Final Report Submitted to the NRC
March 17, 2016

REVIEW OF THE NRC'S 10 CFR PART 37 REGULATIONS AND THE COMPLETENESS OF THE NRC'S PROGRAM REVIEW TEAM'S REVIEW

Brian Dodd, Ph.D.

Independent Assessment Consultant

10313 Cogswell Avenue
Las Vegas, NV 89134

702-254-2346
Cell: 702-219-9021
BDC.mail@cox.net

Table of Contents

1. Overview

1.1. Introduction

This report was written in partial fulfilment of a contract the principal objective of which was to provide an external review and assessment of the 10 CFR Part 37 regulations and guidance to protect risk-significant radioactive materials. Specifically it was to evaluate the NRC's Part 37 internal program review and the completeness of the staff's activities in this regard.

Included in this was the review of the staff's activities related to:

- Comparison of Part 37 to International Atomic Energy Agency (IAEA) recommendations, and to radioactive material security program requirements in other countries (Sections 2, 3, 4, 5, 6, 7).
- Review of inspector training for Part 37 security inspections (Section 8).
- Assessment of background investigations and access control programs, including review of trustworthiness and reliability (T&R) investigations (Section 9).
- Location and tracking of high-risk radioactive sources (Section 10).
- Enforcement and Security Issues Forum (SIF) results (Section 11).
- Inspection experience (Section 12).
- Physical protection during use, storage and transport, including aggregation of sources (Section 13).

1.2. Completeness of the Program Review Team's Activity

The work of the NRC's internal Program Review Team (PRT) continued in parallel to this review. This presented a number of difficulties in that it was a dynamic situation. This report was continuously updated during the term of the contract and in this way it contributed to the direction of the PRT's work. However, the work of the review team continues past the end of this contract and it should be recognized that the text of this report may quickly become out-of-date.

This section will summarize the current status of the PRT's work in each of the program areas. More details are provided in the topic-specific sections.

In order to provide as much value-added content as possible, the report also includes an independent discussion and evaluation of the various areas where appropriate as well as recommendations arising therefrom.

1.2.1. International Comparisons

Comparisons have been finished with all of the relevant IAEA's guidance documents, including NSS-8, 9 and 11. Work has also been completed on comparisons to several other countries' national regulations.

1.2.2. Inspector Training

The PRT has performed a complete review of all the areas of training that it considers to be within its scope.

1.2.3. Trustworthiness and Reliability

A fairly comprehensive review of the access authorization issues has been completed. It includes a comparison with the equivalent nuclear power plant requirements to determine if there are useful lessons regarding their differences. It also discusses the recently issued Temporary Instruction to inspectors to gather T&R data. However, useful results from this will take some time to gather. As well as a review of some other issues identified, it concludes with a comparison with other agencies' T&R procedures, particularly their disqualifying criteria.

1.2.4. Source Tracking

The PRT has reviewed a number of issues with the National Source Tracking System and made some observations with respect to it. The broader issues relating to a complete knowledge of the location and movement of sources have not been addressed.

1.2.5. Enforcement and Security Issues Forum

An action plan has been submitted that covers the work done so far as well as that in progress and planned. The action plan is quite thorough and when complete it should provide valuable information for the PRT.

1.2.6. Inspection Experience

The PRT has performed some analysis of inspector questionnaires and inspection reports. This work is progressing, but needs to be written up with appropriate observations and/or recommendations.

1.2.7. Physical Protection during Use, Storage and Transport

An outline of a program of work has been drafted; however care needs to be taken to ensure that it does not replicate work already done on events and violations by those dealing with enforcement and the Security Issues Forum.

An astute review of the issues relating to aggregation, particularly as they relate to well-logging, is reaching completion and some observations and recommendations made.

1.3. Positive Aspects of the Part 37 Regulations and Guidance

One objective of this report is to identify positive aspects and elements of the existing radioactive material security regulations and guidance that are clear in mitigating security vulnerabilities and should be preserved.

1.3.1. General Comments

- The USA and the NRC in particular is one of the world leaders in nuclear facility and radioactive material regulation. Many countries look to the NRC as an example of a well-organized agency with quality regulations. This needs to be recognized and acknowledged up front.
- The majority of Part 37 is largely consistent with international guidance, but with some significant exceptions that are discussed later.
- The Part 37 regulations are generally quite clear, and provide a balance of performance and prescriptive regulations. There is also a good balance between keeping risk-significant radioactive sources secure and keeping regulations from being overly burdensome.
- The two major guidance documents (NUREG-2155[1] and NUREG-2166[2]) on implementing Part 37 are comprehensive, useful and generally well-regarded by licensees and inspectors alike.
- While being criticized for not giving more definitive details, the T&R guidance is significantly more prescriptive than that given in the IAEA documents that are used by many countries.
- The S-201 materials security course for inspectors has good content and appears to be useful and well-received by students.

1.3.2. Specific Comments

- Continue to allow subjective evaluations for trustworthiness and reliability determinations and do not issue hard and fast disqualification criteria (9.6).
- While the National Source Tracking System (NSTS) may be upgraded or expanded with time, it seems to be tracking changes in the status of sources effectively (10.5).
- Most of the violations of Part 37 appear to be more administrative in nature, such as not having written procedures, rather than actual lapses in source security (11.1, 11.2).
- Generally, the guidance, training and tools for inspectors have been adequate, but continuous improvement needs to be maintained (12.3).
- Retain the sum of the fractions method for determination of a category for an aggregated quantity (13.2.2).

1.4. Summary of Recommendations

In each topic and sub-topic area in the body of the report a brief **summary** is given along with a **discussion** of the issue and a final **recommendation**. Most recommendations are also consolidated here along with references to the applicable section of the text where they are made.

1.4.1. Major Recommendations

There are two recommendations in this report that are significant enough to be recognized separately.

- Come to a common agreement with the National Nuclear Security Administration (NNSA) on threats assessments, potential adversary capabilities and the security standards required to meet these threats. Adjust Part 37 as necessary (1.5.2).
- Revise Part 37 to include graded security measures for Category 3 sources in storage, use and transit (3.2.1, 4.2.3, 4.3.3) and expand the NSTS to include Category 3 sources (10.4.2).

1.4.2. Recommendations

- Focus on improving compliance with existing regulations, especially in industrial radiography (1.5.1).
- Revise Part 37 to include all radionuclides for which there are D-values (2.2, 10.4.3).
- Revise Part 37 to require a delay greater than the estimated local law enforcement agency (LLEA) response time for Category 1 sources (3.3.1).
- Revise Part 37 to require two means of identification and verification for access into a security zone with Category 1 sources (3.4.2).
- Stay abreast of the development of the revisions to IAEA security documents and take the updates into consideration during any revisions of Part 37 and its guidance (3.5, 4.5).
- Adjust the scope of background checks in a graduated manner for T&R determinations, perhaps including an SF85P type form (5.2, 9.5).
- Consider adding a two person requirement and check searches for Category 1 sources, at least during higher risk situations such as source transfer and device maintenance (5.4, 5.6).
- Obtain feedback on the inspector training program from a wider variety of sources (8.2, 8.3, 8.4).
- Begin planning for the transfer of personnel and resources away from Gap training and towards the development of a refresher training module for Part 37 (8.7).
- Analyze the data regarding T&R from the Technical Instruction on the subject as it arrives with a view to informing revised regulations or guidance (9.3).
- Seek advice from appropriate government agencies about how to help licensees perform background checks on foreign nationals (9.6.2).

- Seek feedback from licensees on all aspects of radioactive source location and tracking not just the NSTS (10.2).
- Reconsider requiring real-time tracking of mobile sources as device technology develops (10.3).
- Critically review and evaluate the regulations and guidance related to the most frequent citations to determine whether the causes are due to lack of clarity in the requirements (11.1).
- Continue to analyze the data on violations to try and draw conclusions that may result in further improvements to Part 37 or its guidance (11.2).
- Examine the Security Issues Forum's process and its development of enforcement examples with a view to speeding up the decision making process and publication of guidance to the regions (12.1).
- Continue to seek feedback from inspectors regarding how their guidance, training and tools can be improved (12.3).
- Redefine aggregation; not to change the meaning, but to make it better English and thereby clearer (13.2.1).
- Adopt the guidance, training and source management changes recommended by the PRT for well-logging licensees and inspectors (13.2.4).
- Include Category 3 sources in Part 37 as previously recommended to eliminate the problems related to aggregation of well-logging sources (13.2.4).

1.5. The Security of Radioactive Material Regulatory Program

1.5.1. Regulations, Compliance and the Nuclear Materials Event Database

Summary: An effective regulatory program has both good regulations and good compliance. Reportable event data indicate that getting good compliance is more of a problem than the quality of the regulations.

Discussion: The overall effectiveness of Part 37, or indeed any regulatory system, comprises two components. One is the regulations themselves and the other is the compliance with the regulations. The matrix below illustrates the point that to be most effective both the regulations and the compliance have to be good. Quality regulations with poor compliance result in weak security and vice-versa.

Table 1. Regulations and Compliance

Regulations / Compliance	**Good**	**Poor**
Good	Best	Weak
Poor	Weak	Worst

In a situation with limited resources the question becomes where are those resources best used to provide the largest benefit in security, i.e. in improving the regulations or improving the compliance? Some indication of this might be obtained by examining the information in the Nuclear Materials Event Database (NMED). A review of NMED data for lost, abandoned or stolen sources (LAS) over the last 10 years provides the following table (ignoring irretrievable well logging sources).

Table 2. Event Data on Lost, Abandoned or Stolen Sources over 10 years

	Sources	**Events**				
		No.	**Shipping Error**	**Theft**	**Other/ Unknown**	**Fell off truck/ Left behind**
Category 1	Multiple*	2	2	0	0	0
Category 2	48	32	11	6	2	13
Category 3	35	35*	13	0	16*	6

*Detailed data unavailable.

A glance at this table and an analysis of the underlying data show that human error is by far the most common cause of loss of control. This would suggest that the number of reportable events involving Category 1-3 sources could be significantly reduced by improving compliance with existing regulations rather than revising them. It also shows that loss of control of sources is more of a safety issue than a security issue, in that there were few thefts and none of them seemed to be associated with malicious intent. Many of thefts were ancillary to a vehicle theft and several of them also involved human error as well. Shipping related errors were the most common problem with all categories of sources. Almost all of the Category 2 events involved ^{192}Ir industrial radiography sources and this too provides an indicator as to where the biggest compliance effort should be directed. The number of events and sources are about the same for Category 3 as they are for Category 2.

Recommendation: Focus on improving compliance with existing regulations, especially in industrial radiography. This will reap more rewards in reducing reportable events than changing regulations.

1.5.2. Regulations, Threats and Vulnerabilities

Summary: Threats and vulnerabilities need to be assessed and used as the basis for security regulations to prevent or minimize potential malicious events. However, the NNSA and the NRC have different approaches to threats analyses that lead to different security requirements. They should come to a common agreement on the threats, potential adversary capabilities and associated security standards for any given type of source.

Discussion: In setting regulations, the other aspect that must be considered is the threat of malicious action. Even though there are few past source thefts that have been associated with malicious acts in the USA, improving the security of dangerous sources is necessary to protect against potential future attacks in an increasingly threatening environment. The difficult

question to answer is: are the existing Part 37 regulations sufficient to prevent, or minimize the likelihood of, an event that has not yet happened? Regulations must be written to handle some assumed threat.

To quote the IAEA[7]: *"Security requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness of a radioactive source, the nature of the source and potential consequences associated with its unauthorized removal or sabotage. This graded approach ensures that the highest consequence sources receive the greatest degree of security".*

Two methods are typically used, one is to make a national threat assessment and base the security regulations on that. The other is to develop a design basis threat (DBT), including adversary capabilities, and design the regulations to counter that DBT. In the case of radioactive materials security, the Commission decided to use the threats assessment rather than the DBT approach. Security considerations did not allow review of the threats assessment or the rationale for picking this over the DBT approach, and consequently it is outside the scope of this report. However, it seems that the PRT requested and obtained an updated threats assessment review and were told that it has remained relatively unchanged since the Part 37 regulations were drafted.

Of more concern to this report is the fact that it seems that the NNSA has quite a different approach to source security than the NRC. Their use of potential adversary capabilities and the focus on the insider threat results in them increasing security for the same source beyond that required by the NRC to meet Part 37. While licensees appreciate the free training and security upgrades from the NNSA, having two separate standards is incomprehensible and confusing. It is understood that threats assessment is not an exact science and each analysis could well result in a different estimate as to what the true threat really is, but government agencies should be consistent. There must be a common agreement for a given type of radioactive source in a given location and the security standard set accordingly. To do otherwise is totally incongruent and conveys the impression that source security regulations are random and arbitrary. It then becomes hard to convince licensees to comply with such regulations.

Recommendation: The NNSA and the NRC should come to a common agreement on threats assessments, potential adversary capabilities and the security standards required to meet these threats. These standards should then be compared with those assumed in Part 37 and any necessary revisions made.

2. Radionuclide Scope of Part 37, IAEA Guidance and Other Countries' Regulations

2.1. Introduction

In general, the NRC's Program Review Team (PRT) has done a very good job at carefully comparing the IAEA's guidance with Part 37, identifying differences and making recommendations for change when needed. The team member responsible for this area is commended for her effort. This report will only discuss significant areas worthy of comment at the time of writing.

A major difference between the Part 37 regulations, IAEA guidance and other countries' regulations is the scope of the radionuclides that are covered. While not explicitly discussed in each of the sections below, this difference permeates all of the international comparisons with Part 37, i.e. Category 1 and 2 in NRC texts is not the same as Category 1 and 2 in the text of the IAEA documents or the rest of the world's regulations. The PRT takes the view that this is not an observation because the Code of Conduct allows states to limit the scope of radioactive sources considered: *"States should give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if employed for malicious purposes…"* The PRT argues that the multi-agency Radiation Source Protection and Security Task Force has done this in its 2010 report[4] and re-affirmed the analysis in its 2014 report[5]. In contrast, this current report recommends that all radionuclides be included.

2.2. Radionuclide Scope of Sources Covered

Summary: Part 37 only covers 15 radionuclides rather than the ~370 included in IAEA guidance. Only including these few radioactive isotopes is inconsistent with the normal federal regulatory approach and IAEA guidance. All the radionuclides for which D-values are provided should be included.

Discussion: Part 37 only covers Category 1 and 2 sources of the 16 radioactive materials (15 radionuclides) listed in Table 1 of Appendix A. The IAEA provides D-values[3] for over 370 radioactive materials. When the IAEA and most other countries talk about Category 1 and 2 sources they are talking about *all* sources that have activities above 1000D and 10D for each of these ~370 radionuclides. The NRC is excluding over 350 radionuclides.

