UNITED STATES NUCLEAR REGULATORY COMMISSION INDEPENDENT ASSESSMENT CONSULTANT'S REVIEW OF TITLE 10 OF THE CODE OF FEDERAL REGULATION, PART 37 REQUIREMENTS TO PROTECT RISK-SIGNIFICANT RADIOACTIVE MATERIAL

Cheryl K. Rogers

5/5/16

EXECUTIVE SUMMARY

This report provides an independent review and assessment of the clarity of the requirements set forth in 10 CFR Part 37[11] to protect risk significant radioactive materials, including implementing guidance and best practices documents. Issues deemed to require clarity in Part 37, Implementing Guidance or Best Practices are addressed as recommendations. The data to support recommendations were obtained through interviews with or surveys of eight federal licensees-including two Master Material Licensees, eight private sector licensees, twelve Nuclear Regulatory Commission (NRC) Regional inspectors, seven Agreement State Programs, and NRC's Office of Nuclear Materials Safety and Safeguards (NMSS) and Office of Nuclear Security and Incident Response (NSIR) staff. The complementary roles and authorities of the NRC and the Department of Energy's National Nuclear Safety Administration (NNSA) are discussed. Data were extracted from the Nuclear Materials Event Database (NMED). Violations Data for Part 37 implementation were researched by NRC's 10 CFR Part 37 Program Review Team (PRT). Two GAO reports were used to develop survey questions: GAO-12-925 Report Nuclear Nonproliferation "Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities," (2012) and GAO-14-293 Report Nuclear Nonproliferation, "Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources," (2014). IAEA's "Security of Radioactive Sources," IAEA Nuclear Safety Series No. 11, issued in May 2009 was used as a standard to compare against Part 37.

GAO[5] (p. 25) questioned whether NRC's definition of collocation, [*term used in IC Orders*], may have the unintended consequence of placing a segment of these sources at greater risk or loss, i.e., Category 3 well logging sources that are segregated from each other and not subject to Part 37 requirements. The physical barriers are often robust and special equipment is usually required for source retrieval from downhole storage. This supports the Part 37 Rule Working

Group's determination that having to defeat at least two barriers provides adequate protection for Category 3 sources that could be aggregated to a Category 2 quantity.

Factors contributing to the NRC decision to require the licensee to make the T&R Determination are discussed. Elements of information required for T&R Assessment are reviewed and compared to IAEA's NSS-11[2] report. Concerns identified by GAO, including lack of specific disqualifying criteria, incomplete information, and who is responsible for making the determination are reviewed and evaluated. The elements to evaluate an individual's trustworthiness and reliability are prescriptive requirements. The actual T&R determination is performance-based and subjective based on all available information. It is the licensee's responsibility to determine if an individual is trustworthy and reliable. Text could be added to the Implementing Guidance clarifying that the goal of the T&R determination is more dependent on trustworthiness than on particular crimes that could be construed as indicative of an individual with terrorist activities.

GAO[4] (p. 37) recommended that NRC strengthen its security requirements by providing the specific measures licensees must take. NNSA's Global Threat Reduction Initiative (GTRI), now Office of Radiological Security (ORS), has a prescriptive approach with a set of pre-approved technologies (Tool Box). The result for licensees that accept GTRI enhancements is a blended approach of prescriptive and performance-based measures. The licensee is responsible for the effectiveness of the physical security program and performance testing. NNSA GTRI included training for the licensee and its local law enforcement agency (LLEA) at Y-12 in Oak Ridge, Tennessee, as part of the enhancement process. There are two reasons why Part 37 physical security requirements are performance-based. The first is due to a Commission Policy decision articulated in the 1999 White Paper that is based on extensive research and consideration of the results of more than 50 years of regulating reactors and materials applications. The second

is the practical consideration of the wide variety of licensees and the different operational needs. While it is possible to develop prescriptive regulations, the process would be onerous, inefficient and not robust compared to performance-based requirements.

Best Practices (NUREG 2166) is a good example of collaboration between NNSA and NRC. The NRC and NNSA meet routinely at five different levels of management to ensure each agency is aware of on-going activities. NRC and Agreement States have the authority and responsibility as the regulator. NNSA offers technology and training for licensees and their LLEAs at Y-12, Oak Ridge, Tennessee, as well as advice for licensees.

Seventy percent of NRC's initial 179 inspections against Part 37 resulted in no violations. For Subpart C, "New requirements" to Part 37[12], as compared to the IC Orders, comprised 38 percent of the violations and show that licensees have difficulties with regard to what should be included in the security plan and security procedures.

Thefts of high-risk radioactive sources under ICs and Part 37 requirements have only occurred for industrial radiography devices in Agreement States. The most recent theft was in 2015. Some of these events involved the truck transporting the device. For the thefts reported in the United States, human performance error was the root cause. An NRC staff reviewed and confirmed that seven of eight recent theft incidents reported in ITDB involved industrial radiography devices with Ir-192 sources.

Part 37 is effective in preventing malevolent use of radioactive material. A defense-in-depth approach is used in order that "the failure to meet a performance criterion, while undesirable, will not constitute or result in an immediate safety concern." This conclusion is based on 22 months of experience under Part 37 by NRC licensees. It is a snapshot-in-time and is biased toward fixed facilities and large companies. There have been no reports of an individual with malevolent intent obtaining or attempting to obtain Category 1 or 2 quantities of material.

Table of Contents

1. Introduction

This report provides an independent review and assessment of the clarity of the requirements set forth in 10 CFR Part 37[11] to protect risk significant radioactive materials, including implementing guidance and best practices documents. The review focuses on five issues: 1) criteria for trustworthiness and reliability (T&R) determinations; 2) performance-based vs. prescriptive requirements; 3) definition of "aggregated" sources; 4) transportation challenges for use of mobile sources; and 5) suggestions for improving Implementation Guidance for 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material,"[1] hereafter referred to as Implementing Guidance (NUREG-2155, Rev 1) and Physical Security Best Practices for the Protection of Risk-Significant Radioactive Materials[3], hereafter referred to as Best Practices (NUREG-2166). Issues deemed to require clarity in Part 37, Implementing Guidance or Best Practices are addressed as recommendations. Lines of inquiry considered but not pursued are identified and rationale given within the scope of each section.

2. Congressional Mandate

As a result of the terrorist acts of September 11, 2001, the Nuclear Regulatory Commission (NRC) implemented security requirements for radioactive sources considered to be risk-significant quantities. Congress requested several reports by the Government Accountability Office (GAO). Issues for NRC consideration have been identified by GAO since 2003. Implementation of requirements in a Final Rule, 10 CFR Part 37, took place in March of 2014 for NRC licensees. On December 16, 2014, Public Law 113-235, "Consolidated and Further Continuing Appropriations Act, 2015" was signed by the President of the United States. The statute provides annual funding for Federal Agencies, including the NRC. Section 403 of the legislation requires:

"…the Nuclear Regulatory Commission (NRC) to provide a report to the Committees on Appropriation of the House of Representatives and the Senate that evaluates the effectiveness of the requirements of 10 CFR 37 and determines whether such requirements are adequate to protect high-risk radioactive material. Such evaluation shall consider inspection results and event reports from the first two years of implementation of the requirements in 10 CFR 37 for NRC licensees."

The NRC requested an independent review of the "clarity of the 10 CFR Part 37 requirements, including guidance and implementation." NRC and licensees have 22 months of experience with implementation as of January 2016.

3. Information Reviewed

This review evaluates the experience of the NRC, Agreement States, and licensees in order to identify clarity issues with the newly promulgated regulation, hereafter referred to as Part 37. Suggestions are given for revisions or additions to Implementing Guidance and Best Practices. The data to support recommendations were obtained through interviews with or surveys of eight federal licensees-including two Master Material Licensees, eight private sector licensees, twelve NRC Regional inspectors, seven Agreement State Programs, and NRC's Office of Nuclear Material Safety and Safeguards (NMSS) and Office of Nuclear Security and Incident Response (NSIR) staff. Five Agreement States (Ohio, Iowa, Utah, Minnesota, and Maryland) have inspection experience under compatible Part 37 requirements as of January 2016. All Agreement States have 10 years of experience with the Increased Control (IC) requirements, and this experience is relevant to the effectiveness of Part 37 requirements.

The complementary roles and authorities of NRC and Department of Energy's National Nuclear Safety Administration (NNSA) are discussed. Collaboration between NRC and NNSA is evaluated. Global Threat Reduction Initiative (GTRI) enhancements are reviewed.

Two databases were used for identifying security trends in the United States and internationally. Data were extracted from the Nuclear Materials Event Database (NMED). A small sample of security incidents (eight thefts) from the International Atomic Energy Agency (IAEA) Incident and Tracking Database (ITDB) were reviewed by the NRC's 10 CFR Part 37 Performance Review Team (PRT) and discussed with the three Independent Assessment Consultants (IACs) who conducted an external review of Part 37.

Violations Data for Part 37 implementation were researched by NRC's internal PRT. The data were obtained from several Official Use Only (OUO) sources and substantiated with the actual Notice of Violation to the licensee. The results were summarized and provided to the IACs. This information was used to identify potential clarity issues.

Clarity issues were culled from two sources: Recent GAO reports and feedback from NRC, Agreement States, and licensees. Two GAO reports were used to develop survey questions: GAO-12-925 Report Nuclear Nonproliferation, "Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities" (2012), and GAO-14-293 Report Nuclear Nonproliferation, "Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources" (2014). These reports concern potential security issues with protection of radioactive materials from individuals with malevolent intent. IAEA's "Security of Radioactive Sources" IAEA Nuclear Safety Series No. 11, issued in May 2009 was used as a standard to compare against Part 37. Conclusions are an interpretation of NRC, Agreement State, and licensee feedback and provide the basis for recommendations. Appendix A is provided to cross reference Part 37 and guidance documents to the recommendations made.

4. Subpart A – General Provisions

A. <u>Aggregation of Sources</u>

i. Scope

This section identifies clarity issues with the definition of "Aggregated." Two or more sources that collectively exceed the Category 2 threshold will be subject to the security requirements of Part 37. GAO[5] (p. 25) questioned whether NRC's definition of collocation, [*term used in IC Orders*], may have the unintended consequence of placing a segment of these sources at greater risk or loss, i.e., Category 3 well logging sources that are segregated from each other and not subject to Part 37 requirements.

ii. Summary

The definition of "Aggregated" is understood by the licensees and the inspectors. Security is ensured for Category 3 sources that are segregated, such as well logging sources in storage or fixed gauges at refineries, due to the need to defeat more than one barrier for each source that could potentially be aggregated with other sources to a Category 2 quantity. Access control or direct surveillance are acceptable security measures for Category 3 sources that are momentarily aggregated during a source exchange or gauge removal without the need to implement Part 37 requirements.

B. Observations

A Part 37 Working Group member stated that the definition of collocation/aggregation was developed for the Manufacturing and Distribution (M &D) Orders and used in the IC orders. The term was revised from "collocated" to "aggregated" and defined in Part 37. The definition of aggregated provides a level of reasonableness for the implementation of the security requirements. The requirement to use an additional barrier for the purpose of segregating the sources is beyond the Storage and Control of Licensed Material requirements in 10 CFR Part 20.1801 and 20.1802. The Working Group believed that having to defeat two barriers provided adequate protection against aggregation of Category 3 sources to a Category 2 quantity. An

NRC Regional inspector explained that “collocated” was changed to “aggregated” because for some law enforcement and security entities, collocated can mean located in the same building/general area and not specific to a security zone.

The need to segregate sources is only applicable to a subset of licensees such as well loggers and fixed gauges. One NRC Regional inspector suggested that GAO may not have understood that downhole storage involves placing Category 3 quantities in storage such that it does not meet the definition of aggregated. Well loggers typically do not possess any Category 2 sources, however, their license may authorize a total possession limit above the Category 2 threshold due to multiple sources, locations or a combination of both. These licensees are not under Part 37 requirements as long as the Category 3 radioactive material is not aggregated. A possible exception is a licensee in an Agreement State that requires implementation of Part 37 based on licensees’ possession limits being above the Category 2 threshold.

In response to a question regarding whether aggregation or collocation was a better term, a well logging licensee stated that “collocated is a better description.” An NRC Regional inspector and several Agreement States supported “collocated” as a simpler term that is more easily understood. This well logging licensee stated that they have not “experienced difficulties with our Operations.” An NRC inspector from Region IV stated that although well logging companies are not generally required to implement Part 37 requirements, at least four of the largest companies have implemented security measures similar to Part 37 requirements as a good practice. A Region III Inspector noted that she had inspected a well logging company that did aggregate sources to greater than Category 2 quantities and implemented the Part 37 security requirements. The Region IV inspector noted that well logging sources are often stored in a manner that requires special equipment to retrieve them. There were no issues identified with either the definition of aggregation or the practice of segregation. In conclusion, no further consideration of the clarity of the definition of aggregation is needed.

An NRC staff member who worked on the Best Practices document (NUREG 2166) stated that it is not the intent or practice to require implementation of Part 37 for those instances when Category 3 sources are temporarily collocated or when collocation is an exceptional circumstance e.g., only occurs once a year. The NRC staff stated that if the collocation is a common or routine practice, then the licensee should be under Part 37. This is contradicted by the text in the Best Practices document on p. D-3 and should be revised to state that "*access control or constant surveillance or a combination of both* should be implemented if a physical barrier, which has been installed to isolate the remaining aggregated gauges from other gauges, is breached *temporarily under exceptional circumstances or for a limited period of time*, (e.g., during a source exchange or gauge removal)."

