The licensee shall retain a copy of the advance notification and any revision and cancellation notices as a record for 5 years.

EXPLANATION:

Advance notification, revision, and cancellation records must be maintained for 5 years

QUESTIONS/ANSWERS:

Q1: What is the records retention requirement for advance notification, and revision and cancellation notices, for shipments of category 1 quantities of radioactive material?

A1: The shipping licensee must retain a copy of this information as a record for 5 years. If the revision or cancellation is accomplished by telephone, the license should keep documentation of the conversation.

§ 37.77 Advance notification of shipment of category 1 quantities of radioactive material

§ 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 the information as specified in § 73.21.

QUESTIONS/ANSWERS:

Q1: What do the information protection requirements in § 73.21 specify?

A1: Section 73.21 mostly addresses the general performance requirement 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 certain requirements that are provided in § 73.23.

Q2: Who is required to protect the schedule information?

A2: Any person that receives the schedule information or any other SGI or SGI-M information must protect the information in accordance with the requirements in § 73.21 through 73.23.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment

§ 37.79(a)

Shipments by road.

(1) Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 1 quantity of radioactive material shall:

(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.

(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.

(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.

(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 paragraphs establish the security provisions for shipping category 1 quantities of radioactive material by road.

QUESTIONS/ANSWERS:

Q1: When is the use of a movement control center necessary?

A1: 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 activity of the transport vehicle or trailer. The control centers would be required to monitor shipments on a continuous and active monitoring 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 control over the shipment and 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.

A2: What is meant by an “active monitoring” basis, as discussed in A1 above?

Q2: A movement control center is monitoring on an active monitoring 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 (1) if the shipment deviates from the planned route; (2) if any unscheduled stops occur; or (3) if any stops occur that are longer in duration than expected.

Q3: Where can the movement control center be located? Does it need to be on the licensees’ property?

A3: The movement control center must be a stationary facility (i.e., not a mobile vehicle), and can be located at either the licensee’s site or a third party site. Regardless of location, they must be able to monitor the category 1 shipment at all times and communicate with appropriate law enforcement agencies, should the need arise.

Q4: Are redundant communications necessary?

A4 Yes, redundant communications must be in place that would allow the transport vehicle to contact the movement control center, and LLEA if assistance is needed, at all times. While an escort vehicle is not required, if an escort vehicle is used, it must be able to communicate with the transport driver and the movement control center. The redundant communication must not be subject to the same interference factors as the primary communication method. The same interference factors mean any two systems that rely on the same hardware or software to transmit their signal (e.g., cell tower or proprietary network).

Q5: Why are redundant communications necessary?

A5: 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 in an independent fashion from the primary device, thereby minimizing the possibility that whatever disabled the primary device is unlikely to impact the redundant devices.

Q6: What is a telemetric position monitoring system?

A6: A telemetric position monitoring system is 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. The gathering of this information permits remote monitoring and reporting of the location of a transport vehicle or package. GPS and radiofrequency identification (RFID) are examples of telemetric position monitoring systems.

Q7: Would GPS be required?

A7: No, GPS would not be required. For category 1 material, continuous and active monitoring for shipments is required. Continuous and active monitoring means that at any time while the shipment is enroute, the licensee must be knowledgeable of the shipment's whereabouts. Not specifying a particular technology provides licensees with flexibility to design a continuous and active monitoring system that meets their unique circumstances. However, GPS would be considered an acceptable method.

Q8: When is a second individual needed for the shipment?

A8: 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. The accompanying individual may be another driver. This security measure provides reasonable assurance that the material will be protected from theft or diversion when it is stationary, as well as in emergency situations where it becomes necessary for the driver to stop or leave the vehicle.

Q9: What are the duties of a driver and a second accompanying individual?