It has been argued that the 16 radioactive materials are the only ones to which the Code of Conduct[8] applies, since they are the only ones above the line of Table 1 of Annex I of the Code. However, the Annex I text says that *"Table I provides a categorization by activity levels for **radionuclides that are commonly used**. These are based on D-values which define a dangerous source i.e.: a source that could, if not under control, give rise to exposure sufficient to cause severe deterministic effects. A **more complete listing** of radionuclides and associated activity levels corresponding to each category, and a fuller explanation of the derivation of the D-values, **may be found in TECDOC-1344**, which also provides the underlying methodology that could be*

applied to radionuclides not listed. ***Typical source uses are noted above for illustrative purposes only.****" (Emphasis added.)* So it is clear that there is no intention that the Code should only apply to the 16 radionuclides above the line, or even only the 26 radionuclides in the table.

The multi-agency Radiation Source Protection and Security Task Force in its 2010 report[4] re-evaluated the radionuclides and quantities of greatest security concern to the USA. It began with 3,715 radionuclides and through a five-step, down-selection process essentially concluded that there was no reason to change the listing from that currently in Table 1 of Appendix A of Part 37 i.e. those provided in IAEA Code of Conduct, Annex I, Table 1, above-the-line. The Task Force's latest report[5] (2014) adds nothing further to the analysis and also recommends no change. Essentially, the task force has determined that sources of all other radionuclides (and categories below Category 2) are below regulatory concern for security purposes.

There is no argument that the radionuclides included in Part 37 are the most risk-significant from a security of radioactive sources viewpoint. This much is clear. However, to only include these sources is inconsistent with the general NRC and federal approach to regulations. For example, the tables in Part 20, Appendices B and C include hundreds of radionuclides even though only some of them are significant for the regulatory purposes for which they are listed. Similarly, the Department of Transportation regulations for radioactive materials lists hundreds of radionuclides in its reportable quantity tables, and in its tables of A_1 and A_2 values, even though most of these are never transported.

Conversely, if the NRC applied the same logic to the safety of radioactive materials as it does for security of sources, there would be exclusions in the regulations relating to quantities and radionuclides for which there is no potential harm. NRC regulations should be consistent. Either apply a below regulatory concern approach to both safety and security or apply it to neither. However, since a below regulatory concern rulemaking has been abandoned for safety this approach should not be used for security.

Therefore, for a consistent regulatory approach and because Category 1 and 2 (and Category 3, see 3.2) sources of all radionuclides are by definition dangerous, such quantities of ***all*** radionuclides should be included in Part 37.

Recommendation: Revise Part 37 to include all the radioactive materials for which the IAEA has provided D-values, not just 16 of them.

3. Comparison of Part 37 to the IAEA's Security of Radioactive Sources Guidance

3.1. Introduction

Comparisons with the IAEA's Security Level A for Category 1 sources and Security Level B for Category 2 sources have been analyzed well and comments related to these are included below. The biggest omission in the initial PRT analysis was Security Level C and Category 3 sources. This has since been remedied and the major differences between the IAEA's guidance regarding these sources and that in Part 37 have now been included as observations.

It should be noted that the IAEA is currently revising its main guidance document on the security of sources and re-naming it the Security of Radioactive Material in Use and Storage and of Associated Facilities[6]. The PRT has reviewed this draft, and made similar comments regarding the significant distinctions in the revision as those in Section 3.5. However, the focus of this current section is on existing IAEA guidance.

3.2. Security Level C – Category 3

3.2.1. Category Scope of the 10 CFR Part 37 Regulations

Summary: The Part 37 regulations only apply to Category 1 and 2 radioactive sources whereas the IAEA's Code of Conduct on the Safety and Security of Radioactive Sources[8] and the IAEA's security guidance[7] also cover Category 3 sources. Part 37 should be revised to include provisions for additional security of at least all the Category 3 sources listed in Annex I of the IAEA Code of Conduct, but preferably all radionuclides per Section 2.2.

Dangerous Sources: The NRC's mission statement says: "The NRC licenses and regulates the Nation's civilian use of radioactive materials to protect public health and safety, promote the common defense and security, and protect the environment."

Category 1, 2 and 3 sources are dangerous[23]. A dangerous source is *"a source that could, if not under control, give rise to exposure sufficient to cause severe deterministic effects"*[23]. If part of the NRC's mission is 'to protect public health and safety' it is hard to understand why it does not include security of dangerous Category 3 sources in Part 37. See Appendix I for photos of injuries caused by Category 3 sources.

The non-inclusion of Category 3 sources is a significant deviation from international guidance, the purpose of which is to provide *"support for the international harmonization of measures for the control of radiation sources and their security"*[23]. In this regard the USA is not harmonized.

Code of Conduct: Furthermore, the USA was one of the first signatories to the IAEA's Code of Conduct on the Safety and Security of Radioactive Sources[8] as well as a major force in the development of the 2003 revision yet it does not conform to the Code. The Code states that it *"applies to all radioactive sources that may pose a significant risk to individuals, society and the*

environment, that is the sources referred to in Annex I of this Code." Annex I includes Category 3 sources of certain radionuclides.

In the section on legislation and regulations, the Code states:

"18. Every State should have in place legislation and regulations that:

(a) prescribe and assign governmental responsibilities to assure the safety and security of radioactive sources;

(b) provide for the effective control of radioactive sources;

(c) specify the requirements for protection against exposure to ionizing radiation; and

(d) specify the requirements for the safety and security of radioactive sources and of the devices in which sources are incorporated.

19. Such legislation and/or regulations should provide for, in particular:

…

(g) requirements for security measures to deter, detect and delay the unauthorized access to, or the theft, loss or unauthorized use or removal of radioactive sources during all stages of management;"

The NRC has argued that the requirements in 10 CFR Part 20.1801 and 1802 as well as requirements for specific licenses (industrial radiography, medical, well-logging) provide adequate security of Category 3 sources. However, these provisions clearly do not meet the guidance in 19.(g) of the Code of Conduct. Nor do they meet the guidance in the IAEA's Security of Radioactive Sources, NSS-11[7] in many significant respects.

NRC's Regulatory Analysis: The NRC's own Regulatory Analysis for Final Rule Expansion of the National Source Tracking System (NSTS)[9] is relevant in this context. The staff recommended that the NSTS be expanded to include Category 3 sources (but the Commission's 2-2 split decision stopped the process). If the staff recommended expanding the tracking system with such justifications as those quoted below, surely it should recommend expanding the security requirements in Part 37 to Category 3?

*"**Public Health (Accident/Event).** Expanding the NSTS to Category 3 sources would provide a life cycle account for these sources, which will improve accountability and control over the sources which should have a positive effect on public health."*

*"**Safeguards and Security Considerations.** Expanding the NSTS to Category 3 sources will provide a life cycle account for those nationally tracked sources, and will enhance NRC's ability to protect public health and safety".*

"Lowering the NSTS tracking threshold to include Category 3 sources will improve regulatory oversight and licensee accountability of these sources which the IAEA has defined as dangerous sources and are a security concern if there is minimal control regarding authorized possession."

Potential Issues: In the development of the Revised Code of Conduct there was discussion relating to the practical difficulty of including Category 3 sources because of their large number. This is the pragmatic reason for the 'as a minimum' wording of Section 11 of the Code, which was a compromise with those who wished to include Category 3.

"11. Every State should establish a national register of radioactive sources. This register should, as a minimum, include Category 1 and 2 radioactive sources as described in Annex 1 to this Code."

It is perhaps also the reason why the Commission did not agree to the staff's recommendation to extend the National Source Tracking System[9] (NSTS) to include Category 3 sources. The NRC has stated that there are about 8,000 Category 1 and 2 sources and about 1,400 licensees of these sources. The NRC estimates[9] that there are about an additional 5,200 Category 3 sources and about an additional 1,000 licensees of these sources. Revising Part 37 to include Category 3 sources will have a significant impact on licensees, but it will also improve the security of the most desirable sources from a terrorist viewpoint, i.e. the still dangerous, but the less secure, and more readily acquired Category 3 sources. To this end it seems as if the Global Material Security program, having secured most of the Category 1 and 2 sources is now continuing its mission by securing the higher activity Category 3 sources.

Recommendation: Include additional security measures for Category 3 sources in Part 37 consistent with the graded approach in current regulation and NSS-11[7] Security Level C. As a minimum include the radionuclides in Annex I of the Code of Conduct, but preferably include all the radionuclides (per Section 2.2).

3.3. Security Level A – Category 1

3.3.1. Objectives and Delay

Summary: The IAEA's goal for the security of Category 1 sources is to prevent removal, while the NRC's goal is to respond to unauthorized access to Category 1 (and 2) sources. This is a major difference that needs resolution (or better justification). Since Category 1 sources are extremely hazardous the possibility of their removal and malicious use is of particular concern. Therefore, Part 37 should be modified to bring it as close as practically possible to the IAEA objective.

Discussion: The IAEA's goal for Security Level A, which is applicable to Category 1 sources, is to *"prevent unauthorized removal of a source"*[7] and its objective of response is specifically to *"provide immediate response to assessed alarm with sufficient resources to **interrupt and prevent the unauthorized removal**"*. This is different than Part 37, where the general performance objective in 37.41.(b) is that *"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"* and in 37.49.(d) *"requesting, without delay, an armed response from the LLEA"*.

There are two considerations at the heart of the difference. First, neither the USNRC, nor a licensee, has the jurisdiction over local law enforcement agencies (LLEAs) to require a response sufficiently quickly and with sufficient resources to 'interrupt and prevent' unauthorized removal. Second, while Part 37 requires a security zone as well as *"immediate detection of any attempted unauthorized removal of the radioactive material from the security zone"* there is no specific requirement for delay time to be built into physical barriers.

It has been argued that most Category 1 sources are large and difficult to move or remove from their devices or shielding. Further, if unshielded they would be lethal within a few minutes to an hour and, therefore, they are 'self-protecting'. Suffice it to say that there is classified evidence to dismiss the validity of these arguments.

Even though the NRC has no authority over LLEAs, it might still be possible to move closer to the IAEA's goal of preventing source removal by modifying the regulations to include a performance requirement relating to built-in delay. The Category 1-only requirement could read something like: *The security zone shall include barriers designed to provide a delay time greater than the estimated LLEA armed response time.* This gets around the jurisdiction problem and the local variability problem because all the licensee would have to do is ask the LLEA what its estimated average armed response time would be. The licensee would then use that as the basis of the security zone design using a standard security analysis of the delay associated with various types of barrier constructions against a given threat capability. It seems that these data are available, but this approach assumes that the NRC can obtain such information and provide it with an appropriate classification to Category 1 licensees.

It is recognized that a facility designed to provide a certain delay for a given threat capability in real life may or may not result in an actual delay sufficiently long for the armed response to interdict the actual adversary and prevent removal of the source, but it should provide a significantly better chance of success than just meeting the current requirements.

Recommendation: Modify Part 37 to bring it as close as practically possible to the IAEA objective for Category 1 source security by including a requirement something like: *The security zone shall include barriers designed to provide a delay time greater than the estimated LLEA armed response time.*

3.4. Other Issues Identified

3.4.1. Adjustments for Mobile Uses

Summary: NSS-11 in Appendix IV gives illustrative security measures. Under adjustments for mobile uses, Security Level B, in the response section, it lists *"Immediate initiation of response to interrupt",* with the suggestion of providing LLEAs advance notice of their presence to help achieve this. The NRC does not have a requirement for advanced notice. However, there is no difference in the real IAEA requirement and what is included in Part 37 and therefore this issue need not be considered further.

Discussion: The PRT initially made this an observation, noting that advanced notice was considered during the drafting of Part 37 and rejected, partly because of the practical difficulties of implementation. However, it should be noted that Appendix IV is only *'illustrative'*. The actual relevant text in Table 2 is *"Implement appropriate action in the event of unauthorized removal of a source."* This does not even specify an LLEA response. This report notes that the IAEA guidance itself is sufficiently covered in Part 37.49.(d), and therefore, the item should not be an observation.

A cursory evaluation of national average response times to 911 emergency calls seems to be about 10 minutes according to the American Police Beat[10]; however there may be a wide range of response times. Even if the licensee takes no individual action other than calling 911 requesting an LLEA response it is felt that this adequately meets the NSS-11 guidance.

Recommendation: Since there is no significant difference between the IAEA guidance and Part 37 requirements this item should not be an observation, nor considered any further.

3.4.2. Access Controls for Security Level A

Summary: NSS-11-suggested security measures for Security Level A (Category 1) include a combination of two or more verification measures e.g. swipe card plus a PIN. Part 37 does not include any set number of ways. Since this is a relatively easily implemented, graded measure that provides additional security for Category 1 sources, it should be included in Part 37.

Discussion: The PRT initially did not make this an observation, but this status was later changed. The two means of verification is a recommended IAEA security measure to meet the security objective: *"Provide access controls to source location that effectively restrict access to authorized persons only."* While this objective is common to all security levels, NSS-11 does state *"Where an objective is shown in Table 2 as the same for two or more security levels, it is intended that the objective be met in a more rigorous manner for the higher security level."* Requiring two verification measures for Security Level A and one for Security Levels B and C seems like an appropriate graded approach.

Recommendation: Revise Part 37 to require two means of identification and verification for access into a security zone with Category 1 sources, especially since it is quite easy to implement.

3.5. Draft Revision of Security of Radioactive Material in Use and Storage and of Associated Facilities

Summary: The IAEA is in the process of revising NSS-11 and has issued a draft for member state comment. The PRT has reviewed the draft and come to similar conclusions as this report i.e. there is no significant impact on the Part 37 review effort.

Discussion: The IAEA is revising its basic security of sources guidance document (NSS-11) and has released a draft for member state comment. An initial review of the draft revised document[6], published in January 2016 for member state comment, indicates that there are few changes that

impact the previous discussion in this report. Generally, the changes are positive and improve the clarity of the guidance. A discussion of some of the main distinctions follows.

Recommendation: The NRC should stay abreast of the development of the revisions to this and other IAEA documents and if Part 37 or its guidance is revised, take the updates into consideration.

3.5.1. Expansion of the Scope

The draft clarifies that the implementing guide applies to all radioactive material and not just sealed radioactive sources. It specifically mentions radioactive waste, unsealed radioactive material and large components such as those from nuclear facilities. Consequently, it has an expanded section on how to adjust categorization (up or down) to determine an appropriate security level (A, B or C) based on such things as practice, mobility/portability, increased threat, half-life, ease of handling, large volume activated or contaminated objects, location and waste.

3.5.2. Portable Sources

In NSS-11, while portable sources were considered in Security Level B, the adjustments of measures for them were included in the last appendix. In the revised draft, they are directly included in the Security Level B table in the main body of the document. This emphasizes their significance.