C. Conclusions and Recommendations

In regard to the GAO[5] (p. 25) issue of "NRC's definition of collocation may have the unintended consequence of placing a segment of these sources at greater risk," the licensee and NRC inspectors are aware of the requirement, beyond 10 CFR 20.1801 and 1802, for an additional physical barrier to segregate sources. The physical barriers are often robust, and special equipment is usually required for source retrieval from downhole storage. This supports the Part 37 Rule Working Group's determination that having to defeat at least two barriers provides adequate protection for Category 3 sources that could be aggregated to a Category 2 quantity.

The Best Practices document (NUREG 2166) states on page D-3 that Part 37 should be implemented for all instances of collocation. The guidance does not allow consideration of a temporary situation such as source exchange or the infrequency of occurrence. This is contrary to the intent and current practice, which permits temporary collocation under exceptional circumstances. This issue was not raised by licensees who segregate their sources, however, it is not consistent with current practice, and the text in the guidance document should be revised.

Recommendation:

1. Revise the Best Practices document (NUREG 2166) to clarify the circumstances when aggregation does not require implementation of Part 37 regulations. A suggested revision is: "the licensee must implement *access control, constant surveillance or a combination of both* if a physical barrier, which has been installed to isolate the remaining aggregated gauges from other gauges, is breached *temporarily under exceptional circumstances or for a limited period of time* (e.g., during a source exchange or gauge removal)."

5. Subpart B – Background Investigations and Access Control Program

A. Trustworthy and Reliability (T&R) Determinations

i. Scope

This section reviews if the T&R determination process is clear to licensees and suggests enhancements to guidance. Feedback from private sector licensees, federal licensees, and inspectors is presented. Factors contributing to the NRC decision to require the licensee to make the T&R Determination are discussed. Elements of information required for T&R Assessment are reviewed and compared to IAEA's NSS-11[2] report. Concerns identified by GAO, including lack of specific disqualifying criteria, incomplete information, and who is responsible for making the determination are reviewed and evaluated. The T&R determination process under 10 CFR Part 73 for individuals granted unescorted access in Nuclear Power Plants (NPPs) is considered. Violations Data, a compilation of initial violations under Part 37, are reviewed for trends. A licensee and two Agreement States mentioned difficulties understanding who should evaluate the initial or reinvestigation of the Reviewing Official (RO). This issue was considered but not pursued due to lack of violations. Enhancements to clarify Part 37 requirements are suggested for the Implementing Guidance.

ii. Summary

Licensee and inspector feedback identified challenges to the Unescorted Access Authorization Program. Issues identified were difficulties with making a subjective determination and a need for guidance on how much information should be included in the procedures. The determination process places the responsibility on the licensee to gather, evaluate and decide if an individual can reasonably be expected to be trustworthy and reliable. Emphasis should be placed on the trustworthiness aspect of the determination in the guidance. Private sector licensees are more uncomfortable with this T&R determination process than federal licensees.

Licensees specifically expressed discomfort with reviewing Federal Bureau of Investigation (FBI) background checks and suggested that a specific list of disqualifying crimes should be provided. Part 37 regulations, Implementing Guidance and Best Practices provide substantive resources for the licensee's T&R determination process. The NRC does not provide a checklist or specify disqualifying criteria in Part 37. The NPP industry, regulated under 10 CFR Part 73, developed a set of potentially disqualifying criteria with Nuclear Energy Institute (NEI) 03-02 (OUO). Similar to Part 37 requirements, NPP licensees must make a judgement call based on the available information. A rationale is given as to why this process must be performance-based and a suggestion made on how to address the discomfort of private sector licensees.

Violations Data from March 19, 2014-September 25, 2015, show 54% of the violations for Subpart B are for 'new requirements' to Part 37 as compared to IC requirements. Most of the violations were Severity Level IV, non-escalated enforcement action. One violation was a Severity Level III, potentially escalated enforcement action. Implementing Guidance should be enhanced to address the 'new requirements,' especially the unescorted access program, implementing procedures, and annual program review.

B. Observations

i. Private Sector Licensees

Private sector licensees stated that they faced challenges in determining which employees are trustworthy and reliable. Issues raised were: the determination is very subjective and results in inconsistencies across the industry; lack of expertise in conducting background checks and evaluation of criminal history reports; and determining who is suitable for T&R determinations such as Radiation Safety Committee members and ancillary personnel. One suggestion made was to include specific items identified during the criminal history check that would disqualify the individual from unescorted access. This idea was also suggested by an Agreement State. One commenter notes that for employees who could not meet the requirements and had to be re-assigned, the company appreciated that it gave them a legal framework to use. One commenter suggested that NRC consider a program similar to the Transportation Safety Administration's (TSA) Transportation Worker Identification Credential (TWIC) process in which the licensee provides the background information, and the NRC completes the T&R evaluation and provides the conclusion back to the licensee. Another licensee suggested that a security professional is needed to interpret the FBI background data. He said he has learned to put more weight on willfully writing bad checks, as that shows the individual is not trustworthy.

One licensee raised a question concerning the 10-year re-investigation requirement for ROs. He thought it was awkward, since he functioned as both an RO and the licensee, to determine who should adjudicate the background check. The licensee has two ROs, so they plan to adjudicate each other. An Agreement State stated that they have raised this issue to NRC.

ii. Federal Licensees

Federal licensees did not experience challenges or identify problems with making T&R determinations because a background check is a condition of employment. U.S. Army, Uniform

Services Uniform Health System, and U.S. Air Force stated that permanent employees are fingerprinted and adjudicated through the Joint Personnel Adjudication System (JPAS). Veterans Administration (VA) uses National Agency Checks. Another licensee reported that they have to do Single Scope Background Investigations (SSBI) for personnel who have access to biological agents. Since the high-risk source is collocated with the biological agent, only personnel that are in the Personnel Reliability Program can have access to that room.

One Federal licensee with a large program of contractors and visiting fellows complained about the 7-year review period specified in 37.25. If they were Federal employees, they could be adjudicated under Homeland Security Presidential Directive-12 (HSPD-12), National Agency Check with Written Inquiries (NACI) Level 1 background investigation under a 5-year time-frame (37.29(a) would be applicable). Since they are not Federal employees, they must undergo a Moderate Risk Background Investigation (MBI) Level 5b, which meets the 7-year time-frame. The alternative process is much more expensive and takes longer. A Radiation Safety Officer (RSO) stated that this change would vastly assist in the T&R approval process for these individuals.

iii. NRC Regional Inspectors

NRC Regional Inspectors expressed a range of viewpoints on the T&R determination process. One inspector stated that the IC/Order requirements are nearly the same as the Part 37 requirement. Another felt that licensees and ROs are aware that the individuals they hire form the foundation of their business, and those individuals need to have integrity and be reliable. Licensees with mobile sources, i.e., industrial radiography, often deny unescorted access and employment to applicants with sufficiently serious driving infractions, such as drunk driving or speeding. An inspector noted that the majority of licensees do not have applicants with criminal records with the exception of radiographers that may have a criminal history, including drug

possession, domestic abuse, petty theft, or writing bad checks. Each category of licensee has different ideas of the type of criminal record they will and will not accept in making its T&R determination. Another inspector commented that NRC provided almost no guidance on what was acceptable and what was not for T&R determinations. Radiological personnel are now being asked to perform a security function according to another inspector. He suggested that more guidance needs to be developed for use by human resources (HR), security, and radiation safety personnel at licensees' facilities.

Inspectors also noted that Hospitals and Blood Irradiator Laboratories have had their own HR guidelines for hiring in place for many years. Federal facilities or large medical facilities already require security clearances and background checks as conditions of employment. One inspector stated that a licensee noted that its HR qualifications for hiring are actually more stringent than Part 37 T&R determination requirements.

There is still confusion about whether an RO has to have access to the high-risk radioactive material. An inspector noted that a lot of T&R determinations are made by HR personnel and not radiation safety and would not need access. Part 37 requires access be granted to the RO.

Licensees expressed frustration that if there was a [terrorist] incident, the blame would be placed on the licensee. The inspector noted that if the NRC provided the "green light/red light" for the T&R determinations, i.e., the NRC made the T&R determination, responsibility for any [terrorist] incident would fall on the NRC. In his opinion, licensees were not feeling challenged from a "lack of security experience and training," but from a liability standpoint.

iv. NRC Decision to Require the Licensee to Make T&R Determination

When the NRC issued orders for Panoramic and Underwater Irradiators and Manufacturing and Distribution (M&D) licenses, it did so under its "common defense and security" authorization. An

M&D licensee stated that under the Order issued in 2003, the T&R Official [now RO] was nominated by the licensee, and the NRC completed the T&R evaluation and provided the evaluation back to the licensee. According to the Federal Register Notice for Part 37[11], (p. 16923), a major change since those initial Orders were issued is that Congress passed, and the President signed, the Energy Policy Act (EP Act) in 2005. Section 149 of the Atomic Energy Act was amended to authorize the Commission, if they deemed it necessary, to require any individual who is to be permitted unescorted access to high-risk radioactive material to be fingerprinted and that an FBI criminal history background check be conducted. NRC issued Part 37 under its health and safety authority for two groups of licensees: those formerly under NRC jurisdiction due to issuance of Orders under "common defense and security" authority and those licensees formerly under NRC and Agreement States jurisdiction due to issuance of [Increased Controls] Orders under "health and safety" authority. This allows Agreement States to have jurisdiction and be responsible for implementation, inspection, and enforcement of Part 37 compatible regulations.

When Part 37 was a proposed rule, comments were requested on who should be responsible for approval of the RO. The discussion in the Federal Register for the Final Rule[11] (p. 16949) stated that some [Agreement] States may not have the authority to adjudicate fingerprints for approval. NRC may not have had the authority to adjudicate T&R determinations for the RO under its health and safety authority according to an NRC project manager. NRC made the decision for the licensee to approve the RO with an evaluation conducted similar to that required for an individual needing approval for unescorted access. The NRC[11] (p. 16949) decided that "implementing these regulations under the NRC's public health and safety authority avoids potential complications with licensees being subject to dual regulatory authority for a single licensee. Agreement States can impose these requirements because they provide a 'reasonable assurance' of preventing the theft or diversion of Category 1 and Category 2

radioactive material that has a potential to result in significant adverse health impacts and reasonably constitutes a threat to public health and safety."

The issue of who should make the T&R determination for employees requiring unescorted access to high-risk radioactive material was not discussed directly in the Federal Register Notice for Part 37. In response to a comment cited in the Final Rule[11] (p. 16957) asserting that licensees do not have the knowledge or skill to ensure that personnel are reliable and trustworthy, the NRC states, "These determinations do not require specialized knowledge or skills and are similar to the determinations that licensees make in hiring decisions." The same T&R determination process is used for ROs and employees requiring unescorted access to high-risk radioactive material. If the NRC determined that the licensee is responsible for determining whether the RO can be certified as T&R, a similar logic can be applied as to why the NRC determined that it is the licensee's responsibility to make the T&R determination for employees requiring unescorted access. The licensee is in the best position to make the evaluation if it is a subjective determination based on trustworthiness.

v. Elements of Information Required for T&R Assessment

Elements of information required for the T&R determination in 10 CFR 37.25 are prescriptive. They include fingerprinting and background investigation, verification of true identity, employment history verification, verification of education and reference checks, and character and reputation of the individual who has applied for unescorted access. NRC has exceeded IAEA's NSS-11[2] standards by requiring fingerprinting and background checks. NSS-11[2], (p. 32) states, "The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's regulations or as determined by a regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person."

With the exception of fingerprinting and background checks, the elements of information are similar to the elements of information required for any job applicant. Abundant guidance is available for licensees in Implementing Guidance (NUREG 2155) and Best Practices (NUREG 2166) documents. Implementing Guidance states that background investigations under 10 CFR 37.25 are designed to identify past actions that might call into question an individual's T&R and provides detailed suggestions for the determination, (see Appendix A, pages 57-58 & Annex A). It may be helpful to clarify that the bottom line is trustworthiness or truthfulness of the individual. Guidance in Best Practices (pages 3-4) provides suggestions on how to assess potentially negative criminal history information, e.g., individual's age and maturity at the time of the conduct. Appendix A, Best Practices, contains suggestions of topics to address for access authorization and trustworthiness and reliability in the Physical Security Plan, (page A-7).

vi. Lack of Specific Disqualifying Criteria

Part 37 requires licensees to document the basis for disqualifying a candidate for unescorted access to radioactive material in quantities of concern. NRC does not have detailed information on how many individuals are denied unauthorized access and what types of information licensees use to disqualify candidates. NRC inspectors will gather information for one year under Temporary Instruction (TI) 2800/042[14] to: determine if licensees have: chosen to establish criteria, collect and document specific information on the T&R determination process and review the effectiveness of the access authorization program and background investigation requirements. NRC inspectors stated that, in their experience, licensees do not develop specific disqualifying criteria but make T&R determinations on a case-by-case basis.