A9: The driver (and/or the accompanying individual) must periodically call into the movement communication center to provide a verbal status of the delivery. The driver (and/or the accompanying individual) is expected to maintain constant visual surveillance of the surrounding environment during transport. If the driver requires a break and the transport vehicle stops, either the driver or the accompanying individual must maintain constant visual surveillance of the immediate environment of the transport vehicle while it is not in motion. At least one of the individuals must periodically walk around the transport vehicle during the time it is not in motion to help confirm there are no apparent safety-related or security-related issues associated with the vehicle. In addition, the periodic walk-around must include visual surveillance of the surrounding area to confirm there is no evidence of tampering with the contents of the vehicle or unusual or suspicious activity in the immediate vicinity of the transport vehicle. Note that the accompanying individual must 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

§ 37.79(a)

Shipments by road.

(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.

(3) Each licensee who delivers to a carrier for transport, in a single shipment, a category 2 quantity of radioactive material shall:

(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.

(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

(iii) Use carriers that have established tracking systems that require an authorized signature prior to releasing the package for delivery or return.

EXPLANATION:

These paragraphs establish the security provisions for shipping category 2 quantities of radioactive material by road.

QUESTIONS/ANSWERS:

Q1: What are the physical protection requirements for road shipments of category 2 quantities of radioactive material?

A1: Licensees shipping category 2 quantities of radioactive material by road must maintain constant control and/or surveillance during transit and have the capability for immediate communication to summon appropriate response or assistance. Licensees shall establish a security zone around the radioactive material. The licensee may use the transport vehicle as the security zone boundary. Access to the security zone shall be limited to authorized individuals. Licensees must monitor, detect and respond to any unauthorized access to the security zone. The licensee must maintain access control when the transport vehicle is stopped

at a hotel, restaurant, gas station, or other location. Additionally, the licensee must have the capability to summon the LLEA to request armed assistance for an actual or attempted theft of the radioactive material.

Q2: What are the requirements when a licensee delivers to a carrier for transport, in a single shipment, a category 2 quantity of radioactive material?

A2: The licensees must use a carrier that has an established package tracking system. An established package tracking system means a documented, proven, and reliable system routinely used to transport objects of value. The package tracking system must allow the shipper or transporter to identify when and where the package was last located and when it should arrive at the next point of control. The licensee is required to use a carrier that maintains constant control and surveillance during transit and has the capability for immediate communication to summon appropriate response or assistance. The carrier must also require an authorized signature prior to releasing the package for delivery or return.

Q3: What constitutes an appropriate “tracking system” for the requirement to use a carrier that utilizes a package tracking system during shipment?

A3: Licensees must use carriers that use package tracking systems for shipments containing category 2 quantities of radioactive material, per consignment. Such a tracking system must provide information concerning the accountability of, and chain of custody for, the package to assist the carrier and/or licensee in determining if the shipment is lost or missing and with any subsequent investigation (e.g., last known location and intended next location, time of last communication with driver, etc.).

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment

§ 37.79(b)

Shipments by rail.

(1) Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 1 quantity of radioactive material shall:

(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.

(ii) Implement an NRC-approved monitoring plan that is designed to prevent the use of the shipment for malevolent purposes while the shipment is in the classification yard.

(iii) Ensure that periodic reports to the communications center are made at preset intervals.

EXPLANATION:

This paragraph establishes 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: Licensees that ship category 1 quantities of radioactive material by rail must ensure that the rail shipments are monitored by a telemetric position monitoring system or an alternative tracking system reporting to a licensee, third-party, or railroad communications center which meets certain criteria. The communications center must provide positive confirmation of the location of the shipment and its status. The communications center also needs to be prepared to implement preplanned procedures in response to deviations from the authorized route or to a notification of an actual or attempted theft or diversion of a shipment, or any suspicious activity related to a shipment. These procedures include the identification of, and contact information for, the appropriate LLEA 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.

The licensee must have an NRC-approved monitoring plan to ensure that no unauthorized access to the shipment takes place while the shipment is in a railroad classification yard.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment

§ 37.79(b)

Shipments by rail.

(2) Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 2 quantity of radioactive material shall:

(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.

(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

(iii) Use carriers that have established tracking systems that require an authorized signature prior to releasing the package for delivery or return.