3.5.3. Security Management

The security management measures in the draft document are separated out and expanded in scope. These measures, including T&R determinations and security plans, apply to all security levels (A, B and C), but are intended to be applied in a graded approach. Generally, all the measures are covered in Part 37, but as noted elsewhere, Part 37 only applies them to Category 1 (≡ Security Level A) and Category 2 (≡ Security Level B), but not to Category 3 (≡ Security Level C) sources.

4. Comparison of Part 37 to the IAEA's Security in the Transport of Radioactive Material Guidance

4.1. Introduction

The Program Review Team has made a comprehensive comparison of the IAEA's guidance on transport security with Part 37 as well as the Department of Transportation's regulations and has drawn generally reasonable conclusions. The text in this report provides an additional independent assessment and in some cases reaches different conclusions.

Again, it should be noted that the IAEA is currently revising its main guidance document on the Security of Radioactive Material in Transport[11]. The PRT has not reviewed or analyzed this draft, but this report provides comments on the significant distinctions in the revision in Section 4.5.

4.2. Security Levels and their Thresholds

The IAEA's Security in the Transport of Radioactive Materials[12] guidance includes three security levels entitled: *"enhanced security level", "basic security level", and "prudent management practices"*. It also has provision for additional security measures for particularly sensitive transports or during times of increased threat. Some of the thresholds of these levels differ from the Part 37 equivalent and some of the requirements are different. The threshold levels are discussed here and their associated measures later in Section 4.3. To help in the comparison, the chart in Appendix II was generated.

4.2.1. Enhanced Security Level Threshold

Summary: The thresholds for the higher security requirements in Part 37 and NSS-9 have subtle differences. An analysis shows that the Part 37 threshold is more conservative and simpler to apply and therefore, need not be changed.

Discussion: The threshold of the enhanced security level in NSS-9 for those radionuclides covered in Annex I of the Code of Conduct is 10 times the D-value per package i.e. Category 1 and 2 materials. For all other radionuclides it is 3000 times the A_2 value per package. In contrast, Part 37 requirements cover Categories 1 and 2 for all radionuclides. Part of the reason for the IAEA's inclusion of A_2 values is to attempt to account for denial of use (of property) from radioactive material dispersion, rather than just the deterministic health effects upon which the D-values are based.

Of the ~370 radionuclides given in the D-value and A-value tables, several of them have unlimited values. An analysis of the rest shows that in all but three cases 10 times the D-value is smaller than 3000 times the A_2 value. This means that Part 37 is more conservative than NSS-9 by generally requiring the enhanced security measures at lower levels than NSS-9. Further, Part 37 is simpler to apply because only D-values are referenced rather than two criteria.

If Part 37 is revised to specifically include Category 3 sources in a graded approach, then another threshold clearly will need to be introduced; however, there seems to be little benefit in modifying the Category 2 and above threshold in Part 37.

Recommendation: There does not seem to be any reason to adopt the combination threshold (10D or $3000A_2$) that is used in the IAEA guidance given in NSS-9.

4.2.2. Additional Security Measures Level

Summary: The IAEA has provisions for increasing security under certain circumstances and provides some suggestions for the increased measures. While the NRC regulations do not have any such provision, the security measures for Category 1 quantities include many of the same requirements and therefore Part 37 should not be changed in this regard.

Discussion: NSS-9 has provisions for increasing security *"in view of the design basis threat, the assessment of the prevailing threat, or the nature of the material being transported"*. Part 37 has no equivalent. However, Part 37 makes a distinction between certain requirements for Category 1 and those for Category 2. Many of the additional security measures in the IAEA guidance are already included in the Part 37 requirements for Category 1 quantities. Furthermore, the list in NSS-9, Section 4.4 is *'not exhaustive'* and includes things *"States may consider"*. In light of these considerations, there does not seem to be a need to revise Part 37 to allow for special additional security measures.

Recommendation: Many of the additional security measures in the IAEA guidance are already included in the Category 1 requirements in Part 37, and so it does not need to be changed.

4.2.3. Basic Security Level Threshold

Summary: US regulations do not have an equivalent security level or requirements for radioactive material transport and it is a significant omission. As a minimum, Part 37 should be revised to include graded security provisions for Category 3.

Discussion: The threshold for the IAEA basic security level is defined by default as being above radioactive material that poses *"a sufficiently low risk of radiological hazard that it does not present a security concern. Such material includes very small quantities (excepted packages with an activity level not exceeding the level permitted for the radionuclide when it is not in special form), material of low activity concentration and low level contaminated objects that can be transported (LSA-I and SCI-I)"*. The US regulations do not have an equivalent security level. This means that there is a sharp delineation of security measures from the general Part 20 controls for all radioactive material to those required for Category 1 and 2 materials. This again illustrates the need to include Category 3 quantities into Part 37 in a graded manner. It should be noted that even if this were to be done, there would still be a security requirements gap between the materials that the IAEA discusses as *'not presenting a security concern'* and the Category 3 threshold.

Recommendation: Include graded transport security provisions for Category 3 quantities of radioactive materials in Part 37 similar to those of the IAEA's basic security level.

4.2.4. Prudent Management Practices Level

Summary: While the IAEA and the USA have similar default requirements, they are applied to vastly different quantities of material. Applying them to quantities less than Category 3 will bring them into closer alignment, albeit still with a significant gap.

Discussion: The IAEA's *'prudent management practices'* security level just includes the basic control measures incorporated into their International Basic Safety Standards[13]. Essentially this is equivalent in requirements to the default provisions in Part 20 to keep radioactive material *'secure from unauthorized removal'*. However, the level of application is vastly different as discussed above.

Recommendation: Consistent with the previous recommendation, these provisions should be applied to radioactive material quantities less than Category 3.

4.3. Transport Security Measures

4.3.1. Enhanced Security Measures

Summary: An overall comparison of the two sets of measures indicates that the Part 37 requirements are generally equivalent to NSS-9, with Part 37 providing significantly more detail (more prescriptive) than the IAEA in several areas. There are a few areas in the basic security requirements (incorporated by reference) that would be worthy of consideration by the NRC for inclusion in Part 37.

Discussion: The requirements in NSS-9 for the enhanced security level are in addition to those at the basic security level, so the sum of both were compared to those in Part 37 for Categories 1 and 2. It appears as if the additional NSS-9 requirements for the enhanced level are all covered in the Part 37 regulations. Indeed, in many instances Part 37 provides more prescriptive and thereby more detailed requirements than those in NSS-9, Section 4.3.

However, it seems as if some of the requirements at the basic security level do not have equivalents in Part 37. These include: a) use of closed or sheeted conveyances whenever possible; b) consideration of additional security measures if an open conveyance has to be used, such as guards, shielding against rocket propelled armor piercing weapons, enhancing route surveillance or response capability; c) personnel identity verification; d) security inspections of the conveyance; and, e) exchange of security related information between operators. With the exception of shielding against rocket propelled armor piercing weapons (which seems excessive for this security level), these measures might be considered for inclusion in any revision of Part 37.

Conversely, some of the requirements in Part 37 do not appear to have equivalents in NSS-9. These include: a) safe havens; b) State escorts; c) an individual accompanying the driver; and, d) the specific reporting times for events.

Recommendation: Consider the topics included in the basic security measures in NSS-9 that do not appear to be in US security regulations to determine if they would be worthy of inclusion.

4.3.2. Additional Security Measures

Summary: Many of the IAEA's additional security measures are incorporated in the Category 1 requirements of Part 37; however, others are not and these should be evaluated for potential inclusion.

Discussion: The US regulations do not have any requirements related to additional security for an increased threat or a particularly sensitive shipment of radioactive material. However, many of the measures included in NSS-9 Section 4.4 for additional security are already present in the Part 37 requirements for Category 1 shipments.

The measures that do not seem to be included in US security regulations for radioactive material shipments are: a) formal approval of security plans; b) guards accompanying transports; c) sabotage resistant package; d) security inspection of conveyance; e) specially designed conveyances; and, f) pre-shipment contingency plan exercises. Introduction of some of these in the USA such as specially designed packages and conveyances might have a prohibitive impact; however, others such as pre-shipment security inspections would seem to be good practices with minimal cost.

Recommendation: While there does not appear to be a need for additional security measures for an increased threat in the USA, those included in IAEA guidance should be evaluated to determine if they would enhance Category 1 transport security with minimal detrimental impact.

4.3.3. Basic Security Measures

Summary: The USA does not have any security regulations equivalent to the IAEA's basic security measures. This is a huge gap that should be remedied with a revision to Part 37.

Discussion: The IAEA's basic security measures are non-trivial and cover radioactive material greater than excepted non-special form material, LSA-1, SCO-1 up to 10D (the Category 2 lower threshold) or $3000A_2$. This level spans the lower categories of sources, but most significantly includes Category 3. The only measures that US regulations specifically capture in this range are:

a) Transfer only to authorized operators and confirmation that the recipient is capable of receipt. (e.g. 10 CFR 30.41(c), requiring copy of license showing authorization to receive the material);
b) Verification of integrity of locks and seals. (49 CFR 173.412(a), regarding seals for Type A packages);
c) Security awareness training (49 CFR 172.704(a)(4));
d) Written instructions (49 CFR 604(a)(3)(ii), since only emergency contact information is required at the basic level);
e) Advanced notification of shipment dates and expected arrival (49 CFR 173.22(c)); and,

f) The *'secure from unauthorized removal or access'* requirements (10 CFR 20.1801 and 1802).

The other eleven requirements in Section 4.2 of NSS-9 are not specifically covered. As can be seen, even the requirements that do have a USA equivalent are spread over a whole range of federal regulations. Consolidating them in Part 37 makes a lot of sense.

While there may not be a need for additional transport security for the complete range covered by the IAEA's guidance, the USA should at least cover Category 3 sources.

Recommendation: Consistent with the recommendation in Section 3.2 of this report, Category 3 sources should be included in a revised Part 37 to include graded requirements similar to those at the IAEA's basic security level for transport.

4.3.4. Prudent Management Practices

Summary: The measures under the IAEA's prudent management practices as expanded in the International Basic Safety Standards[13] and the basic radioactive material controls in 10 CFR Part 20.1801 and 1802 are reasonably equivalent. The big distinction is the level at which they are applied as discussed in Section 4.2.4.

4.4. Comparison of Categories with DOT Quantities

Summary: The IAEA, the NRC and the DOT all have different quantity criteria for their various requirements. An analysis of about 350 radionuclides shows that some similar security measures will be initiated at different quantities under each of the regimes. While this can be confusing for licensees, in practice the distinctions do not significantly affect security.

Discussion: As part of the analysis for this section, a comparison was made between the source categories and the various quantities in the Department of Transportation (DOT) regulations for radioactive material. This is because some of the security-related regulations are based on the D-values and some are based on the A-values. The approximately 350 radionuclides listed in the D-value and A-value tables were evaluated (except those with unlimited values).

As discussed already, the NSS-9 guidance has a basic security/enhanced security dividing line that is partly based on 10D and partly on $3000A_2$. For all radionuclides except three, $3000A_2$ is larger than 10D and quite a lot larger in most cases. Therefore, the 10D criterion is more conservative.

Type B quantities of radioactive material are those in excess of the A_1 value for special form radioactive materials and the A_2 value for normal form radioactive materials. Type B quantities must be shipped in Type B packagings which are more rugged and designed to withstand transport accidents. This may incidentally provide a little more security, but that is not the primary purpose. While many Category 1, 2 and 3 sources will be special form, it should be remembered that not all sealed sources are special form. They have to be certified as meeting the special form criteria to be considered as such. Analysis shows that 130 radionuclides in special form have Type B values less than 10D and 58 of them are less than D. Similarly, 226

radionuclides in normal form have Type B values less than 10D of which 136 are less than D. This means that in general the Type B requirements are applied at activities much less than the Part 37 requirements. The major security related requirement for Type B packages is advance notification of date and expected arrival of the shipment (49 CFR 173.22(c)).

DOT regulations define a Highway Route Controlled Quantity (HRCQ) as 3000 times the A_1 or A_2 value or 1,000 TBq, whichever is less. A comparison of the source category criteria and the HRCQ criteria shows that there are 16 radionuclides with HRCQ values less than 10D (only one from the Code of Conduct, Annex I) and three with values less than D. So, for just a very few radionuclides the HRCQ requirements are applied at activities less than the Part 37 requirements. The major specifically security-related HRCQ requirements (in addition to the Type B advanced notification) are the need for a transport security plan (49 CFR 172.800(b)(15)) and more in-depth security training (49 CFR 172.704(a)(5)) beyond the security awareness training (49 CFR 172.704(a)(4)). However, the HRCQ preferred routing requirements may incidentally help security as perhaps may the other requirements (registration, labelling, placarding). Interestingly, it seems as if the DOT regulations for preferred routing analysis via rail (49 CFR 172.820(c)) are much more detailed (prescriptive) than those for public highway. In addition, these regulations state that the *"rail carrier must analyze the safety **and security** risks for the transportation route(s)"*. The highway routing analysis only seems to have guidelines[14] rather than regulations and these do not seem to consider security.

Recommendations: While it would be easier and less confusing for licensees if the various agency's quantity criteria for their guidance and regulations were harmonious, if does not seem to make a significant difference from a security viewpoint.

This report is specific to 10 CFR 37, but the evaluation indicates that more could be done regarding the inclusion of security considerations in highway routing guidance or regulations.

4.5. Draft Revision of Security of Radioactive Material in Transport

Summary: The IAEA is in the process of revising NSS-9 and has issued a draft for member state comment. The PRT should review the draft and use it to provide further clarification to Part 37 guidance as appropriate.

Discussion: The IAEA is revising its guidance regarding security of radioactive material in transport (NSS-9) and has released a draft[11] for member state comment. An initial review of the draft revised document, published in January 2016, indicates that there are few changes that impact the previous recommendations in this report. Generally, the changes are positive and improve the clarity of the guidance and its consistency with that of NSS-11. A number of the significant differences between this revision and the existing NSS-9 are briefly highlighted.

Recommendation: The PRT should review the draft revised document and the NRC should consider incorporating useful clarifications as it considers any revisions to Part 37 or its guidance.

4.5.1. Security Levels

The thresholds of 10D (for Code of Conduct Annex I radionuclides) and 3000 A_2 (for all other radionuclides) is retained for the enhanced security level. However, the additional security measures are now more associated with sources ≥1000D (Category 1), rather than just when there is an increased threat. In addition, the listing of those packages under prudent management practices is more specifically defined by UN number.

4.5.2. Sabotage

There is much more emphasis and guidance on measures related to reducing the likelihood of sabotage. In particular, there is a statement that *"States should identify which shipments may require protection against sabotage."*

4.5.3. Security Measures

The security measures associated with each of the security levels are now much more clearly spelled out in the revised document and, perhaps more importantly, are more consistent with NSS-11. The measures are such that they broadly correlate as shown in the table below.