The TI data will show the specific types of information that resulted in denial of the individual for unescorted access. This will be useful in understanding the specific challenges that licensees face with evaluating information and making subjective determinations. The NRC inspectors will

determine and document whether a “conviction, charge, or report” involving seven categories of circumstances occurred: three pertaining to terrorist activities, “misrepresented, falsified, or omitted relevant information”, “felonies that may, in the opinion of the RO, indicate poor judgement, unreliability, or untrustworthiness,” “reliable derogatory information from a previous employer or other NRC-licensed facility” and “was involved in any other conduct or subject to any other circumstances which, in the opinion of the licensee certifying official, tend to show that the individual may not be trustworthy or reliable.”

vii. Incomplete Information

GAO[5] (p. 31-32) identified one example of a licensee determination when information was not available. The FBI background check was incomplete. Although it is not clear how the information eventually came to the licensee’s attention, the additional information caused the T&R official to state that she would not have granted unescorted access if all the information had been available. The licensee has the responsibility to re-evaluate and update the determination any time new background information becomes available. There is a method in Part 37, (37.23(e)(4)), for withdrawal of unescorted access authorization approval if the RO deems it necessary due to unfavorable information. The NRC contacted the Agreement State for information and concluded that this was an isolated incident. In conclusion, the issue of a lack of available information at the time of determination does not require further consideration as the RO has a mechanism to withdraw the authorization in Part 37.

viii. Reviewing Officials (ROs) Makes T&R Determination

The second instance of a questionable determination raised by the GAO[5] (p. 32) concerned a T&R Official (RO) who stated that he considered an individual a risk but was over-ruled by his supervisor. The individual was later arrested for stealing from the company. Best Practices states, “*the management of the organization must provide the requisite authority, leadership,*

support, and resources to the physical protection program." This example highlights that the T&R determination is closely linked to the hiring decision. In conclusion, the issue does not warrant further consideration as Part 37, (37.23(b)), requires the RO(s) to make the T&R determination.

ix. Nuclear Power Plant Experience with T&R Determination Process

The NPP experience with T&R determinations is relevant and provides insight into the issues surrounding specifying disqualifying criteria. The Final Rule[16] (p. 13931) for Power Reactor Security Requirements states, "The Commission does not agree that the NRC's unescorted access requirements described in § 73.56 [similar to Part 37 for access authorization program] and § 73.57 need to contain prescriptive disqualifiers for access. Licensees are required by § 73.56(h) in this final rule to *consider all of the information obtained* [emphasis added] in the background investigation for determining whether an individual is trustworthy and reliable before granting unescorted access." The nuclear industry, through the NEI, developed a guidance document, NEI 03-01. Licensees can commit to following NEI 03-01, (Official Use Only), and will be inspected against this procedure. The terminology used in NEI 03.01 is "potentially disqualifying criteria" according to NRC staff. A former NRC NPP Security Inspector explained that T&R Determinations required under 10 CFR 73.56 are performance-based. He explained that many decisions to deny unescorted access are based on lack of truthfulness in the information given by the applicant. If each power reactor licensee must make a decision to grant or deny access to its facility based on "all of the information obtained", then it makes sense that the requirement is performance-based in order to permit the licensee flexibility to assess truthfulness. The regulation is prescriptive in describing all the information that must be evaluated. Performance-based requirements are discussed in the Section 6.

Personnel Access Database System (PADS) is operated by Canberra and Associates under contract to NEI for the nuclear industry. This system came about as a result of Orders requiring an information sharing database (now in 10 CFR Part 73). Each NPP enters the individual's name into PADS and whether they were granted or denied access. The reason why is not specified. If it was a denial or unfavorable termination, then the NPP has to contact the previous employer to discuss. There is a Task Force comprised of NPP and NRC Heads of Access/Fitness for Duty representatives who meet quarterly to discuss PADS issues. There are early stages of discussion going on now about how to standardize disqualifying criteria. A best practice for consideration may be for an industry, such as industrial radiography, to develop an information sharing database of individuals approved and denied unescorted access.

x. Violations Data

Violations Data show 54% of the violations are for "new requirements" to Part 37, Subpart B, identified on the Comparison Chart[12], as compared to IC requirements. Violations of the 'new requirements' are: (1) security training not given to individuals granted unescorted access, (3) informed consent not done, (16) implementing procedures lacking, (1) not performing an access authorization program review and (1) not documenting the annual review. All the new requirement violations were Severity Level IV, non-escalated enforcement. There was one Severity Level III violation, potentially escalated enforcement, concerning granting access to an individual prior to completing a background investigation.

xi. Implementing Guidance (NUREG 2155)

Implementing Guidance for Part 37 utilizes a Question and Answer (Q&A) format because Part 37 is a new regulation. The document addresses every portion of the regulation and is organized the same as Part 37. The approach is similar to the guidance issued for 10 CFR Part

20 when it underwent a major revision. Standards for Protection are applicable to every user of radioactive material, however, 10 CFR Part 20 is not a 'licensing' part of the regulations. Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material applies to a sub-set of users that includes many types of licensees, however, Part 37 is also not a 'licensing' part of the regulations.

Information that can be modified and used by a licensee for their unescorted access program includes Annex A, Additional Guidance for Evaluating an Individual's Trustworthiness and Reliability for Allowing Unescorted Access to Certain Radioactive Material, and Annex B, Sample Consent Form for Background Investigations. Although the licensee is not required to submit its procedures, the extent of information required to meet 37.23(f) could be discussed, and a sample procedure added to the Implementing Guidance.

The elements of information and background investigation process are prescriptive, see Fig. 1. A checklist or 'audit' would assist the licensee with its annual review of unescorted access program.

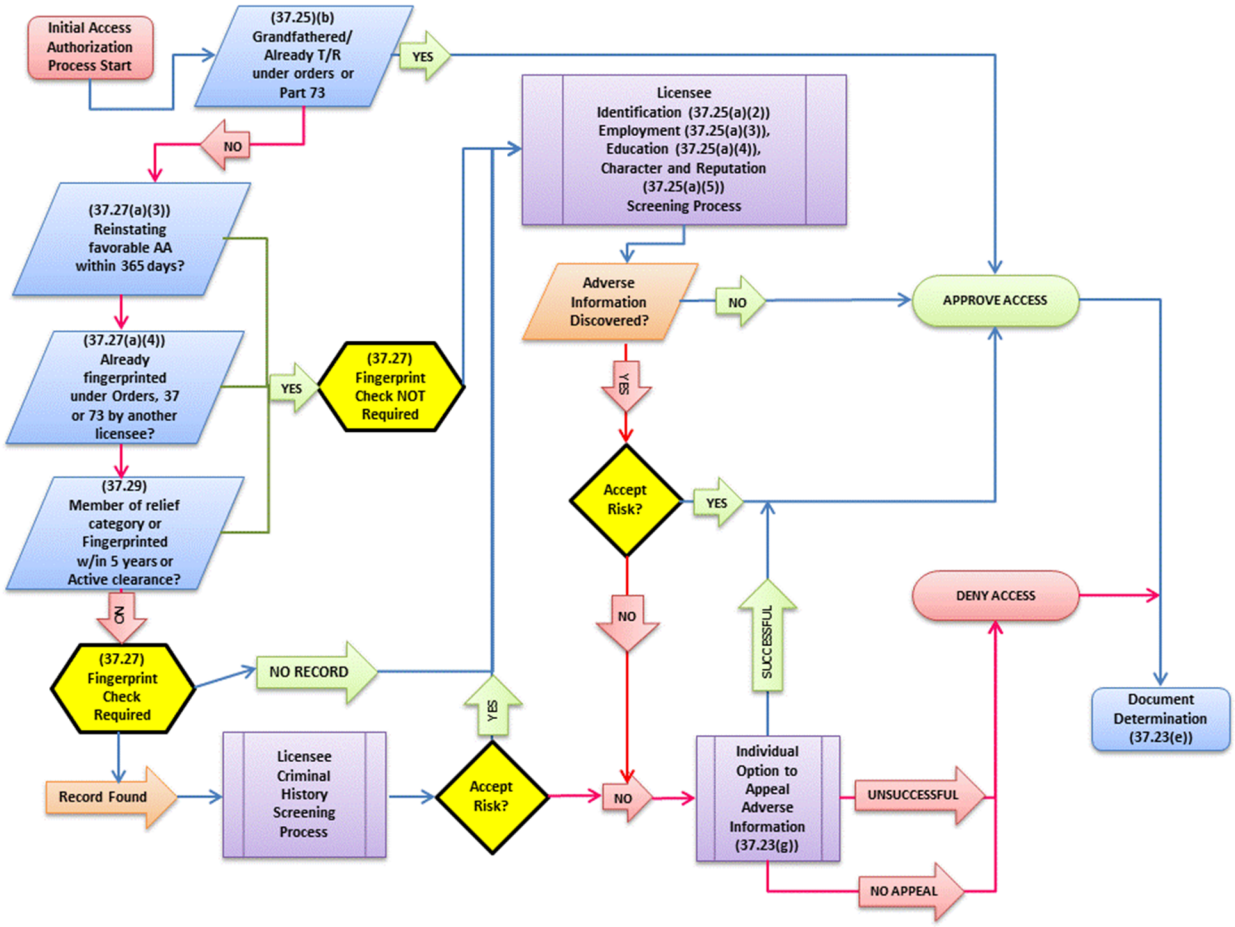

Figure 1, from NUREG 2166, Fig. 3.1

C. Conclusions and Recommendations

The T&R determination process is similar to making a hiring decision with the addition of fingerprinting and FBI background check. The elements to evaluate an individual's trustworthiness and reliability are prescriptive requirements. The actual T&R determination is performance-based and subjective, based on all available information. It is the licensee's responsibility to determine if an individual is trustworthy and reliable. Private sector licensees are uncomfortable with reviewing FBI background checks, as they are unsure what they should be looking for. A suggestion was made by an Agreement State to specify a short list of offenses such as treason or theft. One licensee boiled the determination down to whether an individual is

trustworthy based on truthfulness. This approach is supported by an NRC NPP Security inspector who observed that many of the denials are due to lack of truthfulness. Text could be added to the Implementing Guidance clarifying that the goal of the T&R determination is more dependent on trustworthiness than on particular crimes that could be construed as indicative of an individual with terrorist activities. The T&R determination is time-consuming if someone does have a record, but the information can be ferreted out or a probationary period used. An individual has the right to see the basis for the denial of unescorted access and must be given the opportunity to correct the information. An individual may request that information used to make the T&R determination be shared with another company. A best practice could be to set up an information-sharing database for a particular industry, for example, industrial radiography.

Licensees may use any or all of the potentially disqualifying criteria from the Implementing Guidance, Annex A, to deny unescorted access. They may set their own criteria such as a TWIC credential. Best Practices also provides guidelines on what to consider when it is necessary to make a judgement call due to potentially disqualifying information. T&R determinations are made on a case-by-case basis for many organizations and companies according to NRC inspectors. Large medical organizations and the Federal government do not have the same challenges as smaller organizations or businesses. A Temporary Instruction will provide valuable information on what kind of information results in denial of unescorted access in December 2016. Results should be reviewed for any lessons learned and shared as appropriate.

Initial inspections under Part 37 identified clarity issues as shown by the Violations Data and reported by NRC Regional inspectors. Implementing Guidance should be updated with additional information or model procedures to assist licensees in complying with 10 CFR 37.23(f). There were also violations cited against lack of annual program review and failure to

document the review. The inclusion of a checklist or 'audit' form would benefit licensee compliance and, thus, ensure the effectiveness of the unescorted access program.

Recommendations:

2. Add text to the Implementing Guidance (NUREG 2155) clarifying that the purpose of the T&R determination is essentially to determine if someone is trustworthy by assessing their truthfulness.

3. Add to Best Practices (NUREG 2166) that an industry, such as industrial radiography, develop an information sharing database of individuals approved and denied unescorted access similar to sharing of information in PADS for NPPs.

4. Review the results of Temporary Instruction 2800/042[11] for examples of the licensee's basis for making a negative T&R determination. Identify whether the basis is subjective, i.e., an evaluation of truthfulness, or specific criminal offenses. Use this information to develop additional guidance.

5. Add detailed information of content needed for access authorization program procedures required by 10 CFR 37.23(f) to Implementing Guidance (NUREG 2155).

6. Include a checklist or 'audit' form that could be used to conduct and more uniformly document the annual unescorted access program review required by 10 CFR 37.33(a) to Implementing Guidance (NUREG 2155).

6. Subpart C – Physical Protection Requirements During Use

A. Performance-based Requirements versus Prescriptive Requirements

i. Scope

This section discusses performance-based versus prescriptive requirements and licensee feedback concerning lack of clarity with Subpart C requirements. Issues raised by GAO[5] (p. 8, 10, 11) challenging the effectiveness of the requirements for physical protection of radioactive material are evaluated. Performance-based requirements were portrayed as: only general provisions, minimum requirements, implemented from a menu of options, providing a general framework, too broadly written and not providing specific directions. GAO[4] (p. 37) recommended that NRC strengthen its security requirements by providing the specific measures licensees must take. GAO[5] (p. 11) states that the NNSA's Global Threat Reduction Initiative (GTRI) program has implemented security measures "*to raise the security to a level that is above NRC/AS* [Agreement State] *requirements*". GAO[4] (p. 39) report states:

> "*It stands to reason if NNSA has identified security vulnerabilities…and taken actions to address them, then the NRC's existing security controls need to be strengthened."*

Finally, GAO[5] (p. 40) recommended that NRC and NNSA collaborate more effectively. GTRI enhancements were reviewed, and collaboration between NRC and NNSA was assessed.

ii. Summary

The history and experience of deterministic (prescriptive) and performance-based requirements are reviewed, and the rationale for selection of performance-based requirements by the Commission is discussed. Terms such as 'flexible approach' and 'framework' are explained by referencing a White Paper on Risk-Informed and Performance Based Regulation[13]. NNSA's GTRI, now Office of Radiological Security (ORS), has a prescriptive approach with a set of pre-approved technologies (Tool Box). NRC supports the NNSA efforts, but considers them enhancements instead of upgrades. NNSA also considers these enhancements as above and beyond what is required to secure the high-risk radioactive material[6] (Module 15, page 5).