EXPLANATION:

This paragraph 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: As a minimum requirement, the licensee must have the capability to contact the shipping carrier and determine the approximate location of the shipment. Licensees shipping category 2 quantities of radioactive material by rail must use a carrier that has an established package tracking system. An established package tracking system means a documented, proven, and reliable system routinely used to transport objects of value. 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. The licensee is required to use a carrier that maintains constant control and surveillance during transit and has the capability for immediate communication to summon appropriate response or assistance. The carrier must also require an authorized signature prior to releasing the package for delivery or return.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment

§ 37.79(c)

Procedures.

(1) Each licensee who makes arrangements for the shipment of category 1 quantities of radioactive material shall develop written normal and contingency procedures to address:

(i) Notifications to the communication center and law enforcement agencies;

(ii) Communication protocols. Communication protocols must include a strategy for the use of authentication and duress codes and provisions for refueling or other stops, detours, and locations where communication is expected to be temporarily lost;

(iii) Loss of communications; and

(iv) Responses to an actual or attempted theft or diversion of a shipment, or any suspicious activities related to a shipment.

(2) Each licensee who makes arrangements for the shipment of category 1 quantities of radioactive material shall ensure that drivers, accompanying personnel, train crew, and movement control center personnel are appropriately trained in normal and contingency procedures.

EXPLANATION:

Licensees shipping category 1 quantities of radioactive material must have procedures for both normal and contingency situations and must ensure that workers are trained in the procedures.

QUESTIONS/ANSWERS:

Q1: What types of procedures and training are necessary for shipping category 1 quantities of radioactive material?

A1: Licensees shipping category 1 quantities of radioactive material must ensure that both normal (i.e., applicable during routine conditions) and contingency (i.e., applicable during unusual or unexpected events) operating procedures are developed to address notifications; communication protocols; loss of communication; and response to an actual or attempted theft or diversion of a shipment, or any suspicious activity related to a shipment. The licensee is required to ensure that drivers, accompanying personnel, railroad personnel, and movement control center personnel are appropriately trained in the normal and contingency procedures.

Normal operating procedures directly reflect the regulatory requirements, and describe activities conducted under routine or ideal circumstances or conditions. Contingency procedures must envision what could go wrong with respect to meeting the regulatory requirements during preparations for transport or during the actual transport of the radioactive material. Contingency procedures should address appropriate actions for both envisioned aberrant situations as well as those that are known to have previously occurred during notification or transport of radioactive material by any licensee.

Q2: What would be included in the communication protocols?

A2: The communication protocols must include a strategy for the use of authentication and duress codes and provisions for refueling or other stops, detours, and locations where communication is expected to be temporarily lost. A list of phone numbers applicable for use by the driver and the movement control center to notify LLEA in the event of an emergency is also required to be maintained and available.

Q3: Should a licensee document the training?

A3: Licensees are not required to document the training. In some cases, it will be the carrier and not the licensee itself that conducts the training. However, in order to demonstrate compliance with the requirement, licensees are encouraged to document that the training occurred.

§ 37.79 Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment

§ 37.79(d)

Investigations.

Each licensee who makes arrangements for the shipment of category 1 or category 2 quantities of radioactive material shall immediately conduct an investigation, in coordination with the receiving licensee, of any shipment that is lost or unaccounted for after the designated no-later-than arrival time in the advance notification.

EXPLANATION:

If a shipment does not arrive by the no-later-than arrival time, the shipping licensee must conduct an investigation.

QUESTIONS/ANSWERS:

Q1: What should a licensee do if the shipment does not arrive by the no-later-than arrival time?

A1: A licensee that has shipped category 1 or category 2 quantities of radioactive material must immediately initiate an investigation for any shipment that has not arrived at the receiving licensee's facility by the designated no-later-than arrival time. The no-later-than arrival time would be defined as 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 longer than 2 hours after the estimated arrival time for a shipment of category 1 quantities of radioactive material and 4 hours after the estimated arrival time for a shipment of category 2 quantities of radioactive material.

Q2: What should be included in an investigation?

A2: The licensee should have procedures that indicate the steps to be taken in the event an investigation is warranted. The type of investigation will depend on the circumstances of the lost or unaccounted for material. As a starting point, the licensee should check with the carrier to determine the last known location. If it is clear that the material was stolen, the licensee would defer to the LLEA investigation.