Table 3. Comparison of IAEA Security Level Terminology and Source Category

Security Level		
Transport	**Use and Storage**	**Sources**
Additional	A	Category 1
Enhanced	B	Category 2
Basic	C	Category 3
Prudent Management Practices	Basic Safety Standards	Category 4, 5

There are now modal-independent and modal-specific provisions included in the guidance as well as a new section on portable and mobile devices.

5. Comparison of Part 37 to the IAEA's Prevention and Protective Measures against Insider Threats

5.1. Introduction

The IAEA has published a document[15] on measures against insider threats. It is No. 8 in the Nuclear Security Series (NSS-8). Initially, the NRC's Program Review Team had not compared this guidance with Part 37; however this has now been done and a number of observations made that are consistent with this report.

In describing its scope (Section 1.3) NSS-8 says that it *"covers unauthorized removal of nuclear material and sabotage of nuclear material and facilities"*, so at first sight it might appear not to be applicable to radioactive sources. However in the next paragraph it says *"Guidance and measures presented in this guide can also be applied to the physical protection of other materials, including radioactive sources or radioactive waste."* Many of the measures are directly applicable to the security of radioactive sources, but because of its primary focus on nuclear material, they tend towards those more suited for the higher level Category 1 sources. Nevertheless, it is still worth comparing the Part 37 requirements against NSS-8.

NNSA's greater emphasis on the insider threat often results in them installing upgrades to deal with issues discussed in NSS-8.

It should be noted that there are many areas of agreement between Part 37 and NSS-8, so only those areas where there are significant differences are included in the discussion below.

5.2. Trustworthiness

5.2.1. Motivation

Summary: NSS-8 discusses motivation for insiders to carry out sabotage or theft, but Part 37 does not mention it at all and it probably should.

Discussion: Much of NSS-8 covers the issue of trustworthiness; however it does so at a somewhat deeper level than Part 37. An example of this is the discussion of motivation in Section 2 and elsewhere. *"Motivation may include ideological, personal, financial and psychological factors and other forces such as coercion."* Part 37 does not mention motivation at all. Determining a person's motivation for anything is fraught with difficulty and may be impossible. However, it **is** possible as part of the background check to look for *"undesirable behavior or characteristics, which may indicate motivation."* It is also possible to look at factors, such as those listed above, which may incline a person to be untrustworthy.

Recommendation: Include some text in Part 37 that requires *"looking for undesirable behavior or characteristics which may inform motivation"*.

5.2.2. Scope of Background Checks

Summary: The scope of background investigations in NSS-8 is broader than in Part 37. Some consideration should be given to expanding the Part 37 listing to make it more consistent with NSS-8, if legally possible. See also Section 9.5 in this regard.

Discussion: The list of background check areas in NSS-8, 5.3.(b) includes *"criminal records, references, past work history, financial records, medical records and psychological examinations/records."* The first three of these are also included in Part 37.25 in the list of things the *"background investigation must include at a minimum"*, but the last three are not. There may well be legal issues that would prevent a licensee from investigating financial, medical and psychological records and perhaps that will preclude their inclusion in any future regulation. Nevertheless, a trustworthiness determination would be better if these aspects could be included. The discussion in Section 9.5 is also relevant here.

Recommendation: Consider including other records in the background investigation per Section 9.5, if doing so is not prohibited by other laws or regulations. This more intense investigation could perhaps be reserved for higher risk, Category 1, sources in a graduated system.

5.2.3. Graduated Background Checks

Summary: IAEA guidance says that background checks should be graduated; but Part 37 is not. It has the same requirements for both Category 1 and Category 2 radioactive sources. Part 37 should be revised to include some graded requirements, especially if Category 3 is included.

Discussion: NSS-8, 5.3.(b) states that the *"depth of the trustworthiness checks should be graded according to the level of access the individual has"*. Part 37 has the same background investigation requirements for both Category 1 and Category 2 radioactive sources and is not graded at all. Consideration should be given to grading the trustworthiness checks, especially if Category 3 sources are brought into Part 37.

Recommendation: Revise Part 37 to require different degrees of background investigation depending upon the category of radioactive material to which the person will be granted unescorted access. Category 1 could include additional considerations, such as those discussed in 5.2.1 and 9.4. If Category 3 is included in Part 37, it could perhaps have slightly reduced requirements.

5.3. Compartmentalization

Summary: The compartmentalization discussed in NSS-8 to prevent a single individual having the knowledge, access and capability for sabotage or theft, is a good concept; however, practical application in many facilities would be difficult.

Discussion: There are provisions in NSS-8, Sections 5.3(c), (h) and (i) for compartmentalization which do not seem to be covered in Part 37 apart from the need-to-know concept in 37.31(b). Compartmentalization in NSS-8 includes compartmentalization of information, physical

compartmentalization of areas, and compartmentalization of activities. The concept is that no one person alone should have the knowledge, access and capability to perform a malicious act or steal material.

Recommendation: While this requirement might be suitable for high-risk, large facilities with a large staff, it is probably not realistic for a licensee with only one or two sources and few staff. Perhaps wording could be included in Part 37 about including compartmentalization *'as much as possible, consistent with the operation'*. However, the access controls associated with the security zone is about the best that can be done with most facilities.

5.4. Two Person Rule

Summary: The two person rule is included in NSS-8, but not in Part 37. Such a requirement could be added for higher risk situations.

Discussion: NSS-8 includes the two person rule in the section on detection (5.4.1). It states: ***"****The objectives of surveillance measures are to ensure that the activities of any authorized employee are always monitored by at least one other experienced, authorized employee in order that unauthorized acts on the part of one can be immediately detected and reported (the 'two person rule')."* The two person rule is not included in Part 37.

Recommendation: If regulations are to be graduated, then consider adding a two person requirement for Category 1 sources, at least during higher risk situations such as source transfer and device maintenance.

5.5. Tracking of personnel

Summary: Real-time tracking of personnel, as NSS-8 seems to imply, is probably excessive for most facilities, but systems such as key-card logging provide useful information and perhaps some deterrence.

Discussion: NSS-8 Section 5.4.1 includes an interesting discussion regarding the tracking of personnel. *"Tracking the movement and location of personnel within the facility assists in protecting against violation of access rules and also in providing useful information after an incident. Existing technology makes it possible to track each worker throughout a facility by recording the locations and areas visited each day by the worker and the times that each location was visited. Awareness that a facility has a tracking system may deter a worker from carrying out unauthorized activities. Further, tracking records may be used during the investigation of a malicious act to generate an initial list of suspects."* There is no such specific provision in Part 37. Tracking of personnel in real time with a GPS type system seems to be a little excessive; however many key-card type of access controls have an entry and exit logging system that provides much of the same information.

Recommendation: Tracking of personnel entering or leaving security zones or other areas of interest could be included in Part 37 as an example of topics that should be included in the security plan.

5.6. Searches

Summary: The IAEA guidance discusses certain checks and searches of personnel entering or leaving the secure area. This is not currently included in Part 37; but it could become part of a graduated security program.

Discussion: NSS-8 recommends (5.4.1) that checks are made to prevent insiders taking in *"tools, material and weapons that are unavailable or not allowed within the facility to carry out a malicious act."* In addition to radiation detectors at exits to detect unauthorized removal, NSS-8 also suggests using manual searches of persons leaving from secure areas. Part 37 has no requirement for searches.

Recommendation: If regulations are to be graduated, then consider adding such checks as a requirement for Category 1, at least during higher risk situations such as source transfer and device maintenance.

6. Comparison of Part 37 with Equivalent Regulations in other Countries

Summary: Source security regulations in several countries were compared with Part 37 in an effort to determine if any good practices can be transplanted to the USA. However, the PRT staff effort was significant and the gains were minimal, so it was terminated at five countries.

Discussion: The PRT has compared the US regulations with the equivalent regulations for the security of radioactive sources in a number of other countries. These countries include Spain, Finland, Canada, Australia and France. It is not always easy to do this comparison because of differences in legal structure as well as language problems. While the effort has been substantial, this report feels that the benefit of the exercise is marginal and no further work should be expended with more comparisons. It was an interesting concept to see if the USA could learn from other countries, but ultimately it has been of little value. The conclusions of the comparisons will be well-reported by the PRT and no effort will be made here to repeat them other than to say that in general, other countries conform more directly to the IAEA guidance than the USA, particularly in the matter of Category 3 sources.

Recommendation: Do not examine or compare equivalent regulations in any more countries.

7. Comparison of Part 37 to the European Union's High Activity Sealed Source (HASS) Directive

Summary: As a measure of the completeness of the NRC's Program Review Team's (PRT) work relating to international security program requirements, the EU's HASS Directive[16] was checked for security related regulations. Only very generic requirements were found in Article 6 (b) through (d).

"(b) regularly verify, at specific intervals which may be determined by Member States, that each source and, here relevant, the equipment containing the source, is still present and in apparently good condition at its place of use or of storage;

(c) ensure that each fixed and mobile source is subject to adequate documented measures, such as written protocols and procedures, aimed at preventing unauthorised access to or loss or theft of the source or its damage by fire;

(d) promptly notify the competent authority of any loss, theft or unauthorised use of a source, arrange for a check on the integrity of each source after any event, including fire, that may have damaged the source and, if appropriate, inform the competent authority thereof and of the measures taken;"

Recommendation: These requirements are easily covered by the existing 10 CFR Part 20 and Part 37 regulations and no further action is needed.

8. Evaluation of Inspector Training Review

8.1. Introduction

The major purpose of this report is to evaluate the Program Review Team's (PRT's) work for completeness. Therefore, this section will primarily discuss and focus on the *review* of the inspector training program rather than the training program itself. Comments are still made regarding the actual training, when it is felt that this input is of value.

It was decided that the best way to perform the assigned task would be to outline how a training program review could be conducted and compare that with what the PRT did.

8.2. Performance Evaluation

Summary: One method of checking the effectiveness of a training program is to evaluate how well its graduates are performing. While the NRC has a performance indicator that might at first sight be of value, it was determined that this was primarily for evaluating program performance rather than individual performance. However, consideration might be given to initiating methods for the consolidation of inspector performance data to allow for an analysis of commonalities and trends.

Discussion: One method of looking at the effectiveness of inspector training is to look at how well the inspectors are doing the job. Questions that could be asked include:

- Are inspectors making mistakes?
- If so, how often?
- How significant are any errors?
- Are there any commonalities to the problems?

Analysis of the answers to these questions would inform the effectiveness, or otherwise, of the training program. For example, if there is an area where inspectors are making the same mistake frequently, it would imply a need to fix that area of training to emphasize the regulation, or correct a misperception. Conversely, if they are doing a great job most of the time, one could conclude that the training is quite good and any adjustments would be minimal.

Patterns of issues might provide input as to where the training needs revision. If there is a pattern of problems with new inspectors, then the implication is that initial training might be at fault, whereas if experienced inspectors have difficulties perhaps the Gap training needs examination. Similarly, perhaps the health physics inspectors being cross-trained in security might be having difficulty.

The NRC has a procedure for conducting reviews of NRC Regional and Agreement State radioactive materials programs using the common performance indicator, Technical Quality of Inspections[17]. This procedure looks to be quite good and requires a systematic sampling and review of inspections and inspectors. However, its primary purpose revolves around program performance rather than individual performance. Individual performance is evaluated as part of

the normal human resources functions, but there does not currently seem to be a mechanism for the assessment of common problem areas or trends.

Recommendation: Consideration might be given to initiating methods for the consolidation of inspector performance data to allow for an analysis of commonalities and trends.

8.3. Feedback from Licensees

Summary: Licensee feedback is a useful way of getting information about inspections and inspector competencies which in turn provides information on their training. Such feedback should be sought.

Discussion: Obtaining feedback from those who have been inspected is another useful method to evaluate the training of inspectors. For example, licensees could be asked if they felt that inspectors were sufficiently knowledgeable about the regulations or whether they appear to have gaps in their understanding. Are inspectors giving confusing or conflicting information about the regulatory requirements of Part 37 or are they consistent with each other? Is there consistent enforcement for the same or similar violations? All these can point to areas that may need re-examination of the training program. It is understood that there is a reluctance to inspect inspectors, but the purpose here is to not to evaluate inspectors, but their training.

There are a number of topics about which the PRT is planning to interview licensees, but their inspection experience and the quality of the inspectors is not among them. This is because the PRT regards the collection of information concerning inspectors' interactions with licensees is beyond the scope of the review. While it is agreed that this is not the main focus of the licensee feedback events, it still seems like a useful opportunity to gain valuable knowledge that should not be missed.

Recommendation: In planned stakeholder interviews, meetings, and webinars, request feedback from licensees about their inspection experience and their generic assessment of inspector competencies and consistencies.

8.4. Feedback from Inspectors

Summary: Valuable information about training can be obtained from those who have been through a course. It appears as if this is now being sought and evaluated by the PRT, but it would be valuable to extend the scope.

Discussion: Interviewing current inspectors is an excellent way of getting information regarding the completeness and quality of their training. It seems as if the GAO[18] did this and found that some of them (6 of 48) did not feel they were trained well enough to be qualified to do security inspections. Questions could be put to inspectors regarding whether they felt there were any gaps, problems, common issues, or deficiencies in their training. They can be asked about the quality of the training, including: instructors, documentation, hand-outs, exercises, facilities and examinations. It is informative to ask questions immediately after training, and this is being done for the Technical Training Center (TTC) course S-201, but it could be repeated six months

or a year later. Sometimes people do not realize the significance or value of what they have been taught until they have worked in the job for a while.

In addition, there is value in selecting two or three standard, situational knowledge questions of inspectors to see if they know the answers. The quality of responses speaks not only to the training program, but their assimilation of the material.

The TTC uses student feedback forms for the S-201 course and the PRT has discussed with them how these are used for continuous course improvement. However, it is unclear if there are similar forms for the other courses. In addition, there does not seem to be any mechanism to obtain feedback several months after a course.

Recommendation: Immediate feedback from new and experienced inspectors has been obtained and used to improve the S201 course. However, consideration should be given to obtaining similar feedback from the other courses, as well as several months later to help evaluate retention of the training material.

8.5. Feedback from Trainers

Summary: Trainers typically know their courses, students and materials better than anyone, so that they can identify issues and solutions more rapidly than external evaluators. It appears as if the PRT has interacted well with the relevant trainers to get their feedback.

Discussion: Instructors of courses know how well their material is coming across to their students and what subjects are not being understood. It does not take too much time as a teacher to realize when there is a communication breakdown or to figure out the areas in which students are having difficulties. For this reason instructor feedback is essential in evaluating any training program.

When trainers review examination question answers, it soon becomes clear when there is a common misconception. This may well be occurring because of the difficulty of the material or because of how that portion is being taught or presented. For example, rather than a lecture, that portion might be better as a worked problem, exercise or class demonstration.