Some licensees have not accepted NNSA's enhancements due to not meeting their operational needs. Collaboration between NRC and NNSA was reviewed, and the agencies interactions were evaluated.

B. Observations

i. Performance-based versus Prescriptive Requirements

Performance-based regulations for physical security of high-risk radioactive material are more effective than prescriptive regulations. The NRC came to this conclusion in 1999 as documented in SECY-98-144, White Paper on Risk-Informed and Performance-Based Regulation[13], referred to as the 'White Paper.' The Commission advocated "the use of risk-informed and ultimately performance-based approaches" to regulation. The White Paper notes that "the probabilities of accidents for adversely affecting public health and safety" were quantified in 1975 in Reactor Safety Study, WASH-1400. The promulgation of performance-based requirements for physical security in Part 37, specifically 10 CFR 37.41(b), is a result of the Commission Policy.

The White Paper notes that the situation is more complex for materials licensees than reactors. In discussion with NRC staff concerning the concept of more prescriptive regulations, the staff stated it would be difficult to address all the categories of licenses subject to the security requirements. There are variations of use within a category, as each licensee has different operational needs. To pursue the idea of the scope required to develop prescriptive regulations, the following categories of licensees, according to Inspection Procedure[10] (IP 87137, p. 1) would need to be addressed: 1) manufacturing and distribution facilities; 2) self-shielded irradiators; 3) open-beam calibrators; 4) pool type irradiators; 5) medical facilities with blood irradiators and/or gamma-ray stereotactic (gamma-knife); 6) radio-pharmacies; 7) industrial radiography; and 8) licensees transporting Category 1 and Category 2 quantities of radioactive material.

Further regulatory guidance would need to be developed to address the products, issues, and processes to be employed. Interpretation would be required for any deviation from the prescribed requirements for specific licensee situations. The NRC has a lot of experience with the prescriptive approach and is familiar with developing guidance to assist licensees. The White Paper states, "the current body of regulations, guidance and license conditions is based largely on deterministic analyses and is implemented by prescriptive requirements."

The Commission acknowledges that the current regulations are largely prescriptive but advocates for a risk-informed, performance-based approach. This approach, according to the White Paper, "relies on measurable (or calculable) outcomes (i.e. performance results) to be met." Additional characteristics are: 1) "objective criteria [emphasis added] to assess performance are established;" 2) performance history; 3) "flexibility [emphasis added] to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes [emphasis added]; "and 4) "a framework [emphasis added] exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern. The Commission has decided that, when feasible, performance-based requirements are advantageous, because they will encourage innovation and improved performance.

The approach to inspection differs depending on whether prescriptive or performance-based requirements are used. "A prescriptive requirement specifies particular features, actions or programmatic elements to be included in the design or process, as the means for achieving desired outcome" according to the White Paper. An inspector reviewing a licensee against prescriptive requirements would use a lengthy checklist to evaluate whether required elements were in place. It is possible that a licensee could have all the specified elements but not be able

to achieve the outcome due to an unknown local condition, e.g., limited cell phone coverage or a difference in operational conditions that is not recognized.

In summary, there are two reasons why Part 37 physical security requirements are performance-based. The first is due to a Commission Policy decision articulated in the 1999 White Paper that is based on extensive research and consideration of the results of more than 50 years of regulating reactors and materials applications. The second is the practical consideration of the wide variety of licensees and the different operational needs. While it is possible to develop prescriptive regulations, the process would be onerous, inefficient, and not robust compared to performance-based requirements. The flexibility granted the licensee to develop the security program entails a great deal of work to develop a security plan identifying the specific targets (high-risk radioactive sources), the security assessment methodology and provide information on how the design of the security system achieves sufficient protection. The bottom line is that the licensee must demonstrate that the high-risk radioactive material is secured from those with malevolent intent.

ii. National Nuclear Security Administration (NNSA) Global Threat Reduction Initiative (GTRI) Program

NNSA's GTRI program has prescriptive requirements for certain technologies based on risk as specified in an internal OUO document, "Protection and Sustainability Criteria" (2010). GTRI's domestic security enhancements program aligns with one of three mission statements[19], specifically to "Protect high priority nuclear and radiological materials from theft." The physical protection security enhancements must meet Part 37 performance-based requirements. Licensees who enrolled in the voluntary GTRI program discuss any problems they have with its security measures with NNSA. The NNSA conducts an on-site walk-through for each facility. GTRI used a model vulnerability assessment that is representative of the type of site and use of material. Each licensee is provided with recommendations and offered technologies that were

standardized and pre-approved from the NNSA “Tool Box”. Licensees could select any or all of the recommendations taking into account their preferences and operational needs. Two licensees, a pool irradiator and an industrial radiography company, declined GTRI-proposed enhancements. One licensee stated that the reason was a clear disconnect between understanding the purpose of the use of radioactive materials and the proposed security measures. The licensee further explained that NNSA needs to understand what we do in order to design a system that works. The licensee has been proactive in providing tours to NNSA staff and hopes the next generation of security measures will be a better fit. The result for licensees that accept GTRI enhancements is a blended approach of prescriptive and performance-based measures. The licensee is responsible for the effectiveness of the physical security program and performance testing. NNSA GTRI included training for the licensee and its LLEA at Y-12 in Oak Ridge, Tennessee as part of the enhancement process. NNSA conducted follow-up visits for the first 3-5 years, depending on the contract signed by the licensee. When the contract expires, the licensee is responsible for maintenance and testing of the equipment.

The GTRI enhancements provided the licensee with a robust detection system according to one NRC Regional inspector. A Federal licensee who participated in the GTRI program stated that this resulted in best practices for his facilities. Two licensees particularly liked being able to contact the NNSA contractor with physical security issues or problems. One licensee is no longer under contract and must pay for the service. She stated that she felt comfortable asking for advice from the GTRI staff because they gave her a “best practices” answer without attributing the practice to a particular licensee. The licensee must ensure that the GTRI enhancements are integrated into its security program including, for example, the communications system. GAO[4] (Introduction to report) was concerned about the sustainability of the NNSA program enhancements due to the fact that the licensee was not required to pay

for and continue the annual maintenance. Part 37 requires the licensee to conduct annual maintenance and testing. Over time, new approaches will be developed that are more efficient and cost-effective. These new approaches should be included in Best Practices (NUREG 2166) or shared with licensees and regulators in a manner that does not violate protection of security information requirements.

iii. Collaboration between National Nuclear Safety Administration (NNSA) and Nuclear Regulatory Commission (NRC)

Best Practices (NUREG 2166) is a good example of collaboration between NNSA and NRC. NNSA contributed information on the available technology and equipment to consider for physical security. NRC contributed the detailed explanations for access authorization, security plans and procedures, training, Local Law Enforcement Agency (LLEA) coordination, information protection, and maintenance and testing. As one NRC inspector observed, best practices are exhibited by engineering over administrative controls, incorporating redundancies to avoid single point failure conditions, and training personnel in the "why" and not just the "what". Licensees who have promoted safety culture tenets-specifically fostering a questioning attitude-have a better chance at identifying vulnerabilities. Licensees are still learning about the availability of this document. For some, it came out after they had already implemented a program or received an NNSA enhancement at their facilities.

The NRC and NNSA meet routinely at five different levels of management to ensure each Agency is aware of on-going activities. 1) The Radiation Source Protection Task Force (Task Force) is federally mandated to review source protection every 4 years. Fourteen different agencies participate. The Task Force meets semi-annually, and there is more activity in the months leading up to the report deadline. 2) There are tri-lateral meetings with senior management officials from Department of Homeland Security (DHS), NNSA, NRC, and FBI, which meet approximately annually to address source security. 3) The Division Directors for

NRC and Department of Energy (DOE) have quarterly conference calls. 4) The Branch Chiefs for DHS, NNSA, and NRC meet via teleconference quarterly. 5) The Government Coordinating Council Meeting (GCC) is another federally-mandated group that meets. The Director of ORS reports that she is comfortable picking up the phone and coordinates monthly with her counterparts at NRC. A senior staff member at NRC stated that things get done at the Branch level fairly well, however, higher level coordination needs to occur more often to ensure that senior management is aligned and overall agreement occurs. NRC staff report that the relationship is more open now. Chairman Gregory B. Jaczko wrote a letter[15] to The Honorable Byron Dorgan, Chairman of the Subcommittee on Energy and Water Development, Committee on Appropriations, United States Senate, in September 2010 describing the distinct and complementary roles that NRC and NNSA have for source security.

NRC has invited NNSA staff to attend threat assessment meetings in order to stay attuned to the current threat environment. Similarly, NNSA is sharing some of its strategies and OUO documents such as Protection and Sustainability Criteria (2010). NNSA is considering a briefing to share its Potential Adversary Capabilities (PAC) approach-currently undergoing an update-to enhance protection against a defined threat level. NNSA is trying to be consistent with US interagency assessments, avoid redundancies or inconsistencies.

iv. Private Sector Licensees

One licensee stated that if the regulations were more prescriptive, it would accommodate improved consistency in interpretation and application. He stated that he has been challenged as to whether the measures are extensive enough. An Agreement State suggested that a set of requirements could be developed for one type of licensee, for example, industrial radiography. Involving LLEA with determining the level of security needed for the particular facility would be advantageous. He also reported that some LLEA have been troublesome to contact, let alone

work with, and suggested that NRC and the Agreement States should take steps to ensure LLEA involvement. Another licensee stated that NRC should list what is needed for physical security.

One licensee stated that he had a million-dollar NNSA enhancement and would not want prescriptive requirements, especially if it meant going back and changing its security measures. The security system has evolved over time, and they are pleased with the current approach. They appreciated the assistance given by the GTRI team in developing the enhancement plan over a 3-year time period and during implementation in the fourth year. The training for its LLEA at Y-12 in Oak Ridge, Tennessee was lauded, although they did report scheduling difficulties due to the need to have the training close to the installation date of the physical protection system.

A licensee stated that an inspector challenged whether information was protected, although the server for the computer system is properly maintained and secured. The personal computer was secured and password protected. The licensee resolved the protection of information issue by using laptop computers without network access. Another licensee reported a similar issue with a networked computer. They also resolved the issue by dedicating a stand-alone computer.

v. Federal Licensees

Most of the Federal licensees did not identify issues with the performance-based physical security requirements in Subpart C. A majority of the Federal licensees surveyed had accepted NNSA GTRI voluntary enhancement to their physical protection systems. They particularly appreciated the training offered to them and its LLEAs at Y-12, Oak Ridge, Tennessee. Another Federal licensee reported that NNSA is in the process of installing a remote central monitoring system that will enhance its capabilities.

One licensee stated a preference for prescriptive requirements and provided the following text as an example, “the area must have key-card access, monitored 24 hours and motion detectors.” This licensee is also under requirements for biological agents. Another licensee reported that an inspector told him that he had to have a camera although he had other measures in place. A third noted a best practice of including a clock in the field of view of a surveillance camera to provide assurance that the screen shot was not ‘frozen.’

vi. NRC Regional Inspectors

NRC Regional Inspectors did not identify issues with performance-based requirements. One inspector reported that although many licensees complained early in the process, after having worked with performance-based requirements, all now understand what is required and no longer complain. Another noted that no two licensees are the same in implementation, therefore, inspectors are left to interpret whether the licensee meets the intent of the regulation and are in compliance. A third stated that he has not received any requests for more prescriptive regulations. Finally, one inspector noted that licensees would appreciate a checklist from the NRC to ensure that they have covered all the prescriptive requirements that exist in the regulations.

C. Conclusions and Recommendations

Performance-based regulations are effective and incorporate the ability to respond to new technology and threat information. Most licensees are comfortable with the performance-based regulations, although they had concerns about whether they could be challenged on adequacy of measures implemented. Licensees have the responsibility to develop an effective security program by evaluating their operations and selecting strategies, equipment, and procedures. NNSA’s GTRI Program has been a source of best practices for detection enhancements, particularly for the Federal licensees surveyed. The Commission has chosen the performance-

based approach for physical security because it has been shown to be better than prescriptive requirements. In addition, there are a variety of licensee types and operational constraints that make a prescriptive regulatory approach onerous and inefficient.

NRC and Agreement States have the authority and responsibility as the regulator. NNSA offers technology, training for licensees and its LLEA at Y-12, Oak Ridge, Tennessee, and advice for licensees. Since licensees will develop new approaches, and new technologies will be implemented, this information should be collected and shared. For example, one licensee stated that it would have been helpful to have more support in working with LLEA. If another licensee improved its working relationship with its LLEA by attending NNSA training at Y-12, it should have a way to share this information. Offering the NNSA training to licensees who are having difficulties establishing a relationship with its LLEAs should be considered, without the requirement to sign up for an NNSA enhancement. The idea of including a clock in the field of view of a surveillance camera should be available to those licensees who use surveillance cameras. These are unique examples and may not be universally applicable, however, there should be a way to share this information among the regulatory community.