§ 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(d), 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 of the determination 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. An Agreement State licensee notifies the Agreement State.

Q2: How frequently should the licensee provide updates to the NRC Operations Center?

A2: The licensee should provide updates when new information is received. In addition, the licensee should discuss with the NRC what the frequency of needed updates should be. It will be determined on a case-by-case basis.

§ 37.81 Reporting of events

§ 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: When a licensee determines that a shipment of category 2 quantities of radioactive material is lost or missing, the licensee 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. An Agreement State licensee notifies the Agreement State.

§ 37.81 Reporting of events

§ 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 shall 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: What would a licensee be required to do if there is an attempt to steal or divert a category 1 shipment?

A1: For shipments of category 1 quantities of radioactive material, 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. An Agreement State licensee notifies the Agreement State.

Q2: What types of activities might be considered suspicious?

A2: Suspicious activities might include another vehicle seeming to follow or stay alongside the transport vehicle for long durations, someone asking the driver a lot of questions about their vehicle and its contents at a stop, or someone taking pictures of the vehicle either at stop or while the vehicle is moving, etc..

§ 37.81 Reporting of events

§ 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 shall 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: What would a licensee be required to do if there is an attempt to steal or divert a category 2 shipment?

A1: For shipments of category 2 quantities of radioactive material, 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 NRC Operations Center as soon as possible. An Agreement State licensee notifies the Agreement State.

Q2: What types of activities might be considered suspicious?

A2: Suspicious activities might include another vehicle seeming to follow or stay alongside the transport vehicle for long durations, someone asking the driver a lot of questions about their vehicle and its contents at a stop, or someone taking pictures of the vehicle either at stop or while the vehicle is moving, etc.

§ 37.81 Reporting of events

§ 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 shall notify the NRC and the LLEA upon recovery of any lost or missing category 1 quantities of radioactive material.

QUESTIONS/ANSWERS:

Q1: Should licensees make notification that a lost or missing category 1 shipment has been found?

A1: Yes. The licensee must notify the LLEA and the NRC Operations Center when a lost or missing shipment has been located. An Agreement State licensee notifies the Agreement State. This notification would be considered an update on the initial notification. Without this notification, regulatory authorities and LLEA would waste resources continuing any search for the material.

§ 37.81 Reporting of events

§ 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 shall 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 on the initial notification.

§ 37.81 Reporting of events

§ 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. 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 include sufficient information for NRC analysis and evaluation.

EXPLANATION:

The licensee must provide to the 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 types of information should be included in the written report?"

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. 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.

§ 37.81 Reporting of events

§ 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 is information on who stole the material, or that the device was found with the radioactive material removed.

Subpart E – (Reserved)

Subpart F – Records

§ 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:

Q1: Is a licensee required to keep the original of a record?

A1: No, a licensee is not required to keep the original of record. The licensee can keep a reproduced copy or a microform copy. A document may be retained as an electronic copy. The record must be legible.

§ 37.103 Record retention

§ 37.103

Licensees 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.

EXPLANATION:

Licensees are required to maintain records required by the regulations until the Commission terminates the license, unless a retention period is specified in the regulations.

QUESTIONS/ANSWERS:

Q1: If Part 37 does not specify how long to keep a record, is the licensee required to keep it and 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 until the license is terminated.

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:

None for this section.

§ 37.107 Violations

§ 37.107(a)

The Commission may obtain an injunction or other court order to prevent a violation of the provisions of --

(1) The Atomic Energy Act of 1954, as amended;

(2) Title II of the Energy Reorganization Act of 1974, as amended; or

(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 for this section.

§ 37.107 Violations

§ 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:

(1) For violations of --

(i) Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended:

(ii) Section 206 of the Energy Reorganization Act;

(iii) Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;

(iv) Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

(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 for this section.

§ 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 for this section.