Trainers can also provide feedback on the quality of the students that they are getting and whether or not they have the prerequisite knowledge to be successful in a course. It seems as if the PRT has discussed these issues with the TTC staff and with the trainers for the other courses.

Recommendation: None. The PRT has interviewed instructors from all the relevant courses to get their feedback on limitations, students, and potential improvements.

8.6. Training Course Evaluation

There are many elements that make up a good training course. These vary from the temperature of the room, to the readability of the slides, to the clarity of the instructor's speaking voice.

There are four courses for inspectors that need evaluation:

- The Technical Training Center (TTC) course S-201;
- The Gap training course;
- The Reactor Temporary Instructions training;
- The Agreement State training.

Each of these needs to be evaluated in the areas listed in the subsequent sections for a comprehensive review of inspector training courses.

8.6.1. Facilities and Logistics

Summary: Good training facilities and logistics enhance learning by removing distractions and hindrances. It is as important to evaluate these as it is the course content.

Discussion: Many logistical factors go into a good training experience. They include the:

- ambient light;
- comfort of the chairs;
- room temperature;
- view from windows, if any;
- break facilities;
- restroom location;
- audio-visual/projection equipment;
- equipment for demonstrations and exercises;
- availability of student supplies such as paper, pens, markers, post-its;
- availability of reference resources;
- communications and Wi-Fi availability; and,
- friendly support staff.

Each of these needs to be evaluated to determine if they are helping or hindering the learning process. Typically, they only get noticed by the students and mentioned on feedback forms when they are a problem. If they are handled well, no-one notices them.

It appears as if the PRT identified these items as evaluated by NRC staff during the normal review processes, but did not address them directly themselves.

Recommendation: None. While it would be useful to have the PRT's assessment of these aspects documented, they appear to be appropriately handled in routine staff reviews of training courses.

8.6.2. Teaching Modes and Schedule

Summary: Incorporating a variety of teaching modes and including them in the right place in an appropriate length schedule greatly facilitates learning. These aspects need evaluation as much as content.

Discussion: A good training course allows for learning through a mixture of seeing, hearing and doing in a variety of ways to maintain the students' interest and attention. This also allows for the fact that while different people learn best in different modalities, each of us benefits from a combination of them. Methods include lectures with visual aids, videos, demonstrations, and hands-on exercises as well as site visits. They should be put together in a well thought out schedule of reasonable length with frequent breaks. These allow for students to stretch their legs and interact with each other and the instructors. Scheduling exercises or site visits after lunch helps to counteract the natural drowsiness that comes with a full stomach.

Recommendation: None. PRT members have attended the courses under consideration and have determined their training modes and schedules to be appropriate.

8.6.3. Content

Summary: Course content is the most important aspect of training evaluation. The PRT has done a good job at evaluating course content.

Discussion: The content of a training course is clearly of the utmost importance. It needs to be:

- on topic (minimal diversions to tangential areas);
- understandable and at the appropriate level for those attending;
- progressive, i.e. basic to advanced or broad background to specific details.
- accurate;
- interesting;
- varied;
- up-to-date; and,
- relevant to the students, so they know why they need this information.

Presentation slides should be easily readable with few words and incorporating pictures or video where possible.

Content was the main focus of the initial Program Review Team effort. So this area appears to be well covered. A review of the Gap training slides, showed them to be of a high quality for content and visual variety, with some useful practical examples. The Reactor Temporary Instructions training slides seem to be good for textual content, but lacking in visual variety such as pictures and graphics. There has not been opportunity to review the slides for the other training courses or any of the other materials.

It was noted that the PRT did a good job in picking up on some potential problems with the Gap course and the GTRI presentation at the TTC course S-201, and they seem to have been resolved

rather quickly. However, while the new Office of Radiological Security (old GTRI) presentation slides are visually appealing, many of them have too much text in too small a font.

The PRT noted the need for a refresher course as well as more course capacity, which are being addressed.

Recommendation: None. The PRT seems to be doing a good job at reviewing training course content and making appropriate comments.

8.6.4. Instructors

Summary: Excellent instructors are probably the most important factor in the success of a training course. The faculty involved in each of the classes should be critically evaluated and any problems remedied.

Discussion: Quality instructors are essential for quality courses. A quality instructor is:

- clear, i.e. easily heard;
- understandable;
- interesting;
- dynamic;
- personable;
- confident;
- open to questions;
- professional;
- experienced; and,
- knowledgeable.

If students are provided with anonymity and they are given the opportunity, they will provide valuable feedback on instructor quality. An instructor who wants to develop and improve will review the feedback and take appropriate notice of the comments. Those who do not correct their issues should be replaced.

The NRC's Human Resources Training and Development (HRTD) organization has an operating procedure[19] for the evaluation of training that appears to be quite good. This includes a well thought out instructor evaluation form for the end of a course. The PRT has not reviewed data from these forms because it has determined that instructor evaluations are outside the scope of their review.

Recommendation: None. Instructors are evaluated by their course directors and NRC supervisors on a recurring basis via the Technical Training Center processes.

8.6.5. Handout Materials

Summary: Hard copies of slides and other materials enhance the learning process. Handouts for all the courses should be evaluated for quality.

Discussion: The learning process is enhanced when students have good handouts, perhaps in the form of a manual. Quality handouts replicate or expand on content that has been presented visually or orally, so that it may be reviewed later. Not only does this enable the student to check something that might be confusing fairly quickly after a presentation, demonstration, or exercise, but it helps them look back weeks or months later. Typically, they will remember hearing something about the subject, but cannot recall exactly what it was. Handouts reinforce learning.

Handouts need to be kept current and they need to be easily readable; not copies of copies of copies. While some instructors might not like it, it has been found to be beneficial for students to have hard copies of the slides, so that they can more easily follow along and write notes on them directly as needed.

Recommendation: None. It has now been determined that the PRT has evaluated the handouts from each of the courses and found them to be adequate for providing the necessary information to inspectors for their use and review.

8.7. Need for Other Courses

Summary: The universe of Part 37 training appears to be well covered, except for a future need for refresher training. Planning for the transition from Gap training to refresher training should be underway.

Discussion: The question to be considered is whether the scope of the existing training for Part 37 covers all the current needs or not. It would appear that it does, except perhaps for refresher training. As identified by the PRT, the refresher training on Part 37 can be included in the generic refresher training for materials inspectors. The training format and content still needs to be developed.

At some point the Gap training will no longer be required as each inspector eventually will be trained on the Part 37 requirements. It seems logical that the effort associated with the Gap training can be redirected towards the refresher training. The PRT has made the use of S-201 material as an online refresher an observation; however initial and refresher training have different objectives and it would be better to develop a separate refresher.

Recommendation: Begin planning for the transfer of personnel and resources away from Gap training and towards the development of a refresher training module for Part 37.

9. Trustworthiness and Reliability

9.1. Introduction

Ultimately, it is impossible to determine if a person is totally trustworthy and reliable. NUREG-2155[1] acknowledges it is difficult in stating that *"a judgment of any individual's dependability is inherently qualitative and not readily amenable to objective measurement or evaluation."* Even with the most rigorous screening or vetting program of the most secretive of national agencies there are still traitors and spies. No-one can know what goes on in a person's mind. Even the Bible says so: *"For who among men knows the thoughts of a man except the spirit of the man which is in him?" (1 Corinthians 2:11).*

Accepting this premise means that a trustworthiness and reliability (T&R) determination comes down to a balance of the cost or effort against the level of acceptable risk. The latter may also depend upon the consequences of being wrong. In Part 37 the balance is defined as the point where there is *"reasonable assurance that an individual is trustworthy and reliable."* But even this is subjective, so no matter where the NRC puts the balance point it is likely to be criticized.

There are a number of measures that are cheap and simple to apply and that minimally impinge on privacy. These include checking the identity and basic facts provided by the person being evaluated. Other measures are time-consuming, personnel-intensive and personally intrusive. Included in this category would be lie-detector tests and the type of effort that the FBI puts into the high-level security clearance investigations. Then there are some measures in between, such as checking criminal, financial or medical records which is where most of the debate about the appropriate level resides.

9.2. Issues Identified by the PRT

Summary: The PRT has done a good job of identifying and examining many of the complex issues related to T&R. Additional issues identified in this report are addressed later in this section.

Discussion: The PRT has made considerable progress in a comprehensive examination of access authorizations and T&R determination issues. The team's report will not be repeated here, but only a brief summary of significant issues that were identified.

Recommendation: The PRT should continue work on these issues, but also review those covered in subsequent sections of this report.

9.2.1. Employment History Gaps

Part 37 does not currently have a provision relating to the activities of individuals while unemployed. Consideration should be given to including some guidance regarding investigation of employment history gaps.

9.2.2. Insider Mitigation Program and Continuing T&R Activities

Part 37 does not have anything equivalent to the Part 73.55 insider mitigation program. In addition, the focus of the regulations and guidance is on initial T&R determinations. Consider broadening guidance by adopting some of the insider mitigation provisions to cover initial and continuing T&R activities.

9.2.3. Different Requirements for Access to Information vs. Access to Material

Access to security plans requires a T&R determination but fingerprinting and criminal history checks are not required as part of this determination. The logic behind this distinction compared to an unescorted access authorization to the material should be re-evaluated.

9.2.4. No Criminal Disqualifying Offenses Established

In a contrast with several other agencies, the USNRC has not published any disqualification criteria. Some licensees would like to have such criteria. (See also 9.6.1.) One of the objectives of the Temporary Instruction[20] on this topic is to determine if licensees have established their own criteria.

9.2.5. Approval of Reviewing Officials

Under the previous orders, the NRC approved reviewing officials. In general, this could not be continued and still allow agreement states to completely regulate the security of radioactive sources because of differing legal authorizations. However, there does not appear to be much pressure to require the NRC to do the T&R determination for reviewing officials.

9.2.6. Screening of Licensees vs. T&R of Reviewing Officials

The NRC screens license applicants and licensees appoint reviewing officials, but the focus for the license application screening is quite different than that for a T&R investigation. So there could be an implication that a licensee is not determined to be trustworthy and reliable. Perhaps consideration should be given to adding a T&R determination to the licensee screening process, at least for licenses subject to Part 37.

9.2.7. FBI Follow Up of Personnel in the Terrorist Screening Database

There is no formal agreement between the FBI and the NRC regarding actions when there is a fingerprint match with a person on the FBI's terrorist database. Essentially, the NRC trusts that the FBI will take appropriate action. Consideration might be given to the establishment of a memorandum of understanding between the two agencies similar to that in place for power reactor licensees.

9.2.8. No Personnel Access Database for Materials Licensees

Power reactor licensees have established a common database regarding persons granted or denied access, but there is no equivalent database for materials licensees. At this time there does not seem to be a significant impetus or coordination effort to establish such a database.

9.2.9. Submission of Reviewing Official Certification

The process for submitting the certification that a reviewing official is T&R is not clear and leads to difficulties. This primarily appears to be an internal NRC organizational issue that may need fixing.

9.2.10. Personal History Disclosure

For operational efficacy, consideration should be given to using disclosure mechanisms used in various federal agency forms such as the National Agency Check or the Transportation Worker Identification Credentials (also see Section 9.5).

9.2.11. Issues for Certain Service Providers

There may be an issue of enforceability regarding relief from fingerprinting and criminal history checks if service providers do not possess Category 1 or 2 quantities of radioactive material.

9.2.12. Reinvestigation

The L clearance reinvestigation period has been changed from 10 years to 5 years. Consequently, Part 37 may need to be changed for consistency.

9.3. Analysis of Effectiveness

Summary: Data are needed to evaluate the effectiveness of the current regulation and the PRT has initiated a process for inspectors to gather such information over the next year. These data should be analyzed and reviewed for program improvements as they come in.

Discussion: One measure of how well the current regulations are working is whether or not they are being effective at weeding out untrustworthy or unreliable people. However, this is difficult to determine. An absence of events involving insiders perhaps provides some indication that the system is satisfactory, or conversely that it has not yet been tested by an adversary. Another measure would be to determine how many people initially regarded as T&R were later found out to be not so. A significant number of these would indicate the need for more rigorous background checks. A comparison of the numbers of people who 'pass' the T&R determination compared to those who 'failed' also would be informative. Is the ratio reasonable? One would expect a large percentage of people to pass, but not 100%. Answering the questions require data.

Since licensees are not required to submit such data to the NRC, the PRT has initiated a Temporary Instruction[20] to inspectors to collect and document specific information regarding licensees' T&R determination processes for one year. Gathering these data is essential to the T&R review process and the PRT is to be commended for initiating it. Little further analysis can be done until the data are collected.

A recent evaluation of NMED data for events involving lost, abandoned or stolen Category 1 and 2 sources over the past 10 years shows that out of 91 events, only one involved a person acting suspiciously. However, it appears as if this person did not have unescorted access authorization. No events appear to have been a result of T&R issues.

Recommendation: The PRT has started the data collection process and little further can be done to evaluate the effectiveness of the current T&R regulations until some information is gathered. However, these data should be analyzed and reviewed for program improvements as they come in, but certainly in a year's time (2017).

9.4. Comparison with the IAEA Guidance

Summary: Most IAEA guidance with regard to T&R is non-specific. However, it does discuss the issue of motivation which does not appear to be explicitly addressed in Part 37. Some consideration might be given to including it.

Discussion: In comparing the IAEA guidance with regard to T&R there are two things to note. First, in most of the IAEA security of sources guidance there is very little specificity. There are just statements such as a requirement that *"each individual is suitably trained, qualified, and determined to be trustworthy"* and conversely *"unless determined to be trustworthy, they should not be granted unescorted access"*.

IAEA guidance on trustworthiness in the context of the insider threat is discussed in more detail in Section 5.2 of this report. As mentioned in that section, the second main distinction with the IAEA approach is the concept of attempting to determine motivational or coercion factors such as greed, ideology, revenge, psychological, physical dependency and financial issues. Most of these are not specifically addressed in Part 37. However, they are mentioned in the NUREG-2155[1] guidance, and perhaps should have a more prominent place in the regulations.

Recommendation: As recommended in Section 5.2.1, consider including some text in Part 37 that requires *"looking for undesirable behavior or characteristics which may inform motivation"*.

9.5. Comparison with other T&R Programs

Summary: Comparing the Part 37 T&R program with similar programs in other agencies is a valuable exercise and has been done to a certain extent by the PRT. An evaluation of the background check requirements of federal jobs requiring different levels of security has led this report to recommend the use of SF86P, or a similar form, as part of the T&R determination process.

Discussion: One way to check the reasonableness of the background check process for the determination of T&R is to compare that which is in Part 37 with similar programs in other agencies. The PRT has done this with about six different agencies/programs, but without drawing any conclusions, other than suggesting the linkage of T&R indicators with existing disclosure mechanisms (9.2.10). The PRT has also compared the disqualifying criteria used by these other agencies, noting that there are none in Part 37 (9.2.4).