Recommendations:

7. Consider methods to share best practices information such as updating Best Practices (NUREG 2166), disseminating lessons learned periodically with generic information notices, or holding a Regulatory Information Conference.

8. Consider offering NNSA GTRI Y-12 Oak Ridge, Tennessee, training to licensees who are having difficulty establishing a good working relationship with its LLEA, even if they have not accepted an enhanced security system provided by NNSA.

D. Violations Data for Subpart C

i. Scope

This section reviews Violations Data for clarity issues by looking at violations with the potential for Enforcement (Severity Level III) and violations against 'new requirements', as identified from the comparison chart.[12] The term 'Security Zone' is evaluated and the methods of restricting access in 10 CFR 37.47(c) are discussed. Potential clarity issues with weekly verification checks, (37.49(a)(3)(ii)), are raised. Although there were two violations against granting access to security plans or procedures, the details of who was involved, i.e., IT staff, are not known. This issue was not pursued due to lack of information. Implementing Guidance and Best Practices are discussed.

ii. Summary

"New requirements" to Part 37[12], as compared to the IC Orders, comprised 38% of the violations and showed that licensees have difficulties with regard to what should be included in the security plan and security procedures. Violations Data indicate possible clarity issues with security zones and weekly verification checks. Recommendations are made to revise Implementing Guidance to address these clarity issues.

E. Observations

i. Violations Data

Part 37 requires a security plan in comparison to the IC Orders, which required a documented program. Twelve violations were issued against 10 CFR 37.43 Security Plan and eighteen against 37.43(b)(1), Implementing Procedures. Other "new requirements" cited were training or refresher training on the licensee's security program, maintenance, testing and calibration program/records, security program review/results documented, and reporting of events.

The Severity Level III violations in the Violations Data for Subpart C were:

- not protecting security information-three licensees (37.43(d));
- granting access to security plan or procedures before evaluating a need to know and conducting a background investigation-two licensees (37.43(d)(3));
- not establishing the capability to continuously monitor, detect and assess, without delay, all unauthorized entries (37.49);
- not providing alternative means of communication (37.49(c)(2); and
- not having two independent physical controls that form tangible barriers for a mobile device (37.53(a)).

The Violations Data show possible trends in both effectiveness of the new regulation and clarity issues. Seventy percent of NRC's initial 179 inspections against Part 37 resulted in no violations. The conclusions that are being drawn from these data are from 30 percent of licensees that were found in non-compliance. When the Agreement States all implement Part 37 compatible requirements in March 2016, a large group of licensees may be dealing with similar issues.

When a source is used out in the field at a temporary job site or the source is in transport, the security zone may be more difficult to maintain. Five violations were issued against 10 CFR 37.47, Security Zones. Temporary security zones, although not a new concept, are required to be maintained using isolation, direct control, or a combination of isolation and direct control. Security zones must be incorporated into procedures-including use at temporary job sites. See review of NMED events in Section 7.

Five violations were issued against 10 CFR 37.49(a)(3) ii, weekly verification checks. This is not a "new requirement" according to the comparison chart[12]. However, the requirement to

perform a weekly check is apparently “in addition to” the requirement to detect, assess, and respond for Category 2 quantities of radioactive material in storage. Implementing Guidance suggests that if an electronic tamper-indicating device is used, it should be armed at all times, except during maintenance and calibration. NSS-11[2] (p. 37) offers the following explanation for this requirement: “Weekly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include: 1) physical checks that the source is in place; 2) verification of seals or other tamper-evident devices; and 3) measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.”

ii. NRC Regional Inspectors

An NRC inspector related that the most common issue with Part 37 requirements was that licensees failed to understand the specific requirements as they related to a security plan [37.43(a)(1)(i)], security procedures [37.43(b)], and access authorization procedures [Subpart B]. Licensees relied too heavily on the programs they already had in place to comply with the IC Orders, had not significantly revised their procedures and security plans, and underestimated how many new procedures they needed to develop-essentially one for each requirement. An inspector stated that the requirements of 37.43(b), Implementing Procedures, were too vague, as Part 37 includes multiple sections and individual requirements. He suggested requiring each licensee to provide the plans and procedures required by Part 37 for review as part of the licensing process, and to provide license reviewers with guidance as to what is a requirement and what is a “best practice.” Another inspector noted that the concept of a “Security Zone” needed to be established in procedures and the Security Plan. Maintenance and training need to become more formalized and put into procedures. One inspector noted that licensees did not

always perform an explicit review for the access authorization [Subpart B] and security programs [Subpart C].

The requirement for a weekly verification check is subject to different interpretations by licensees. Some licensees thought they already met the requirement with their alarm systems that are set to detect, assess, and respond. Other licensees did not think the sentence construction was clear, i.e., what exactly did 'weekly' apply to? In addition, it is not clear what meets the requirement of a physical check, i.e., is a count of the devices sufficient or should a radiation survey be performed? Including additional background information in the Implementing Guidance, such as the purpose of the weekly verification check and/or using NSS-11 text as appropriate, will enhance understanding of this requirement.

iii. Federal Licensees

Federal licensees noted that implementation of Part 37 required considerable effort and was very time consuming. Minor clarity issues with Part 37 requirements were identified including: spelling out the NRC's expectation that a licensee's internal investigation involving input from the LLEA constitutes required reporting of suspicious activity and whether 37.43(c) requires annual security training for irradiator users. Two non-VA licensees mentioned that they appreciated receiving and revising the Veteran's Administration (VA) National Health Physics Program (NHPP) model procedures for a Security Plan and seven implementing procedures.

iv. Security Zones

The term "security zone" is new for those licensees formerly under ICs. The Comparison Chart[12] (p. 30-31) shows that 'security zone" was in the Orders for Panoramic and Underwater Irradiators and states that IC Orders required the licensee to monitor, detect, assess and respond to unauthorized access. Physical protection of radioactive material by either a "continuous physical barrier" (isolation) or "direct visual surveillance" (access control) or a

combination are the methods specified in 37.47(c). Another new concept is that security zones may be permanent or temporary. The regulations only address “transitory or intermittent business activity.” The regulations do not directly address use at temporary job sites. An Agreement State raised the issue of how to define the security zone in the security plan and procedures for temporary job sites, i.e., does this require constantly amending security plan and procedures? Another Agreement State thought it was a good idea to define the security zone in the plan and procedures for the intermittent business activity of source exchange.

It is often necessary during industrial radiography field work to use multiple individuals to ensure that access is restricted while the source is exposed. The implementing guidance states that an unapproved individual [not permitted unescorted access] may be used, however, an approved individual must monitor the unapproved individual. This raises a potential safety concern if the correct number of approved individuals are not available to restrict access during source exposures.

An area restricted for safety may also be restricted for security. The Implementing Guidance[1] (p 155-156) discusses how a well-logger could use a “restricted area” and an Industrial Radiographer could use a “high radiation area” for the security zone. Industrial radiographers must be vigilant of changes in status from temporary to permanent security zone. When they are operating in a ‘temporary’ security zone and have approved individuals available, it is acceptable to use constant surveillance. When radiographers operate in a ‘permanent’ security zone, i.e., the high-risk source is considered in storage, they must alarm and disable their vehicle. The Implementing Guidance[1] discusses how a truck breakdown could be handled (p 162). Security measures must be applied when the transport vehicle is stopped at a hotel, gas station, or other location, (p. 117).

v. Implementing Guidance (NUREG 2155)

Although physical protection strategies and measures are performance-based, there are many procedures required. New prescriptive requirements in Subpart C are 37.43 Security Plan, 37.43(b) Security Procedures and 37.55 Security Program Review. The Security Plan procedures must address "*37.43, 37.45, 37.47, 37.49, 37.51, 37.53, and 37.55"* or as the Implementing Guidance suggests: training, establishment and maintenance of security zones, monitoring, detection, assessment, and response measures; maintenance and testing measures; the reporting of events; and the periodic review of the program.

The Implementing Guidance includes a checklist of topics for the security plan that is from NSS-11[2]. It is a generic list, (see Appendix A), that each licensee may use to see if all topics are addressed, but no further detailed guidance is available. Based on the number of citations and feedback from the NRC Regional Inspectors, it appears that additional guidance for security plans, procedures, and annual security program review checklists would assist licensees in staying compliant with Part 37 and, thereby, ensuring an effective security program.

vi. Best Practices (NUREG 2166)

NRC Regional inspectors expressed a range of opinions on Best Practices. NUREG 2166 is sufficient, contains useful background information, and may be most helpful to new applicants or for construction of a new room or facility. This was supported by one Federal licensee who stated that it did provide guidance that was useful to the facility design office when a new irradiator room was being constructed. Another inspector cautioned that some of the best practices involve additional expense and should not be proposed to others as the "gold standard." A third inspector noted that there is a continuum of risk mitigation between meeting the regulations all the way to best practices. Just because one licensee develops a new or

different approach, an inspector observed, not all licensees will find it valuable or beneficial. The inspectors reported that they did discuss or provide the Best Practices document to licensees when they were on inspection.

Information sharing between licensees is assumed to occur but not many examples were reported. One inspector gave an example of collaboration among licensees regarding how to do T&R determinations on prestigious faculty who may be from countries that do not have a good relationship with the United States. He was aware of the initial sharing of information between licensees and that it met NRC requirements, but he did not know where or if the best practice was archived. Other inspectors mentioned debriefs of inspections and weekly meetings with Headquarters and other Regions for the Security Information Forum (SIF). Some inspectors referred to regional training and lectures or training with Agreement States. With the exception of the SIF and development of precedence for enforcement, there does not seem to be a good mechanism to share information about trends and best practices.

A Federal licensee suggested that NRC could encourage stakeholder interaction by clarifying how to discuss best practices without violating the 37.43(d) need-to-know regulation. There are specific practices included in the Best Practices Appendices for particular types of licensees. One inspector stated that he would have preferred a better example of the Security Plan and implementing procedures. He thought they should have been separate in the example, (see Appendix A), as they are separate requirements. Finally, he suggested that a self-shielded irradiator license security plan could be a short document that addresses basic information. Best Practices includes suggestions for mobile applications such as industrial radiography and well logging. Constant surveillance must be used when high-risk radioactive materials are “in use” in the field. Licensees will develop new surveillance strategies to maintain the security zone at temporary job sites. New technologies and approaches will be developed regarding alarming the vehicle used in the field. These strategies and technologies should be shared.

Consideration should be given to providing narrative on the problem addressed as well as the solution in order that licensees may determine relevance to their own operational needs.

F. Conclusions and Recommendations

The Violations Data support the issues cited by the NRC inspectors that licensees were not knowledgeable concerning the requirements for the security plan and procedures. Examples of security plans and procedures by license type should be provided in Implementing Guidance. The Violations Data show five violations against Security Zones (37.47). This indicates a possible clarity issue for high-risk sources used in industrial radiography. Four violations were cited against 37.49(a)(3) (ii), weekly verification checks, indicating a possible clarity issue. As one inspector noted that licensees do not always perform an explicit annual review, it is prudent to include a checklist or 'audit' form that could be used to conduct and document the security program review required by 10 CFR 37.55 in Implementing Guidance.

There should be a mechanism developed for information sharing, particularly concerning incidents involving Category 2 mobile use, (Recommendation 6). The remaining Agreement States will implement regulations compatible to Part 37 in March 2016. The NRC experience should be used to provide valuable guidance to the licensees and regulators in Agreement States that are implementing Part 37.

Recommendations:

9. Add model security plans and procedures by license type to Implementing Guidance (NUREG 2155) to assist licensees with required content.

10. Expand discussion on security zones in Implementing Guidance (NUREG 2155) to address surveillance challenges for mobile uses of industrial radiography sources. Include

narrative of problem and solution in order that licensees may determine relevance to operational needs.

11. Include additional background information in the Implementing Guidance (NUREG 2155) such as the purpose of the weekly verification check and/or use NSS-11 text.

12. Include a checklist or 'audit' form that could be used to conduct and document the annual security program review required by 10 CFR 37.55 to Implementing Guidance (NUREG 2155).

13. Share lessons learned from initial Part 37 inspection experience with Agreement States.

7. Subpart D – Physical Protection in Transit

A. Risk for Mobile Sources

i. Scope

The challenges of reducing risk for mobile sources were reviewed by examining NMED[8] data for theft of Category 2 sources. International incidents were reviewed and compared with the events reported in the United States. Review of Category 3 Lost, Abandoned, and Stolen (LAS) events was considered but not pursued, as these were not thefts. NRC, Agreement State staff, and licensees' experience with the License Verification System (LVS) were reviewed.

ii. Summary

Thefts of high-risk radioactive sources under ICs and Part 37 requirements have only occurred for industrial radiography devices in Agreement States. The most recent theft was in 2015. Some of these events involved the truck transporting the device. For the thefts reported in the

United States, human performance error was the root cause. Observations from IAEA's ITDB 2015 Fact Sheet and eight recent thefts reported to the ITDB are discussed.