Appendix A to Part 37—Category 1 and Category 2 Radioactive Materials

Table 1

Appendix A to Part 37—Category 1 and Category 2 Radioactive Materials

Table 1 – Category 1 and Category 2 Threshold[1]

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.

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

[1] Calculations 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 facility or

activity meets or exceeds the threshold and is thus subject to the physical protection requirements of this part.

I. If multiple sources and/or multiple radionuclides are present in a facility or activity, the sum of the ratios of the activity of each of the radionuclides must be determined to verify the facility or activity is less than the category 1 or category 2 thresholds of Table 1, as appropriate. Otherwise, if the calculated sum of the ratio, using the following equation, is greater than or equal to 1.0, then the facility or activity meets or exceeds the thresholds of Table 1, and the applicable physical provisions of this part apply.

II. Use the equation below to calculate the sum of the ratios by inserting the actual activity of the applicable radionuclides from Table 1 or of the individual sources (of the same radionuclides from Table 1) in the numerator of the equation and the corresponding threshold activity from the 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 = activity for radionuclides or source number 1

R_2 = activity for radionuclides or source number 2

R_N = activity for radionuclides or source number n

AR_1 = activity threshold for radionuclides or source number 1

AR_2 = activity threshold for radionuclides or source number 2

AR_N = activity threshold for radionuclides or source number 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:

The appendix lists the radionuclides and associated thresholds at which the material is considered to be a category 1 or category 2 quantity of radioactive material.

QUESTIONS/ANSWERS:

Q1: How does the sum of fractions work?

A1: The sum of fractions methodology, also known as the unity rule, is used to determine if Part 37 applies to a licensee because it is authorized to possess a category 1 or category 2 quantity of radioactive material. A licensee may need to implement the requirements in 10 CFR Part 37 even if it is not authorized to possess any single source or single radionuclide in excess of the category 2 thresholds. For combinations of materials (to include 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 would be required to consider all of the radioactive material

authorized on the license. The following formula for the unity rule would be used to determine if a licensee is required to implement the Part 37 requirements: [(total amount of radionuclide A) ÷ (category 2 threshold of radionuclide A)] + [(total amount of radionuclide B) ÷ (category 2 threshold of radionuclide B)] + etc.....≥ 1. If the sum is greater than or equal to 1, the licensee would be authorized to possess at least a category 2 quantity of radioactive material, and the 10 CFR Part 37 requirements would apply for that license. The Terabecquerels (TBq) thresholds are the regulatory standard, therefore for use in the above calculation convert Curies (Ci) to TBq as follows: n (TBq) = N (Ci) x 0.037 TBq/Ci.

Below are several examples.

Example 1: The licensee is authorized to possess:

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

(5TBq Co-60 + 5TBq Co-60)/0.3 TBq + (20 TBq Ir-192/0.80 TBq) = 58
The sum of fractions is greater than 1, therefore, the Part 37 requirements apply to this licensee.

Example 2: The licensee is authorized to possess:

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

(3 TBq Sr-90/10 TBq) + (0.5 TBq Cs-127/1 TBq) + (0.1 TBqAm-241/0.6 TBq) = 0.97
The sum of fractions is less than 1, therefore, the Part 37 requirements do not apply to this licensee.

Example 3: The licensee is authorized to possess:

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

(3 TBq Sr-90/10 TBq) + (0.55 TBq Cs-127/1 TBq) + (0.1 TBqAm-241/0.6 TBq) = 1.02
The sum of fractions is greater than 1, therefore, the Part 37 requirements apply to this licensee.

Example 4: The licensee is authorized to possess:

- 0.5 TBq Cs-137 (unsealed source)
- 0.3 TBq Co-60 (sealed source)

(0.5 TBq Cs-137/1 TBq) + (0.3 TBq Co-60/0.6 TBq) = 1
The sum of fractions equals 1, therefore, the Part 37 requirements apply to this licensee.

For examples 1, 3, and 4, the extent to which the Part 37 requirements apply depends on the licensee's circumstances and depends on whether an individual has unescorted access to the material and whether the material is aggregated.

The same type of calculation can be conducted to determine if a licensee actually possess a category 1 or category 2 quantity of radioactive material