Another method is to look at the universe of background checks and perform an analysis of what is considered normal for the various levels of security or trustworthiness. The federal government has a series of job application standard forms (SF) that are informative in this

regard. There is an eight page form (SF85) for non-sensitive positions that requires information going back five years. Then there is an 11 page form (SF85P[21]) for positions of public trust that requires data going back seven years, as well as a three page supplemental form (SF86P-S) for selected positions. Finally, there is a 127 page form (SF86) for national security positions that requires information over the past 10 years. By comparing these forms along with the IAEA requirements, the current Part 37 requirements and the nuclear power plant requirements in Part 73.56 the following table was generated.

Table 4. Comparison of Background Check Items for Three Levels of Security.

Level 1	**Level 2**	**Level 3**
Non-Sensitive	**Public Trust**	**National Security**
Since adult or 5 years back	***Since adult or 7 years* back***	***Since adult or 10 years back***
	Level 1 at greater depth plus:	*Levels 1 & 2 at greater depth plus:*
Basic personal history*	Residence history	Foreign activities
Verification of identity*	Fingerprints/Criminal record*	Foreign contacts
Citizenship	Illegal drug activity[+]	Use of IT systems
Education*	Alcohol abuse[+]	Non-criminal court actions[+]
Employment*	Financial records[+]	Association record[+]
Character references*	Foreign countries visited	Behavior observation[+]
Military history	Relatives	
	Medical records	
	Psychological evaluation[+]	

*Explicitly required by Part 37.

[+]Included in guidance: NUREG-2155[1] and/or NUREG-2166[2].

A review of this table shows that the explicit Part 37 requirements mostly only cover the Level 1 background checks of a person in a non-sensitive position. However, this does not show the complete picture because the personal history information disclosed is that which is *"required by the licensee's access authorization program"* (37.23(d)). So the licensee may request more than the information in the Level 1 column; but it is not required to do so. In addition, the guidance in NUREG-2155 and NUREG-2166 include suggestions about checking some of the other areas as shown in the table.

Having said this, there still seems to be a disconnect between the information requested for a job requiring public trust and that required for unescorted access to high-risk radioactive sources. Since SF85P is already an OMB approved form for gathering information for those eligible for a public trust or sensitive position it makes a lot of sense to require the use this form as part of the licensee's T&R determination. Indeed the preamble to the form states that this is its very purpose: *"Background investigations are conducted using your responses on this form…to develop information to show whether you are reliable, trustworthy, of good conduct and*

character, and loyal to the United States…In addition to the questions on this form, inquiry also is made about a person's adherence to security requirements, honesty and integrity, vulnerability to exploitation or coercion, falsification, misrepresentation, and any other behavior, activities, or association that tend to show the person is not reliable, trustworthy, or loyal."

There is a subtle distinction between the self-disclosure required in this form versus the licensee initiated investigation required by Part 37, but the two should be complementary. Adopting a standardized form such as SF86P could help address an issue the GAO[18] identified where a couple of hospital administrators told them that a more centralized background examination process with uniform criteria and standards should replace the current system, which varies from facility to facility.

Finally, it is acknowledged that the PRT in its review and determination of observations is somewhat restricted by the legalities associated with agreement states and imposing background check requirements based on public health and safety laws versus those arising from common defense and security. This may be a somewhat intractable problem and it is certainly outside the scope of this report.

Recommendations: Consider requiring the use of SF86P (or a very similar form) for gathering background information for the purposes of the T&R determination.

9.6. Feedback from Licensees

Feedback from those trying to implement the regulations is essential. It seems as if the PRT is doing this in a variety of ways; however insufficient data have been gathered at this time to inform the evaluative process. As previously mentioned in Section 9.3, a temporary instruction has been issued to enable inspectors to ask licensees certain questions. Also, a small number of licensees have been interviewed jointly by the external consultants and the Program Review Team. Finally, a Federal Register Notice is in preparation to enable one or more stakeholder meetings/webinars to be held to get feedback on this and other topics. Once these interviews and meetings have been completed, it might be possible to answer such questions as to whether the licensees feel that the T&R program is achieving its objectives, whether it is being fair on individuals and if there are any problems that need fixing.

A few issues have been identified as being important to licensees from the questionnaires used as part of the evaluative process by the external, independent consultants. These are discussed in the following sections.

9.6.1. Disqualification Criteria

Summary: There is pressure from the GAO and some licensees to publish T&R disqualification criteria. In fairness to individual situations, pressures to provide hard and fast disqualification criteria for T&R decisions should be resisted.

Discussion: A GAO report[24] in which only a very few licensees were interviewed indicated that they face challenges with making T&R determinations. *"These challenges include limited*

security experience and training and incomplete information to determine an employee's suitability for unescorted access." It also seems as if some at least would like specific disqualification criteria.

While it is understandable that licensees would like more specific guidance on such things as disqualification criteria, this report agrees with the NRC that it is inappropriate to have a hard and fast demarcation. This is because there are so many potential mitigating factors that flexibility and subjective involvement are needed in most decisions.

Some disqualification criteria that have been suggested, such as conviction of treason or an act of terrorism, are so obvious that a licensee would naturally exclude such a person anyway.

Recommendation: In fairness to individual situations, resist pressures to provide hard and fast disqualification criteria for T&R decisions.

9.6.2. Foreigners

Summary: Performing a T&R determination for a recent temporary or permanent immigrant is difficult, with no obvious solution.

Discussion: One of the difficulties that licensees have identified regarding T&R determinations relates to personnel of foreign origin, particularly those relatively new to the USA. This impacts academic and research licensees more than most, since many undergraduate and graduate students are from abroad. In addition, there may be need for them to have unescorted access to sources such as irradiators in order for them to perform research outside of traditional working hours. Clearly, obtaining the necessary background information can be difficult and can be complicated by language differences. There are two tendencies: one is to not bother with the T&R determination and just disallow unescorted access, and the opposite is to rely too much on relatively short term personal impressions of the individual.

There does not appear to be a simple solution to this problem since agencies such as Interpol are unlikely to respond to requests for information from licensees.

Recommendation: None, other than to seek advice from appropriate government agencies about how to help licensees in this regard, then publish guidance.

9.6.3. Military and Government Personnel

Summary: Military and government licensees primarily use their standard security clearance procedure to meet the T&R requirement.

Discussion: Military and government licensees seem to have few issues or problems with respect to the T&R requirements because they can piggy-back on the standard security clearances that are performed for most employees as a condition of their employment.

Recommendation: None.

10. Location and Tracking of Radioactive Sources

10.1. Introduction

The PRT has reviewed the Integrated Marketing Solutions report as well as licensee and inspector responses to questionnaires. Three observations have been made, one of which coincides with a recommendation made in this report. The PRT should continue to seek input from the stakeholder meetings to be held later in the year. So far it has focused on the National Source Tracking System, while this report has taken a broader view of location and tracking of sources.

In general, there are four different methods of determining the location of radioactive sources, all of which are used in various aspects of source security.

10.1.1. Inventories

Inventory or accounting checks at a set frequency determine that a source is, or was, at a particular location when it was checked. The IAEA makes a distinction between inventorying and accounting. The former would check that there is a source present e.g. by using a radiation survey meter; the latter would check that a particular source is present, e.g. by checking the serial number. The frequency of checks varies for different agencies and purposes, but typically is annually or semi-annually. This means that the licensee is only really sure of the location of a source once or twice a year and that in theory it could be missing for almost a year or six months, if this were the only means of detection employed.

A reconciliation inventory is required for nationally tracked sources (See 10.4.1) annually in January. Semi-annual inventories are often associated with leak tests in a number of regulations for specific types of licenses. Some licenses require quarterly inventories.

10.1.2. Bar codes

Bar codes, Quick Response (QR) codes or similar tracking methods record the location of a source, or package containing a source, at the time it is, or was, scanned. These are typically used to track the movement of packages as they leave a shipper and pass through various handling points until delivery. The location of the source/package is only truly known at the time of scanning and it is assumed that it is between its last scan point and the next planned scan point. It could go missing between these two locations and be unnoticed until the recipient reports that it has not arrived as scheduled. This is part of the rationale for the confirmation of receipt and the no-later than arrival time for Category 2 source shipments in 37.75(a)(3).

This type of system meets the requirements of 37.79(a)(3)(i)-(iii) and (b)(2)(i)-(iii) for tracking shipments of Category 2 sources.

10.1.3. Events

Event tracking is where a change in circumstance is reported to a central location or database. The location and status of the source is only known at the time the event is reported. There could be days or years between reports if the source remains in one location and its status does not change.

This is the system used by the National Source Tracking System (NSTS). Every event in the life-cycle of a Category 1 or 2 source of the radionuclides listed in Appendix E of Part 20 is required to be reported by the close of business the next day.

10.1.4. Telemetry

Real time, telemetry tracking enables the precise location of the conveyance, source or package to be determined at any time. This GPS type of system typically shows the location to within a few feet and can be tied in with a cellular system for transmitting information about various other events associated with the conveyance or device. Geo-fencing systems are also available that enable an alert to be sent if a device is moved outside of a defined area. While systems are under continuous development, at the moment trackers are more easily placed on vehicles, packages or devices than they are on the radioactive sources themselves. Clearly, they only track the item to which they are attached. Apart from the size issue there is also a radiation dose and damage issue associated with placing trackers on the actual sources.

This type of system is required by 37.79(a)(1)(iii) and (b)(1)(i) for tracking shipments of Category 1 sources, but has been considered for other mobile sources.

10.2. Licensee Feedback

Summary: As part of its charter the PRT is to obtain feedback on the NSTS, but it would be better if it sought feedback from licensees on the complete location and tracking system for radioactive sources.

Discussion: The PRT's charter requires it to interview licensees and get feedback for possible program enhancements for the NSTS. Some of this has been done, but it should be broadened to get an evaluation of the location and track system as a whole, not just the NSTS.

Recommendation: The PRT should seek feedback from licensees on all aspects of radioactive source location and tracking.

10.3. Mobile Sources

Summary: Tracking high-risk, very mobile sources such as those used in industrial radiography is attractive from a safety and security viewpoint. The technology should be re-evaluated from time to time and a requirement included in Part 37 when it becomes reasonably feasible.

Discussion: There has been some significant discussion about requiring real-time tracking for mobile radioactive sources or the vehicles to which they are attached. Indeed this was the subject of a petition from the governor of Washington State that was denied by the NRC[22] in

2008. The argument is somewhat persuasive in that mobile ^{192}Ir industrial radiography sources (Category 2) get stolen more often than any other single type of high-risk source. The theft of the source is often incidental to the theft of the vehicle to which it is attached and not normally related to malicious intent, but that is not known at the time. The arguments for and against the GPS tracking of these sources or vehicles are well discussed in the Federal Register[22], but as the technology continues to develop the concept should be re-evaluated by the NRC.

One of the NRC's arguments for denying the petition was that it was going to take such things into consideration in the new rulemaking, which eventually became Part 37. However, the only real-time tracking requirement in this regulation is that for Category 1 sources in transit.

Recommendation: As tracking devices become smaller, cheaper and more suitable, reconsider requiring the use of GPS type technology for high-risk mobile radioactive sources such as industrial radiography cameras.

10.4. National Source Tracking System

10.4.1. Background

The National Source Tracking System (NSTS) was developed to conform to the IAEA's Code of Conduct national registry requirements, and it became fully operational in January 2009. Licensees are required to report on life-cycle events (manufacture, transfer, receipt, disassembly, or disposition) involving the Category 1 and 2 sealed sources listed in Appendix E of Part 20 by close of business the next day (Part 20.2207). These sources are known as the nationally tracked sources. Currently, there are about 1500 licensees subject to the tracking requirements, of which ~750 use self-contained irradiators and ~500 are industrial radiographers.

A major effort was made beginning in 2011 to improve the on-line use of the NSTS and to solve a number of practical issues identified by an independent survey. However, it is difficult to determine without another survey if these measures have been effective. Perhaps the PRT's licensee interviews will provide some of this information even though the sample size will be small.

10.4.2. Category 3

Summary: The NRC staff's 2009 recommendation to expand the NSTS to include Category 3 was not adopted, but it should be.

Discussion: In June 2009, the Commission was split 2-2 on whether to expand the NSTS to include Category 3 sources in accordance with the staff's recommendation[9]. Therefore, no further action was taken. The recommendation was quite persuasive (as discussed in Section 3.2.1) and is consistent with IAEA guidance and other recommendations in this report. The NSTS should be expanded.

Recommendation: As a minimum, expand the NSTS to include Category 3 sources of the radionuclides included in Appendix E of Part 20, but preferably for all radionuclides per Section 2.2.

10.4.3. Radionuclides covered

Summary: The listings of radionuclides subject to Part 37 and those included in the NSTS are different, but they should be the same.

Discussion: Aside from the generic discussion about radionuclides covered in the Part 37 regulations (See Section 2.2), there is another disparity that needs attention. The list of radioisotopes covered by Part 37 in Appendix A is different from those covered by the NSTS as listed in Appendix E of Part 20. There are four radionuclides included in the NSTS that are not covered by Part 37, and they are ^{227}Ac, ^{210}Po, ^{228}Th and ^{229}Th. It is recognized that the analyses that gave rise to these listings were probably different and that the Part 37 listing was somewhat of a compromise to bring about international harmonization and conform to the IAEA's Code of Conduct above-the-line radionuclides. However, since the basic purpose of the NSTS and the Part 37 regulations is the same, it is incongruous that the listings are different.

There are two sensible options to resolve the discrepancy. The preferred option of this report is to include all radionuclides in Part 37 *and* Part 20.2207 (the NSTS) per Section 2.2. Alternatively, since the Part 37 listing conforms to the above-the-line listing in Annex I of the Code of Conduct use this listing for the NSTS as well and drop the other four radionuclides in Appendix E of Part 20.

Recommendation: Make the listings of radionuclides included in the NSTS the same as those subject to the Part 37 regulations.

10.5. Overall Assessment

Summary: The location and tracking system in NRC regulations utilizes all four methods discussed in 10.1 and appears to be effective for the sources covered, but it should be expanded.

Discussion: All four of the location and tracking methods are useful for different purposes and must be regarded and evaluated as a single integrated system, along with the detection and physical security requirements. Therefore the evaluative questions for the system are: do we know the location and status of every high-risk radioactive source at any time; and would we quickly know if a source became out of control?

While there are always likely to be some compliance and technical issues, it is the opinion of this report that the answer to these questions is in the affirmative. The complete system in place in the USA appears to be robust and to meet or exceed all international guidance with regard to Category 1 and 2 sources listed in Appendix A of Part 37.