B. Observations

i. Nuclear Materials Event Database[8] (NMED) Data on Thefts

Six thefts of Category 2 quantities of radioactive material occurred in the time period 2006-2015. All were industrial radiography devices containing Iridium-192 (Ir-192) with a maximum activity of 100 Curies. The licensees were operating under IC requirements that are the same as the Part 37 requirements regarding physical protection. The radioactive material was recovered for five of the six incidents. The sixth incident with the source "not recovered" occurred in 2011. The source has now decayed to an insignificant level and does not present a health and safety or security threat. For the six theft events, three involved theft of the truck containing the high-risk radioactive material. These thefts occurred in public locations: hotel parking lot, gas station, and convenience store. Two incidents involved theft of the device containing high-risk radioactive material: one in front of the business facility and one in a hotel parking lot. The sixth incident was not actually a theft. The radiography device was left in a truck parked at an airport without the capability to immediately detect, assess, and respond to an alarm. The truck's alarm system was set off, however, the radioactive material was not stolen. These events were all due to human performance error versus inadequate physical protection systems.

ii. International Experience

According to the IAEA's ITDB 2015 Fact Sheet[17], the majority of Category 2 industrial sources that are reported stolen or lost are those used for non-destructive testing and for applications in construction and mining. The ITDB is a database currently comprised of 131 countries, and the

data are voluntarily submitted and confirmed by the State [country]. On average it appears that there are 24-40 theft or loss incidents reported each year for all quantities of radioactive material. The isotopes are relatively long-lived Iridium-192, Cesium-137, and Americium-201. In the IAEA Annual Report 2013[18] (p. 67), 146 incidents were reported. Of these, four sources were Category 1-3, and three of the four were thefts.

Appendix I of IAEA NSS-6[9], Statistics on Illicit Trafficking Incidents and Selected Cases, shows 70% of incidents from 1995-2006 involved radioactive material, mostly sealed sources. The report states that about 54% of incidents reported by States, show criminal activity such as theft, illegal possession, and attempts to sell or smuggle. Thefts have involved primarily sealed industrial radioactive sources, e.g., sources used in gauges or radiography devices. Case 5 involved the theft of 9.5 TBq (256 Curies) of five industrial devices in Quininde, Ecuador, in 2002. Three of the five devices were bought back from the thieves.

Los Alamos National Security[7] published a paper in 2007 with the purpose of determining the effectiveness of the research community's ability to trace and trend past radiological diversion from regulatory control. The paper was partly in response to the November 2006 murder of Alexander Litvinenko through the ingestion of Po-210 (polonium-210). Streeper, Lombardi, and Cantrell[7] discovered a total of four murders due to radioactive material from reviewing five different databases. In 2007, they concluded that gamma sources are the most commonly misused radioactive material, especially Cesium-137 and uranium, in all the databases except the Defense Science and Technology (DSTO) database. They noted that the most severe cases of misuse were perpetrated by a person with either direct access to the material or the ability to get a license to obtain material. The authors concluded that direct access to the material makes industrial sources the most vulnerable and desirable targets. They reported that ITDB reported Cesium-137 as the most commonly misused radioisotope through 2005.

For Category 2 quantities of radioactive material, industrial radiography devices containing Ir-192 are subject to the most thefts in the United States and internationally. An NRC staff reviewed and confirmed that seven of eight recent theft incidents reported in ITDB involved industrial radiography devices with Ir-192 sources. The motivation for the thefts is not known for the international incidents, but for the United States incidents, the motivation appears likely to be an attempt to steal something of value and re-sell it. Due to lack of access to the specific details of the incidents in the ITDB, it was not possible to determine whether the regulatory requirements of Part 37 would have prevented the thefts or loss incidents. It is clear that mobile use of industrial radiography devices makes them vulnerable to theft.

iii. NRC's License Verification System (LVS)

The NRC confirmed that the LVS was deployed (license files uploaded from Web Based Licensing (WBL)) in May 2013. The NRC licensees began using LVS in March 2014. As most of the manufacturing licensees are in Agreement States, use has been limited. This will change in March 2016 when all the Agreement States must enforce Part 37 requirements. LVS is convenient for a shipper to verify that the recipient of a radioactive source is authorized because LVS tracks the verification. Once the license is pulled up, the shipper reviews it to confirm that the recipient is authorized to receive the source. A licensee can also submit a Form 749 to the Help Desk and receive assistance with the verification. The NRC decided that it would be easier for the Help Desk to maintain the list of Agreement State contacts and coordinate with them. To date, the Help Desk assisted 11 licensees in 2014 and 10 licensees in 2015. They have also handled other issues such as access, user accounts, and status of user accounts, since it is a multi-step process. The Help Desk handled 173 user requests in 2014 and 94 user requests in 2015. Federal licensees who used LVS reported no difficulties. Two private sector licensees noted that you must have knowledge of the current amendment number, or you get an

error message and have to contact the Help Desk or Agreement State. NRC Regional inspectors reported that LVS was user-friendly. One inspector noted that he uses WBL to check for license amendment requests that have not yet been entered into ADAMS. Use of LVS should be evaluated once the Agreement State licensees have begun to use it.

C. Conclusions and Recommendations

Temporary security zones in the field are more difficult to manage. The industrial radiographer has to maintain constant surveillance, even when the source is locked up in truck at the field location. In this situation, the source is considered “in use.” When the radiographer leaves the truck unattended, such as spending the night in a hotel room, the source is considered “in storage,” and the vehicle must be alarmed and disabled. Lessons learned from theft events, corrective actions and follow-up for sustainability of the corrective actions need to be shared. The regulators and licensees must work together to minimize, to the extent practicable, human performance errors. Industrial radiography devices containing Ir-192 are subject to the most thefts in the United States and internationally. LVS has primarily been used by NRC licensees. Once the Agreement States enforce Part 37 requirements, review LVS use for any difficulties.

Recommendations:

14. Make on-going lessons learned from theft incidents, particularly Category 2 industrial radiography sources, available to licensees and regulators. Emphasize corrective actions that have proven successful at reducing human performance errors.

15. Evaluate LVS once the Agreement State licensees have used it for 6 months.

8. Conclusion and Summary of Recommendations

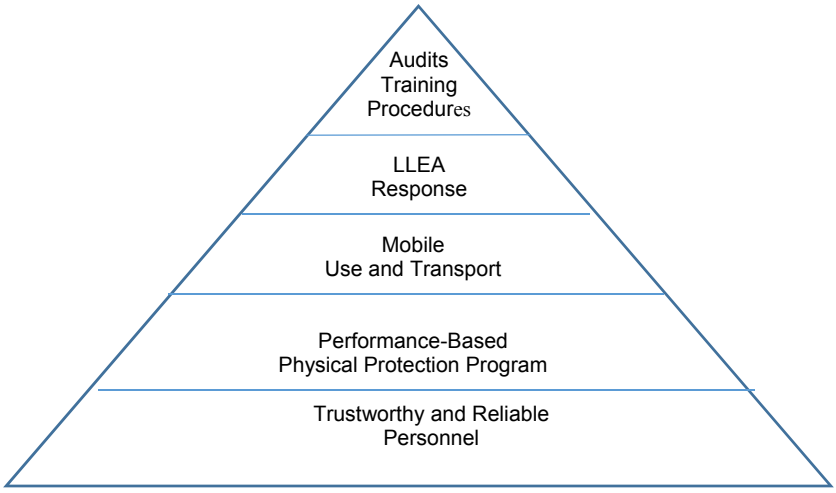

Figure 2: Part 37 Defense-in-Depth

Part 37 is effective in preventing malevolent use of radioactive material. NRC has chosen a risk-informed performance-based security program requirement based on research and experience. A defense-in-depth approach is used, Figure 2, in order that "the failure to meet a performance criterion, while undesirable, will not constitute or result in an immediate safety concern."

This conclusion is based on 22 months of experience under Part 37 by NRC licensees. It is a snapshot-in-time and is biased toward fixed facilities and large companies. Inspections were conducted for 179 NRC licensees. This represents 13% of the total number of licensees based on a total of 1400 licensees[11] (p. 5) in NRC and Agreement States. NRC Regional inspectors and Agreement States shared their experience and relayed concerns of licensees. Federal licensees and private sector licensees provided feedback. NRC staff provided information about development and implementation of Part 37 and guidance.

This report assesses the clarity of the regulations and guidance as part of an assessment of the effectiveness of Part 37 requirements. According to Best Practices, *"An effective physical*

protection program integrates people, procedures, and physical security technology to protect the facility and assets (e.g., category 1 or category 2 quantities of radioactive material) from theft, diversion, sabotage, or other malevolent attacks," (p. 2-1). There have been no reports of an individual with malevolent intent obtaining or attempting to obtain Category 1 or 2 quantities of material. The major source of information for possible effectiveness issues has been Violations Data. Compliance results from the Violations Data show that 30% of licensees had violations. Some of these may be clarity issues. Recommendations are included for revisions to Implementing Guidance and Best Practices.

Issues raised by GAO in the most recent two reports were reviewed and evaluated. "Aggregated" is understood by the affected licensees, i.e., well loggers. Additional measures are taken by licensees over and above the safety measures of 10 CFR Part 20.1801 and 1802. Trustworthiness and reliability determinations are performance-based requirements. This results in case-by-case determinations. Reviews are subjective. The NRC will conduct a one-year review to determine whether specific criteria are used by licensees, and if there are particular difficulties that need to be addressed. GAO characterized the NNSA GTRI enhancements as prescriptive, and NNSA confirmed that they have a Tool Box of pre-approved technology. For those licensees who accepted GTRI enhancements, the actual result is a blend of prescriptive and performance-based according to NNSA. Pool irradiators and industrial radiography licensees are not able to integrate NNSA's set approach into their operations. Flexibility permits the licensee and NNSA GTRI to accommodate the licensee's needs on an individual basis. NNSA staff need to understand the operations of other types of licensees, beyond irradiator and gamma-knife, for the next generation of enhancements.

The theft incidents for Category 2 quantities of radioactive material reported in NMED involved six Category 2 radioactive sources. Thefts are the closest analogy for malevolent intent. These failures were human performance errors versus a lack of physical protection measures. Thefts

of Category 2 industrial radiography sources show that the responsibility for safety *and* security resides with the radiography crew. Procedures, training, and audits are the management tools available to the licensee.

It was difficult to obtain information for this clarity review as the consultants had to be cautious about discussing security measures. Information that was OUO had to be redacted or summarized for the Independent Assessment Consultants. A recommendation (16) is included for data that the NRC's 10 CFR Part 37 Program Review Team (PRT) should review that was not available due to being OUO information.

The information available internationally was limited. In addition, the international ITDB database is voluntary and not standardized. This is in contrast to the excellent data available in NMED that is required to be submitted by the regulators and is standardized.

The opportunity to share safety practices has long been a hallmark of the radiation safety community. Both regulators and licensees exchange good health and safety practices. The ability to share security best practices is restricted as security of information is an issue. A method needs to be developed to share the information that may be useful in a general manner without identifying a specific licensee.

Summary of Recommendations:

1. Revise the Best Practices document (NUREG 2166) to clarify the circumstances when aggregation does not require implementation of Part 37 regulations. A suggested revision is: "the licensee must implement *access control, constant surveillance or a combination of both* if a physical barrier, which has been installed to isolate the remaining aggregated gauges from other gauges, is breached *temporarily under exceptional circumstances or for a limited period of time* (e.g., during a source exchange or gauge removal)."

2. Add text to the Implementing Guidance (NUREG 2155) clarifying that the purpose of the T&R determination is essentially to determine if someone is trustworthy by assessing his or her truthfulness.
3. Add to Best Practices (NUREG 2166) that an industry, such as industrial radiography, develop an information sharing database of individuals approved and denied unescorted access similar to sharing of information in PADS for NPPs.
4. Review the results of Temporary Instruction 2800/042[11] for examples of the licensee's basis for making a negative T&R determination. Identify whether the basis is subjective, i.e., an evaluation of truthfulness, or specific criminal offenses. Use this information to develop additional guidance.
5. Add detailed information of content needed for access authorization program procedures required by 10 CFR 37.23(f) to Implementing Guidance (NUREG 2155).
6. Include a checklist or 'audit' form that could be used to conduct and more uniformly document the annual unescorted access program review required by 10 CFR 37.33(a) to Implementing Guidance (NUREG 2155).
7. Consider methods to share best practices information such as updating Best Practices (NUREG 2166), disseminating lessons learned periodically with generic information notices or holding a Regulatory Information Conference.
8. Consider offering NNSA GTRI Y-12 Oak Ridge, Tennessee, training to licensees who are having difficulty establishing a good working relationship with its LLEA, even if they have not accepted an enhanced security system provided by NNSA.
9. Add model security plans and procedures by license type to Implementing Guidance (NUREG 2155) to assist licensees with required content.
10. Expand discussion on security zones in Implementing Guidance (NUREG 2155) to address surveillance challenges for mobile uses of industrial radiography sources.

Include narrative of problem and solution in order that licensees may determine relevance to operational needs.

11. Include additional background information in the Implementing Guidance (NUREG 2155) such as the purpose of the weekly verification check and/or use NSS-11 text.
12. Include a checklist or 'audit' form that could be used to conduct and document the annual security program review required by 10 CFR 37.55 to Implementing Guidance (NUREG 2155).
13. Share lessons learned from initial Part 37 inspection experience with Agreement States.
14. Make on-going lessons learned from theft incidents, particularly Category 2 industrial radiography sources, available to licensees and regulators. Emphasize corrective actions that have proven successful at reducing human performance errors.
15. Evaluate LVS once the Agreement State licensees have used it for 6 months.
16. The NRC's PRT should review and evaluate:
    - selection of theft reports of from the ITDB, looking particularly at Category 1 or 2 quantities of radioactive material;
    - inspection reports for inspections with Severity Level III violations-determine root causes;
    - inspection reports from Agreement States with theft incidents of Category 2 industrial radiography sources;
    - results of follow-up interview with Agreement State staff regarding effectiveness of corrective actions for Category 2 theft events;
    - the Suspicious Incidents Database; and
    - results of the surveys received from Agreement States.

9. References

[1] U.S.NRC NUREG 2155, Rev. 1, Implementation Guidance for 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," Date Published: January 2015

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

[3] U.S.NRC NUREG 2166, "Physical Security Best Practices for the Protection of Risk-Significant Quantities," Date Published: May 2014

[4] GAO 12-925 Report Nuclear Proliferation "Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities," dated September 2012

[5] GAO -14-293, Report Nuclear Proliferation, "Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources," dated June 2014.

[6] NRC Training Course S-201, NRC Materials Control, Security Systems, and Principles.

[7] LA-UR 07-3686 Diversions of radioactive material and the difficulties in case tracking, Charles Streeper, Marcie Lombardi and Dr. Lee Cantrell, Los Alamos Security and California Poison Control System, San Diego Division (2007) http://osrp.lanl.gov/Documents/LAUR-07-3686.pdf

[8] NMSS Data Analysis Task Force for LAS Events Involving Category 1 or 2 Sources, Draft LAS Events Involving Category 1 and 2 Sources FY 2006-2015, November 6, 2015

[9]IAEA NSS No, 6, Technical Guidance Reference Manual, Combatting Illicit Trafficking in Nuclear and Other Radioactive Material, Appendix I (p. 126-125), 2012

[10]NRC Inspection Manual, Inspection Procedure 87137, 10 CFR Part 37 Materials Security Programs, FMSE/NSIR, http://pbadupws.nrc.gov/docs/ML1403/ML14030A144.pdf

[11]Federal Register-Final 10 CFR Part 37 Rule, Vol. 78, No. 53, Tuesday, March 19, 2013, p. 16922-17022 https://www.gpo.gov/fdsys/pkg/FR-2013-03-19/pdf/2013-05895.pdf

[12] NRC Rule-Comparison Chart http://pbadupws.nrc.gov/docs/ML1132/ML113290229.pdf

[13]Staff Requirements-SECY-98-144-White Paper on Risk-Informed and Performance Based Regulation, dated March 1, 1999 http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1998/secy1998-144/1998-144scy.pdf

[14]NRC Inspection Manual, Temporary Instruction 2800/042, Issue Date: 11/25/15 http://pbadupws.nrc.gov/docs/ML1526/ML15266A314.pdf

[15] Letter from Chairman Gregory B. Jaczko to The Honorable Byron Dorgan, Chairman, Subcommittee on Energy and Water Development, Committee on Appropriations, United States Senate dated September 14, 2010. http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2010/dorgan-09-14-2010.pdf

[16]Federal Register-10 CFR Parts 50, 52, 72 and73, Power Reactor Security Requirements Final Rule, Vol. 74, No. 58/Friday, March 27, 2009/Rules and Regulations https://www.gpo.gov/fdsys/pkg/FR-2009-03-27/pdf/E9-6102.pdf

[17] IAEA Incident and Trafficking Database (ITDB) Incidents of Nuclear and Other Radioactive Material Out of Regulatory Control, 2015 Fact Sheet, http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf

[18] IAEA Annual Report 2013 https://www.iaea.org/publications/reports/annual-report-2013-0

[19] Global Threat Reduction Initiative, Nuclear and Radiological Material Protection, NNSA Fact Sheet

10. Acknowledgements

The author gratefully acknowledges the observations, insights, and effort of the following individuals who contributed to this report.

NRC NMSS: Michelle Burgess, Margaret Cervera, Carrie Crawford, Lisa Dimmick, Adelaide Giantelli, Paul Goldberg, Ernesto Quinones, Angela Randall, Michelle Smethers, George Smith, Irene Wu

NRC NSIR: Gary Purdy, Mark Resner, Sandra Wastler-retired, Duane White, Vince Williams

NRC OGC: Angela Coggins

NRC Operations: Alonzo Richardson

NNSA: Maegon Barlow, Nicholas Butler, Wendy Friedt, and Greg Herdes

Licensees-Private Sector: Chris Dixon - Acuren; Mark Driscoll & Joe Micklos - University of Michigan; John. J. Miller - International Isotopes; Shashadhar Mohapatra, Ph.D. DABR, DABSNM - MedStar Washington Hospital Center**,** Peter Reinhardt & Kevin Charbonneau – Yale University; Phil Simpkin - Baker Hughes; David Tebo - Team Industrial Inc.; Jon Young - Steris Isomedix.

Licensees-Federal: Craig Adams – VA; Kimberly D. Alston – USUHS; Agnes Barlow – VA; Dr. Ramachandra K. Bhat – USAF; Dave Derenzo – VA; Josephine Esteban-Trexler – Military – Army; Bill Fitzgerald – NIH; Walter Furr – VA; Albert LaGroue – VA; Richard Lamoreaux - Military; Cathy Ribaudo – NIH; Wendy Rubin – NIH; Shannon P. Voss – VA; Shen Zhu-Military

NRC Regional Inspectors: James Cassata (I), Jason Dykert (IV), Robert Gallagher (I), Janine Katanic, Ph.D., CHP (IV), Michael LaFranzo (III), John Miller (I), Rick Munoz-retired (IV),

Deborah Piskura (III), Randolph C. Ragland, Jr. (I), Shawn Seeley (I), Jason vonEhr (IV), Scott Wilson (I)

Agreement States: Travis Cartoski-Georgia, Curt Demaris, Craig Lawrence & Earl Fordham-Washington, Randall S. Dublin - Iowa; Sherrie Flaherty & Brandon Juran – Minnesota; Stephen James – Ohio; Eric Skotak – Texas; Mike Broderick & Kevin Sampson - Oklahoma

NRC's Program Review Team: George Smith-Team Leader; Kim Lukes, Ernesto Quinones, Paul Goldberg, William Lee, Juan Peralta, John Adams, Vince Williams, Robert Gattone, Magaret Cervera, Michelle Smethers; Angela Coggins - Legal Support, Carrie Crawford - Administrative Support; Linda Eusebio – Administrative Support.

NRC Working Groups: Two main working groups have been involved with the development and implementation of Part 37. Four groups worked on development of the Part 37 regulation from 2008 through publication of the Final Rule on March 19, 2013. Next, the Implementation of Part 37 Working Group continued with 12 sub-groups. Many of the individuals interviewed or surveyed for this report were on these sub-groups, including Inspection Procedure, Implementing Guidance and Best Practices. The work is on-going, for example, updating Enforcement Guidance.

11. Appendix A-Cross Reference Table of Regulations/Guidance to Recommendations

Subpart	Part 37 Requirement, Implementing Guidance or Best Practice Reference	Action
A	*§37.5 Definition: "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."*	Not an Issue
A	Implementing Guidance[1], *p. 10* *"…a category 2 or greater quantity is considered "aggregated" only if it is located within an area isolated by a single barrier. The licensee may use or store material with radioactivity in category 2 quantities at several locations. This material would not be considered aggregated as long as access to each location is controlled by at least one physical barrier."*	
A	Implementing Guidance[1], *p 114, A2* *"Aggregated has the same meaning as "collocated" in the guidance for the IC orders. The regulations in 10 CFR 37 use the term 'aggregated' instead of 'collocated' to avoid the confusion that could arise when several separate non-aggregated quantities of radioactive material are located at the same site or inside the same facility."*	
A	*Best Practices Guidance[3], Physical Security Practices for Fixed Gauges, p D-3,* *"In addition, the licensee must implement the requirements in 10 CFR 37 if a physical barrier, which has been installed to isolate the remaining aggregated gauges from other gauges, is breached (e.g., during a source exchange or gauge removal), and the total aggregated quantity of radioactive material is equal to, or greater than, the Category 2 limits in 10 CFR Part 37."*	Rec 1
B	*§37.23(b): "<u>Reviewing officials are the only individuals who may make trustworthiness and reliability determinations</u> [emphasis added] that allow individuals to have unescorted access to category 1 or 2 quantities of radioactive material."*	Not an Issue
B	*§37.23(e)(1) Determination Basis "The reviewing official shall determine whether to permit, deny, unfavorably terminate, maintain, or administratively withdraw an individual's unescorted access authorization <u>based on an evaluation of all of the information collected</u> [emphasis added] to meet the requirements of this subpart."*	

B	*§37.23(e)(4): "The reviewing official may terminate or administratively withdraw an individual's unescorted access authorization <u>based on information obtained after the background investigation has been completed</u> [emphasis added] and the individual granted unescorted access authorization."*	Not an Issue
B	*§*37.23(f) "*Procedures. Licensees <u>shall develop, implement, and maintain written procedures for implementing the access authorization program</u> [emphasis added] The procedures must include provisions for the notification of individuals who are denied unescorted access. The procedures must include provisions for the review, at the request of the affected individual, of a denial or termination of unescorted access authorization. The procedures must contain a provision to ensure that the individual is informed of the grounds for the denial or termination of unescorted access authorization and allow the individual an opportunity to provide additional relevant information.''*	Rec 5
B	*§37.25 (a) "Initial investigation. Before allowing an individual unescorted access to category 1 or category 2 quantities of radioactive material or to the devices that contain the material, licensees shall complete a background investigation of the individual seeking unescorted access authorization. The scope of the investigation must <u>encompass at least the 7 years preceding the date of the background investigation</u> [emphasis added] or since the individual's eighteenth birthday, whichever is shorter. The background investigation must include at a minimum:* *(1) Fingerprinting and an FBI identification and criminal history records check in accordance with § 37.27;* *(2) Verification of true identity. Licensees shall verify the true identity of the individual who is applying for unescorted access authorization to ensure that the applicant is who he or she claims to be. A licensee shall review official identification documents (e.g., driver's license; passport; government identification; certificate of birth issued by the state, province, or country of birth [deleted text]* *(3) Employment history verification. Licensees shall complete an employment history verification, including military history. Licensees shall verify the individual's employment with each previous employer for the most recent 7 years before the date of application;* *(4) Verification of education. Licensees shall verify that the individual participated in the education process during the claimed period;* *(5) Character and reputation determination. Licensees shall complete reference checks to determine the character and reputation of the*	

	individual who has applied for unescorted access authorization [deleted text] *(6) The licensee shall also, to the extent possible, obtain independent information to corroborate that provided by the individual (e.g., seek references not supplied by the individual);"*	
B	*§37.33(a) "Each licensee shall be responsible for the continuing effectiveness of the access authorization program. Each licensee shall ensure that access authorization programs are reviewed to confirm compliance with the requirements of this subpart and that comprehensive actions are taken to correct any noncompliance that is identified. The review program shall evaluate all program performance objectives and requirements. <u>Each licensee shall periodically (at least annually) review the access program</u> [emphasis added] content and implementation."*	Rec 6
	Implementing Guidance[1], p. 40, "Q2: How can I protect against an insider threat? *A2: The regulations in 10 CFR Part 37 require licensees to limit unescorted access to category 1 or category 2 quantities of radioactive material to approved individuals. Under 10 CFR 37.25 and 10 CFR 37.27, a background investigation that includes fingerprinting and a Federal Bureau of Investigation (FBI) criminal history records check must determine if an approved individual is trustworthy and reliable. In addition, under 10 CFR 37.43(c), the licensee must provide training to its staff. This training should, among other things, enhance its employees' and contractors' awareness of the requirements in 10 CFR 37.57(b) and 10 CFR 37.81(c) to assess and report, as appropriate, "any suspicious activity related to possible theft, sabotage, or diversion" of category 1 or category 2 quantities of radioactive material. Such activity could include unusual or suspicious behavior by employees or contractor employees with routine access to areas of the site or equipment related to the control of access to a security zone."*	
B	*Implementing Guidance[1], p. 57-58,* *"Q4: What criteria do I use to determine trustworthy and reliability?* *A4: The NRC has not developed a set of criteria for determining T&R because no such list is likely to cover all licensees' needs, and each licensee is in the best position to weigh the many considerations that must support such determinations. Therefore, the licensee is responsible for making T&R determinations for all employees granted unescorted access. The background investigations under 10 CFR 37.25 are designed to identify past actions that might call into question an individual's T&R. Annex A lists some indicators that licensees should consider as potential*	Rec 2 & 4

	concerns. Although the licensee should review this annex in its entirety, the following indicators are provided for convenience: *• impaired performance attributable to psychological or other disorders* *• conduct that warrants referral for criminal investigation or that results in an arrest or a conviction* *• indication of deceitful or delinquent behavior* *• attempted or threatened destruction of property or life* *• suicidal tendencies or attempted suicide* *• illegal drug use or the abuse of legal drugs* *• alcohol abuse disorders* *• recurring financial irresponsibility* *• irresponsibility in the performance of assigned duties* *• inability to deal with stress or the appearance of being under unusual stress* *• failure to comply with work directives* *• hostility or aggression toward fellow workers or authority* *• uncontrolled anger, violation of safety or security procedures, or repeated absenteeism* *• significant behavioral changes, moodiness, or depression* *However, these indicators are neither meant to be all inclusive nor intended to be disqualifying factors. Licensees also may consider extenuating or mitigating factors in their determinations."* *Annex A, p. 108* *The purpose of the T&R determination requirement is to provide reasonable assurance that those individuals are trustworthy and reliable and do not constitute an unreasonable risk to the public health and safety, including the potential to commit or aid theft or radiological sabotage. In evaluating the relevance of an individual's conduct, the* *RO should consider the following factors:* *• the nature, extent, and seriousness of the conduct*	