The GAO seemed to be in agreement regarding the NSTS in stating[18] that: *"We tested these data to ensure both their completeness and accuracy, and determined that these data were sufficiently reliable to use in selecting locations to visit and summarizing by state the total number of buildings, number of buildings with completed security upgrades, and total number of curies."*

Technological research with regard to real time tracking of sources themselves should be continued and incorporated as appropriate.

Ideally, Category 1, 2 and 3 sources of all radionuclides should be included in the complete location and tracking system in a graded manner.

Recommendation: The system appears effective as is, but should be expanded to include all Category 1, 2 and 3 sources of all radionuclides. New technology should be incorporated as it becomes viable.

11. Enforcement and Security Issues Forum Results

11.1. Analysis of Redacted Data

Summary: A review of Security Issues Forum cases related to Part 37 identifies the sections of the regulations that are most frequently cited. These areas should be further evaluated to ensure that the cause of the problems is not lack of clarity or guidance.

Discussion: The Security Issues Forum (SIF) is a means of ensuring that the correct severity level is being assigned to violations of Part 37 and to develop examples for consistent enforcement policy in the NRC Regions. This is beginning to happen. Even though experience has been gained with the increased control requirements, Part 37 is still a relatively new regulation with some different requirements and initially all violations went through the SIF for review.

A redacted summary of about 70 SIF cases was provided for review. In addition, a summary was given of the number of violations against the section of the regulations cited for the period April 2014 through December 2015. An analysis of these data showed that the most frequent citations with approximate numbers were as shown below. The numbers are approximate because of some differences between initial citations and final citations; however some significant trends can be seen from these data.

Table 5. Most cited sections of Part 37 (April 2014 – December 2015)

Citation Frequency	Part 37 Section	Subject
~48	43	General security program requirements
~26	23	Access authorization program requirements
~8	49	Monitoring, detection and assessment
~7	25	Background investigations
~5	41	Security program

Other sections that had about one to five citations include: 21, 31, 33, 45, 47, 51, 53, 55 and 57.

The Part 37.43 citations were fairly evenly distributed throughout (37.43(a) – (d)), while the majority of the Part 37.23 citations were related to reviewing officials (37.23(b)). The Part 37.49 citations were all in the monitoring and detection requirements of 37.49(a).

It is difficult to draw many conclusions from the data provided because of the lack of detail; however, even the information in Table 5 is of benefit. The largest problem area seems to be the general security program requirements (37.43), including the security plan (37.43(a)), its implementing procedures (37.43(b)), associated training (37.43(c)) and information protection (37.43(d)). This is closely followed by the access authorization program requirements of 37.23.

From the paucity of detail in the data provided, it is difficult to tell whether the deficiencies were mostly just of an administrative nature or whether they resulted in a real reduction in security.

The best that can be said is that both are present. Some of the citations are more of the paperwork variety, but others seem to be related to lapses in security.

It is postulated that frequency of the Part 37.43 citations will rapidly decrease after the first round of complete inspections since the licensees at least will have had to develop and implement a security program as a result of the initial citations. Issues related to monitoring and T&R may well be ongoing problems. Subsequently these areas may be worthy of a critical evaluation to ensure that the regulations and guidance are clear and understandable to licensees.

Recommendation: Critically review and evaluate the regulations and guidance related to the most frequent citations to determine whether the causes are due to lack of clarity in the requirements.

11.2. PRT Summary of Enforcement Data

Summary: The PRT is analyzing data relating to inspections and violations with a view to trying to draw conclusions that may result in further improvements to Part 37 or its guidance.

Discussion: The PRT is separately analyzing unredacted data on inspections and violations. Their analysis broadly confirms the results given in the previous section. From the period since the Part 37 regulations became effective until September 25, 2015, there were 179 inspections, of which 126 (70%) had no violations. In the other 30% there were a total of 120 violations, most of which were at Severity Level IV. The most prevalent sections of the regulations cited were those related to implementing procedures (Part 37.43(b)(1)) and access authorization procedures (Part 27.23(f)). This indicates that the issues were mainly of an administrative nature rather than actual breaches in security.

Recommendation: The PRT should continue to analyze the data to try and draw conclusions that may result in further improvements to Part 37 or its guidance.

12. Inspection Experience

This section is largely based on summarization of Regional NRC inspector questionnaire responses, since no specific analysis was received on this subject from the PRT before the end of the contract.

12.1. Enforcement

Summary: Several inspectors perceive that the Security Issues Forum (SIF) has been slow and burdensome in deciding on enforcement and in producing enforcement examples and guidance. These are being developed, but it appears as if they have yet to reach the inspectors.

Discussion: Enforcement consistently seems to be the major challenge with regard to inspections. Since there are a lot of different types of facilities and a variety of ways of meeting the regulatory requirements, it is important for consistency that there be clear guidance on what events are violations and what their severity levels are. While this is perhaps now being developed, it seems as if there was little of real value in the first year or so of the implementation of Part 37. In addition, inspectors are very critical of the SIF, its staffing, its processes and its responsiveness. Some inspectors feel that there are few inspection-experienced members on the SIF, resulting in a lack of a clear understanding of the issues. Even though the purpose of the SIF is to develop enforcement guidance and examples that enable consistency of enforcement it is seen by inspectors as another bureaucratic layer that is very burdensome and slow to respond. There are sufficient questionnaire answers along these lines that it seems to be a common perception, not that of just one or two persons. The enforcement guidance and enforcement examples that the SIF is now beginning to generate are urgently needed by the regions.

Recommendation: Examine the SIF process and its development of enforcement examples and guidance with a view to speeding up the decision making process and guidance publication.

12.2. Regulatory Issues

12.2.1. Implementing Procedures

Summary: The presence and level of detail in implementing procedures has been a problem with several licensees. However, this will likely be taken care of after the first inspection.

Discussion: One of the most significant compliance issues for those being inspected for the first time appears to be their implementing procedures. There are several aspects to this problem.

- Those under the increased controls (ICs) were not required to have as many written procedures, and thinking that Part 37 was almost the same as the ICs, they did not realize the full implications of the new regulations.
- Licensees have been unsure of the number and degree of detail needed for implementing procedures. In several instances it appears that they are somewhat lacking.
- Sometimes it is not easy for inspectors to find a single, specific regulatory reference to cite as a violation because of the broad nature of this aspect of Part 37.

- It appears as if the licensees are working hard to conform to the regulations, but have significant uncertainty about their compliance until that first inspection.

Recommendation: None. The normal inspection process will remedy this problem.

12.2.2. Trustworthiness and Reliability

Summary: While there is a lot of discussion, concern and uncertainty regarding the T&R process, it appears to be working quite well. (See also Sections 5.2 and 9).

Discussion: It appears as if the trustworthiness and reliability programs are working reasonably well. However, it is worth making a number of observations.

- Many T&R determinations are done by the human resources staff. This is particularly true of new hires. An employer is looking for good employees and this is one aspect of that process. If people lie or embellish their applications, they are not trustworthy and not desirable hires.
- Making a T&R determination is always a challenge to licensees because ultimately it is a judgment call that may have repercussions.
- Licensees worry about whether they will be second-guessed by the NRC and what their liability is regarding a wrong decision i.e. if a person judged to be T&R maliciously uses a source. This is not an insignificant burden on the individual reviewing official.
- Since the reviewing official makes the decision, the decision itself is not something the inspector can easily cite (unless perhaps there is clear evidence of a problem that has been ignored). All the inspector can do is to ensure that there is the necessary documentation of the decision.
- Few, if any, licensees have written, firm disqualification criteria.
- Foreign-born employees are a problem because of the difficulty of getting the necessary documentation. This is a particular problem for academic licensees where foreign graduate students are common.
- Military and government licensees and permitees have much less of a T&R issue because of the security clearances that jobs with such organizations usually require.

Recommendation: None.

12.3. Inspection Guidance, Training and Tools

Summary: Generally, the guidance, training and tools for inspectors have been adequate, but continuous improvement needs to be maintained.

Discussion: Initially there were some problems for licensees and inspectors because there was little guidance published until after Part 37 was in force. However, NUREGs 2155 and 2166 were available fairly quickly thereafter and have been very useful and well received. Some, but not all inspectors and licensees felt that there could have been more outreach and that more pro-active communication could have been used before the roll-out of Part 37.

Even though there has been some discussion about difficulties with the concepts and regulations relating to the aggregation of sources, this does not seem to be borne out by questionnaire responses from inspectors or licensees. No-one seems to have any problem with understanding or implementing this part of the regulations.

Most inspectors felt that their training was adequate and generally was at a high quality. However, one NRC inspector believed that there should be a formal training course specifically designed for inspectors tasked with performing 10 CFR Part 37 inspections, thereby indicating that he was probably unaware of the S201 course.

While most agree that performance-based regulations are necessary and better than prescriptive regulations, this does not preclude inspectors wanting and indeed developing their own inspection checklists.

It seems that quite a few inspectors are not aware of the security toolbox, and those that are aware of it do not use it. Inspectors seem to be of the opinion that the National Source Tracking System (NSTS) and Web-Based Licensing (WBL) are useful, but they are not overly enthusiastic about them. These systems appear to do the job required adequately, but improvements could be made to make them more user-friendly and easier.

Recommendation: Continue to seek feedback from inspectors regarding how their guidance, training and tools can be improved.

13.Physical Protection

13.1. Physical Protection during Use, Storage and Transport

Summary: The PRT members responsible for this section were working largely on other issues, but have a plan of action that seems suitable for the task.

Discussion: The PRT has reviewed a number of documents pertinent to assessing Part 37 with a focus on use, storage, and transport. Most of the documents were received in email messages and attachments such as questionnaire responses, comparison tables for IAEA and other organizations and communications of Part 37 assessment information. In addition, the PRT has participated in several telephone interviews of inspectors and licensees which provided additional information regarding their responses to the questionnaires. The PRT has also used its materials inspection experience relative to the NRC Security Orders and Part 37, and has received information from other experienced Regional inspectors to help inform its assessment.

Additional information that is planned to be reviewed to continue the Part 37 assessment of use, storage, and transport include the applicable GAO reports, NRC security regulations, NMED data, escalated enforcement data, and Subpart D to Part 37.

Recommendation: The PRT should complete its plan of action for the review of this topic.

13.2. Aggregation

Notes:

- If Category 3 sources are brought into Part 37, then the aggregation references in the regulations would also need revision.
- While there are subtle differences in the two terms co-location and aggregation, they are used synonymously in this report.

13.2.1. Definition

Summary: The 10 CFR Part 37 definition is not good English and is confusing. It is defined: *"Aggregated means accessible by the breach of a single physical barrier that would allow access to radioactive material in any form, including any devices that contain the radioactive material, when the total activity equals or exceeds a category 2 quantity of radioactive material."*

First, aggregated does **not** mean *'accessible'*. It means *"the collection of units into a body, mass or amount"* (Webster).

Second, aggregated in this definition also ties it to exceeding a Category 2 quantity. However, sources can aggregate to any category quantity and the regulations graduated accordingly. This is somewhat taken into account in Part 37 because it includes the Category 1 or Category 2 qualifier most of the time. However, it would be better to remove the direct link to Category 2 in the definition, especially if the regulations are modified to include Category 3.

Recommendation: Revise the definition into something like: *"Aggregated means an assemblage of radioactive material in any form, including any devices that contain the radioactive material, such that the breach of a single physical barrier would allow access to the total quantity of radioactive material in that location. The category of the aggregated sources is determined by the sum of the fractions method (Ref.)."*

13.2.2. Technical Basis

Summary: In general, the basis for the aggregation of radioactive sources using the sum of the fractions method is technically invalid, even though it comes from the IAEA[23]. However, pragmatically it is a useful and easily implemented method for regulatory control and should be retained. The inherent conservatism of the method may need to be considered in enforcement situations when the sum of the fractions is close to the limit.

Explanation: The D-value[3] is the quantity of radioactivity considered dangerous for each radionuclide. It is the smaller of D_1 and D_2, where D_1 relates to non-dispersed material and D_2 relates to dispersed material. D_1 is determined by calculating the smallest amount of radioactivity that will cause a limiting organ or tissue dose for two separate scenarios (pocket and room). Similarly D_2 is determined by the smallest amount of radioactivity that will cause limiting organ or tissue doses for four separate scenarios (inhalation, ingestion, contamination and immersion). Adding the A/D fractions where the limiting tissue dose and scenario are different is essentially adding fractions of deterministic damage to different organs or tissues. Clearly adding a fraction of the soft tissue limiting dose to a fraction of the limiting lung dose is invalid because the detriments are different. Neither of them is sufficient to cause the dangerous deterministic effects and therefore even if the sum of the fractions exceeds unity the source does not meet the dangerous source[23] definition.

Example: For simplicity, consider two co-located sources of different radionuclides, one where the D-value is determined by D_1 (A) and the other by D_2 (B). Further assume that for source A the D_1 is determined by the pocket scenario while for source B the D_2 is determined by the inhalation scenario. Assume that the activity of source A is 0.4 D_1. This means that it has sufficient activity to give 0.4 of the limiting soft tissue dose (25 Gy-Eq). Assume that the activity of source B is 0.6 D_2. Simplifying, this means that it has sufficient activity to give 0.6 of one of the limiting doses for the inhalation scenario, say red marrow (1 Gy-Eq). Aggregating these using the sum of the fractions means that the aggregate $A/D = \sum_n(\sum_i A_{i,n}/D_n) = 1$ and by definition this aggregation of sources is dangerous. However, source A does not have sufficient activity to produce a soft tissue injury that reduces the quality of life, and source B does not have sufficient activity to cause severe deterministic effects in bone marrow. The impact of source A on the red marrow may or may not be sufficient to push the dose over the limit but the impact of source B on the soft tissue next to the pocket is unlikely to push the dose over this limit. In any case, it is unlikely that both scenarios would occur at the same time to the same person e.g. source A is put into a pocket while source B is dispersed in a respirable form.

Analogy: An imperfect analogy perhaps could be a person receiving a bullet wound with a fatality risk of say 0.4 at the same time as he or she had a virus with a fatality risk of 0.6. The two detriments are different and do not necessarily add up to a fatality.

Conclusion: Strictly speaking, the sum of the fractions method of aggregating sources is only valid when the two or more sources each have the same limiting scenario. This would be true when the sources are of the same radionuclide and have the same physical and chemical form. Therefore, an argument could be made that the sum of the fractions aggregation method should only be applied under in this situation.

Recommendation: Continue to use the sum of the fractions method for evaluating aggregated sources because: a) it conforms to international guidance; b) it is an easily implemented, practical method of regulatory control; and, c) because the quantification of the hazards and detriments associated with D-values has a large margin of uncertainty. However, recognize in enforcement guidance that the method is generally conservative for mixtures of different radionuclides and sources. This might be taken into consideration during enforcement actions for licensees where their sum of the fractions is close to one of the category limits.

13.2.3. Regulatory influence

Summary: Is the current regulation on aggregation of radioactive sources driving licensees towards a more or a less desirable outcome? This question has two components: a) is aggregation (with its associated measures) or dis-aggregation the better option; and, b) are the regulations encouraging aggregation or not? If the answers to these questions were known then the regulations might be adjusted to encourage licensees to adopt the preferred option. However, since there is no clear cut best option, at this point there is no recommendation.

Discussion: The GAO[24] felt that *"colocation may have the unintended consequence of placing a segment of these sources at greater risk of theft or loss."* Essentially, they are assuming that the answer to question a) is that aggregation is better. A greater quantity under more security is preferred over a lesser quantity with less security. Their answer to question b) is that regulations are encouraging dis-aggregation (and thereby increasing the potential for theft or loss of a less than Category 2 quantity). However, this is not at all clear and NRC staff members interviewed do not feel that the regulation encourages one approach over the other.

The analysis of which option is better (aggregation or dis-aggregation) is confounded by the fact that the public perception of the consequences of the theft and actual malicious use of radioactive material are likely not significantly related to the quantity used. This tends to push the argument towards aggregation and its increased security being the preferred choice.

In considering question b), it seems that licensees are typically driven towards conforming to the regulations in a manner that requires the least staff effort and lowest cost. At first sight, it appears that complying with the security requirements for Category 2 or above needs more money and personnel time; however, the cost and effort of keeping sources separate is not insignificant e.g. putting cages around individual gauges. Similarly, if a security zone has

already been established because of a large activity source the additional cost of putting all the other smaller sources in the same zone is minimal.

Recommendation: None. It is not at all clear whether aggregation or dis-aggregation is preferable and whether the current regulations encourage one approach over the other. It should be noted that if additional, graded, security requirements are applied to Category 3 sources the discussion becomes somewhat more moot.

13.2.4. Well-Logging Source Storage

Summary: The PRT has done a good job of evaluating issues related to well-logging sources. It has presented several options, but this report prefers the alternative of including Category 3 sources in Part 37.

Discussion: The PRT has clearly explained the aggregation issues related to the storage of well-logging sources and has examined the pros and cons of possible solutions. This is somewhat linked to the previous section (13.2.3) but is a very specific to the well-logging industry.

1. Well-logging sources are often individually below Category 2 levels, but several of them together without any intervening barrier could form an aggregated Category 2 quantity.
2. If licensees not authorized for possession of Category 2 quantities remove enough sources at one time to constitute a Category 2 quantity, for example, in the process of preparing for daily use or returning sources to storage, this would be a violation.
3. The proximity of multiple sources would make it easier for an adversary with access to the facility and to equipment for handling, shielding, and transporting the sources to accumulate sources to a Category 2 level.
4. A common key is normally used to open all the locks securing the sources in a room or an area. The separate storage pits or containers are considered to be barriers so that the sources are not considered aggregated.

In summary, aggregation of the well-logging sources in storage is prevented largely through licensee operating procedures, such as control of keys, access codes, and keycards that are needed to gain access to material, lifting equipment required to remove them from storage, and tools to handle them. The NRC inspects licensees to ensure that these measures are in place and its view remains that appropriate security is being maintained.

However, the PRT appropriately asks the question as to whether current configurations for storage of well-logging sources provide reasonable assurance against theft of quantities of material aggregated to Category 2 and if not, what measures should be taken to provide reasonable assurance? Options considered are rule changes, guidance changes, training changes and source management changes. This report believes that the guidance, training and source management changes discussed should be implemented regardless of anything else that is done.

The rule changes postulated include: a) elimination of the ability to use a barrier to disaggregate, i.e. apply Part 37 to sources in close proximity; b) licensing and inspection based on possession

limits rather than actual possession; and, c) addition of key control requirements. The pros and cons of these are given

Consistent with previous recommendations, this report prefers an alternative solution which the PRT has not presented, and that is the inclusion of Category 3 source into Part 37 in a graduated manner consistent with IAEA guidance. Since well-logging sources are Category 3 sources the problem goes away and no changes are required to regulations on aggregation.

Recommendations: Adopt the guidance, training and source management changes recommended by the PRT for well-logging licensees and inspectors. Include Category 3 sources in Part 37 as previously recommended to eliminate the problems related to well-logging sources.

14. Appendix I: Injuries Caused by Category 3 Sources

Refs [25, 26]

15. Appendix II:
Comparison of IAEA Guidance and U.S. Regulatory Requirements

International Atomic Energy Agency				United States of America			
Categorization	**Code**	**Security of Radioactive Sources**	**Security in the Transp. of RAM**	**NRC**			**DOT**
RS-G-1.9	**CoC**	**NSS-11**	**NSS-9**	**10 CFR**			**49 CFR**
		Security Level A	*CoC nuclides* / *Other nuclides*	71.5(a)		37.49(a)(3)(i)	*CoC nuclides* / 107.601(a)(1)
		Table 6	**Enhanced Security Level**	Licensee meet DOT transport regs.		Imm. det. of attempted removal	Registration and fee
		Prevent unauthorized removal	Section 4.3.			37.75(a) Transport	172.203(d)(10)
			Basic Security Level plus:	37.21, 37.23, 37.25, 37.27, 37.29		Preplan shipment dep. & arr. times	HRCQ on sh. papers
		Imm. detection of unauth. access	Identification of carriers and consignors	Trustworthiness of auth. individuals		Coord w/ state: escorts/safe havens	172.403(c)
		Imm. detect attempted unauth. removal	Security plan	37.31	Protect information	37.77 Transport	Yellow III label
		Imm. assessment of detection	Adv. notification: mode, exp. delivery time	37.41	Security program	Adv. notification	172.510(a)/172.527(a)
		Imm. comm. to response personnel	Tracking devices e.g. bar code	*Detect, assess, respond to unauth. access*		37.79(a)(1) Road transport	Special placard
Category 1		Detect loss via verification	Communications from the conveyance			Movement control center	172.820(a)(3)
		Delay sufficient to interrupt removal	Devices/equip./arrangments to	37.43(a)	Security plan	Redundant comms	Addtl. rail planning
		Imm. resp. to int. and prevent removal	deter, detect, delay, respond	37.43(b)	Implementing procedures	Cont. active tracking	
		Restrict access to auth. persons only		37.43(c)	Training	Ind. accompany driver	172.800(b)(15) Transport security plan
		Trustworthiness of auth. individuals		37.45	Coord. with LLEA	Procedures	172.704(a)(5) In-depth security training
		Identify and protect sensitive info.		37.47	Security zones	37.79(b)(1) Rail transport	
		Security plan		37.49(a)	Det. unauth. access w/o delay	Telemetric tracking, proc., reports	
		Capability to manage events in cont. plan	**Additional Security Measures**	37.49(b)	Imm. assmt of unauth. entry	37.81(a), (c), (e), (g), (h) Reports	
		Event reporting system	*For increased threat or sensitive transp.*	37.49(c)	Communications capability	LLEA/NRC w/in 1 h for lost/missing	
			Additional training	37.49(d)	Imm. response	LLEA asap of theft, NRC afterwards	
			Licensed ops, sec. plan subject to approval	37.53(a)	Two barriers for mobile dev.	NRC asap recovery	
1000D			Automatic, real time tracking	37.53(b)	Disable vehicle not under surv.		
		Security Level B	Transport control center	37.57(a)	Imm. notify LLEA	37.49(a)(3)(ii)	
		Table 7	National security clearance of personnel		Notify NRC	Weekly phys. checks, tamper devices	
		Minimize likelihood of unauth. removal	Guards	37.71	Verify license for transfer	37.75(b)-(d) Transport	
			Package resistant to sabotage			Coord. no-later than arr. time	
		Imm. detection of unauth. access	Conveyance search and inspection			Confirm receipt or non-arrival	
		Detection of attempted unauth. removal	Special attention to transfer points	CoC above the line nuclides		Notify of changes	
		Imm. assessment of detection	Specially designed conveyances			37.79(a)(2)-(3) Road transport	
		Imm. comm. to response personnel	Response plan reviewed	Industrial Radiography:		Constant control, imm. communication	
Category 2		Detect loss via verification	Exercises beforehand	34.23		Package tracking system, signature	
		Delay suff. to minimize prob. of removal	Written security instructions	Locked device or container		37.79(b)(2) Rail transport	
		Imm. resp. to interrupt removal	Confidentiality of schedules, routes	34.29		Package tracking system, signature	
		Restrict access to auth. persons only	Secure, redundant communications	Quarterly inventory		37.81(b), (f), (g), (h) Reports	
		Trustworthiness of auth. individuals		34.35(c)		NRC w/in 4 h for lost/missing	
		Identify and protect sensitive info.		Locked, phys. secured incl. transport		NRC asap recovery	
		Security plan		34.51			
		Capability to manage events in cont. plan		Cont. direct visual surv. of high rad. area			
		Event reporting system					
10D						CoC above the line nuclides	
		Security Level C	*$3000A_2$*	**Part 20 & License-Specific Controls**			173.22(c)
		Table 8	**Basic Security Level**	Portable guages			Adv. notification of dates and exp. arrival
		Reduce likelihood of unauth. removal	Section 4.2.	30.34(i)			
			Comp. auth. provide threat info.	Two ind. phys. cont. when not surv.			**HRCQ
		Imm. detection of unauth. access	Measures commensurate w/ threat				
		Detection of unauthorized removal	Equiv. measures for storage in transit	Medical licensees:			
		Imm. assessment of detection	Proc. to inquire about undelivered pkgs	35.67			
		Imm. comm. to response personnel	Closed conveyance if possible	Semi-annual leak test/inventory			
		Detect loss via verification	Addtl measures if on open conveyance	35.406			
Category 3		Delay suff. to reduce prob. of removal	Basic security awareness training	Accountability of brachy sources			
		Impl. approp. action in event of removal	Personnel identity verification	35.610			
		Restrict access to auth. persons only	Security verification of conveyance	Auth. user access: remote afterloaders,			
		Trustworthiness of auth. individuals	Written security instructions	teletherapy, gamma knife			
		Identify and protect sensitive info.	Information exchange				
		Security plan	Trustworthiness determination	Well logging:			
		Capability to manage events in cont. plan		39.31(b)			
		Event reporting system		Locked, phys. secured incl. transport			
D				39.35, 37			
		BSS general RAM controls		Semi-annual leak test/inventory			
		1.18, 3.44, 3.55		39.71(a)			
		Prev. sec. breaches - loss of control		Direct surv. during ops.		20.2201 (a)(i) & (b)	
		Prevent loss of control over sources				Imm. telephone report of loss + written	
		2.26					***Type B
		Regain control over lost/stolen sources		20.1801 Stored material			172.704(a)(4) Security awareness tng.
		2.35 Source registers		Secure from unauth. removal or access			
		3.53 Inventory sources		20.1802 Material not in storage		1000*App. C	
				Constant surveillance		20.2201 (a)(ii) & (b)	
		etc...				30 d telephone report of loss + written	
			Excepted non-special form/LSA-1/SCO-1				
			Prudent Management Practices			10*App. C	
			Basic control measures in the BSS				

Generally, nuclear material and waste are not included in table.

* Two out of ~350 radionuclides have $3000A_2$ values less than 10D and one equal to 10D

** 16 of ~350 nuclides have HRCQ values less than 10D

***58 SF nuclides have Type B values < D
130 SF nuclides have Type B values < 10D
136 NF nuclides have Type B values < D
226 NF nuclides have Type B values < 10D

16. References

[1] UNITED STATES NUCLEAR REGULATORY COMMISSION, Implementation Guidance for 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material", NUREG-2155 Rev.1, Washington, (2015).

[2] UNITED STATES NUCLEAR REGULATORY COMMISSION, Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material, NUREG-2166, Washington, (2014).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous quantities of radioactive material (D-values), EPR-D-VALUES, Vienna (2006).

[4] UNITED STATES NUCLEAR REGULATORY COMMISSION, The 2010 Radiation Source Protection and Security Task Force Report, August 11, 2010, Washington, (2010).

[5] UNITED STATES NUCLEAR REGULATORY COMMISSION, The 2014 Radiation Source Protection and Security Task Force Report, August 14, 2014, Washington, (2014).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities (NST048) (Revision of NSS No. 11), Draft Implementing Guide for Member State Comment, IAEA, Vienna (2016).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[9] UNITED STATES NUCLEAR REGULATORY COMMISSION, SECY-09-0086 - Enclosure 2: Regulatory Analysis re: Final Rule: Expansion of National Source Tracking of Sealed Sources (RIN 3150-AI29, Washington (2009).

[10] WOMEN'S SELF DEFENSE INSTITUTE, http://www.self-defense-mind-body-spirit.com/average-police-response-time.html , Accessed: 2015-11-03.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport (NST044) (Revision of NSS No. 9), Draft Implementing Guide, IAEA, Vienna (2016).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

[14] U.S. DEPARTMENT OF TRANSPORTATION, Guidelines for Selecting Preferred Highway Routes for Highway Route Controlled Quantities of Radioactive Materials, DOT/RSPA/HMS/92-02, Washington, DC (1992).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[16] EUROPEAN UNION, COUNCIL DIRECTIVE 2003/122/EURATOM of 22 December 2003 on the control of high-activity sealed radioactive sources and orphan sources, Official Journal of the European Union, L 346/57, Brussels (2003).

[17] UNITED STATES NUCLEAR REGULATORY COMMISSION, Reviewing the Common Performance Indicator, Technical Quality of Inspections, Procedure Number: SA-102, Washington (2007).

[18] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of Radiological Sources at U.S. Medical Facilities, GAO-12-925, Washington (2012).

[19] UNITED STATES NUCLEAR REGULATORY COMMISSION, Human Resources Training and Development Operating Procedure 0410, Rev. 2, Washington (2009).

[20] UNTITED STATES NUCLEAR REGULATORY COMMISSION, NRC Inspection Manual, Evaluation of Trustworthiness and Reliability Determinations, Temporary Instruction 2800/042, Washington (2015)

[21] U.S. OFFICE OF PERSONNEL MANAGEMENT, Questionnaire for Public Trust Positions, SF86P, Washington (1995). Downloadable from: https://www.opm.gov/forms/standard-forms/

[22] UNITED STATES FEDERAL REGISTER, Vol. 73, No. 137, Wednesday, July 16, 2008, p.40767; [USNRC Docket No. PRM-71-13; NRC-2007-0022], Washington, (2008)

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radiation Sources, IAEA Safety Guide No. RS-G-1.9, Vienna (2005).

[24] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources, GAO-14-293, Washington (2014).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Gilan, IAEA, Vienna (2002).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Lilo, IAEA, Vienna (2000).