	• the circumstances surrounding the conduct, including evidence as to if it was deliberate *• the frequency and recency [sic] of the conduct* *• the individual's age and maturity at the time of the conduct* *• the extent to which participation in the conduct was voluntary* *• the presence or absence of rehabilitation and other permanent behavioral changes* *• the motivation for the conduct* *• the potential for pressure, coercion, exploitation, or duress as a result of the conduct* *• the likelihood of continuation or recurrence* *Each case must be judged on its own merits, and the final determination remains the responsibility of the licensee."* *"Q7: How should the T&R determination for my employees be documented?* *"[deleted text] The elements that the licensee is required to consider in making its determination appear in 10 CFR 37.25. Because the basis for the licensee's determination is also the result of a process, a good documentation practice would include the criteria, procedures and records that the licensee used to support the determination."*	
B	*Implementing Guidance[1], p. 59,* *"Q9: If I've determined someone to be trustworthy and reliable, and that individual later takes the material for malevolent use, what actions are expected of me? <u>What liability do I assume because of my T&R determination</u>? [emphasis added]* *A9: <u>If nothing in the background investigation caused a licensee to deny access and if the licensee did everything that was required, it would not be in violation</u> [emphasis added] of the access authorization requirements. <u>The licensee must provide reasonable assurance that persons granted access are trustworthy and reliable</u> [emphasis added]. If the licensee fails to provide that assurance, it will be in violation of the 10 CFR Part 37 requirements, and the NRC will consider enforcement action. However, providing assurance means that the licensee has made a reasonable effort, as required by 10 CFR Part 37, to ascertain T&R and has documented its actions. <u>As long as the licensee can show that it has made</u>*	

	a reasonable good-faith effort, the NRC will not second-guess its decision. (emphasis added) *[deleted text] the NRC does not consider a denial of unescorted access authorization to be a denial of employment. The applicant may still work in areas of the facility outside the security zones or may perform escorted work within the facility."*	
B	*Implementing Guidance[1], p.66* *"A T & R determination provides the licensee's decision with reasonable assurance [emphasis added] that the individual allowed unescorted access will not use the material for malicious purposes."*	
B	*Implementing Guidance[1], p. 68* *"[deleted text] the information obtained from employment history and other background checks may vary widely and because licensees may not be able to obtain sufficient information [emphasis added] to determine compliance with all criteria, the licensee may not be able to avoid having to apply its subjective judgement about an applicant."*	
B	*Best Practices[3], p 2-1* *"Therefore, the management of the organization must provide the requisite authority, leadership, support, and resources to the physical protection program."*	
B	*Best Practices[3], p 3-4,* *"When evaluating the relevance of an individual's conduct, the licensee should consider the following factors: nature, extent and seriousness of the conduct, circumstances surrounding the conduct, including evidence indicating whether it was deliberate, frequency and timing of the conduct (e.g., did it take place recently), individual's age and maturity at the time of the conduct, extent to which the individual's participation was voluntary, presence of absence of rehabilitation and other permanent behavioral changes, motivation for the conduct, potential for pressure, coercion, exploitation, or duress as a result of the conduct, likelihood of continuation or recurrence of the conduct"*	
B	*Best Practices, Appendix A, Developing a Security Plan, p. A-7* *"3.3 Access Authorization* *This section should describe the process necessary for authorizing personnel who need unescorted access to the risk-significant radioactive*	Rec 2 & 5

	material location or secured areas, or both, and access to security-sensitive information to perform their duties (which may or may not be directly related to security). The description should ensure that the process does the following: *• Identifies the positions that require unescorted access.* *• Verifies that the individuals who hold the positions are trustworthy and reliable* *(Section 3.4).* *• Verifies that the individuals who hold the positions have the necessary qualifications and training (Section 3.2).* *• Maintains up-to-date records of personnel approved for unescorted access.* *• Withdraws access authorization when personnel no longer have a need for unescorted access, such as transfer of job responsibilities or termination of employment.* *3.4 Trustworthiness and Reliability* *This section should describe the process for evaluating the trustworthiness and reliability of personnel to determine whether they should be granted unescorted access to nuclear and radiological materials, secured areas, or security-sensitive information. The management process or procedure for evaluating the trustworthiness and reliability of personnel should also indicate requirements for periodic review and any reevaluation for particular circumstances. The description should clearly do the following:* *• Identify the individuals or job descriptions whose trustworthiness must be evaluated* *• Identify the applicable requirements regarding trustworthiness and reliability in regulations for the security of risk-significant radioactive materials, license conditions, or elsewhere, including any requirements that vary depending on other factors.* *• State what records must be maintained and kept confidential as part of the trustworthiness and reliability evaluation."*	
C	*§37.41 Security Program* *37.41(a)(1)*	Rec 9

	"Each licensee that possesses an aggregated category 1 or category 2 quantity of radioactive material shall establish, implement, and maintain a security program (emphasis added) in accordance with the requirements of this subpart." *37.41(b) General Performance Objective:* *"Each licensee shall establish, implement, and maintain a security program (emphasis added) that is designed to monitor, and, without delay, detect, assess, and respond [emphasis added] to an actual or attempted unauthorized access to category 1 or 2 quantities of radioactive material."*	
C	*Implementing Guidance[1], p. 122* *"Security plans are important for the implementation of a performance-based regulation. An adequate plan requires a licensee to analyze the particular security needs of its individual facilities [emphasis added] and to explain clearly how it will implement its chosen security measures [emphasis added] to ensure that they work together to meet the applicable performance objectives."*	
C	*Best Practices[3], p. 2-1* *"Licensees are also encouraged to talk to stakeholders (e.g., other licensees, organizations, or businesses) with knowledge, experience, and expertise [emphasis added] in developing a physical protection program. In addition, licensees should coordinate, to the extent practical, with the responding local law enforcement agency (LLEA) to achieve a comprehensive understanding of the facility and its response needs."*	Recs 3, 4, 7, 8, 13, 14 & 16
C	*§37.41(c)* *Program features. Each licensee's security program must include the program features, as appropriate, described in §§ 37.43, 37.45, 37.47, 37.49, 37.51, 37.53, and 37.55.*	Rec 9
C	*§37.43(a) Security Plan* *§37.43(a)(1)(i)* *"Each licensee identified in §37.41(a) shall develop a written security plan (emphasis added) specific to its facilities and operations. The purpose of the security plan is to establish to licensee's overall security strategy to*	Rec 9

	ensure the integrated and effective functioning of the security program required by this subpart."	
C	*§37.43(b)* *"Implementing procedures. (1) The licensee shall develop and maintain written procedures that document how the requirements of this subpart and the security plan will be met [emphasis added]"*	Rec 9
C	*§37.47 Security Zones* *(a) Licensees shall ensure that all aggregated category 1 and category 2 quantities of radioactive material are used or stored within licensee established security zones (emphasis added). Security zones may be permanent or temporary (emphasis added).* *(b) Temporary security zones must be established as necessary to meet the licensee's transitory or intermittent business activities (emphasis added), such as periods of maintenance, source delivery, and source replacement.* *(c) Security zones must, at a minimum, allow unescorted access only to approved individuals through:* *(1) Isolation (emphasis added) of category 1 and category 2 quantities of radioactive materials by the use of continuous physical barriers (emphasis added) that allow access to the security zone only through established access control points (emphasis added). A physical barrier is a natural or man-made structure or formation sufficient for the isolation of the category 1 or category 2 quantities of radioactive material within a security zone; or* *(2) Direct control (emphasis added) of the security zone by approved individuals at all times; or* *(3) A combination of continuous physical barriers and direct control [emphasis added].*	Rec 9 & 10
C	*§37.49 Monitoring, Detection, and Assessment* *(a) Monitoring and detection. (1) Licensees shall establish and maintain the capability to continuously monitor and detect without delay all unauthorized entries into its security zones [emphasis added]. Licensees shall provide the means to maintain continuous monitoring and detection capability in the event of a loss of the primary power source, or provide for an alarm and response in the event of a loss of this capability to continuously monitor and detect unauthorized entries [deleted text]*	Rec 10 & 11

	(3)(ii) For category 2 quantities of radioactive material, weekly verification [emphasis added] through physical checks, tamper indicating devices, use, or other means to ensure that the radioactive material is present.	
C	*§ 37.55 Security program review.* *(a) Each licensee shall be responsible for the continuing effectiveness of the security program. Each licensee shall ensure that the security program is reviewed to confirm compliance with the requirements of this subpart and that comprehensive actions are taken to correct any noncompliance that is identified. The review must include the radioactive material security program content and implementation. Each licensee shall periodically (at least annually) review the security program content and implementation [emphasis added]* *(b) The results of the review, along with any recommendations, must be documented.*	Rec 12
C	*Implementing Guidance[1], p. 123-124 Contents of Security Plan* *• a description of the radioactive material, its categorization, and its use* *• a description of the environment, building, and facility in which the radioactive material is used or stored and, if appropriate, a diagram of the facility layout and security system* *• the location of the building or facility relative to areas accessible to the public* *• local security procedures* *• objectives of the security plan for the specific building or facility, including the following:* *– the specific concern that will be addressed (e.g., unauthorized removal, destruction, or malevolent use)* *– the kind of control necessary to prevent undesired consequences, including the auxiliary equipment that might be needed*	Rec 9

	– the equipment or premises that will be secured *• security measures that will be used, including the following:* *– the measures to secure, provide surveillance, provide access control, detect, delay, respond, and communicate* *– the design features to evaluate the quality of the measures against the assumed threat* *• administrative measures that will be used, including the following:* *– security roles and responsibilities of management, staff, and others* *– routine and non-routine operations, including an accounting of the source(s)* *– maintenance and testing of equipment* *– a determination of the trustworthiness of personnel* *– the application of information security* *– methods for access authorization* *– security related aspects of the emergency plan, including event reporting* *– training* *– key control procedures* *– procedures to address an increased threat level* *– the process for periodically evaluating the effectiveness of the plan and updating it accordingly* *– any compensatory measures that may need to be used* *– references to existing regulations or standards*	
C	*Implementing Guidance[1], p. 130* *Generally, the security procedures must address how the licensee will implement the applicable features required by Subpart C. Depending on the licensee and its operating requirements, these features <u>would require its procedures (1) to address training, (2) to establish and maintain security zones, and (3) to establish the monitoring, detection, assessment, and</u>*	Rec 9

	response measures; maintenance and testing measures; the reporting of events; and the periodic review of the program. [emphasis added]	
C	*Implementing Guidance[1], p. 158* *"The rule does not prevent the licensee from using an unapproved individual to provide additional continuous direct surveillance, however, the regulation in 10 CFR 37.47(c)(2) does not allow the licensee to rely on any individual who has not been approved for unescorted access to be a monitor of access to a temporary [emphasis added] or permanent security zone [emphasis added] unless an approved individual monitors the unapproved individual."*	Rec 10
C	*Implementing Guidance[1], p. 175* *If a licensee with a category 2 quantity of radioactive material does not use the material weekly or make weekly physical checks to verify its continuing presence, [emphasis added], what "other means" may this licensee use to detect the removal of a category 2 quantity of radioactive material under 10 CFR 37.49(a)(3)(ii)? [emphasis added]* *The intent of the provision for "other means" to detect the removal of a category 2 quantity of material is to give the licensee flexibility to use the method that works best for its facility. Although electronic sensors for detecting the removal of a category 2 quantity of material are not required, [emphasis added], the licensee should consider, as good practice, the application of these devices to category 2 quantities, where feasible, for immediate detection capability. For additional technical guidance on the capabilities and applications of different intrusion detection system technologies, the licensee may refer to NUREG-1959 or NUREG-2166.* *If a licensee decides to use an electronic, tamper-indicating device for detecting the removal of a category 2 quantity of material, the NRC recommends that the system be designed to silently or audibly alarm on any attempt to remove a device or a source from its device. The licensee should arm the tamper-indicating alarm at all times, [emphasis added], other than those for equipment maintenance or calibration. The licensee's security plan should also explain how any method used to detect the unauthorized removal of a category 2 quantity of material will be reliable and effective in meeting the requirements in 10 CFR 37.49(a)(3).*	Rec 11
C	*Best Practices[3], Section 2.1, Determining the Objectives of the Physical Protection Program:* *"An effective physical protection program integrates people, procedures, and physical security technology to protect the facility and assets (e.g.,*	

	category 1 or category 2 quantities of radioactive material) from theft, diversion, sabotage, or other malevolent attacks."	
C	*Best Practices[3], Appendix A, Developing a Physical Security Plan, Resources Equipment and Technology, p. A-11:* *"This section [of the plan] should describe how the current security system is designed and implemented. It should follow the standard practice of identifying the specific target(s) (radioactive sources)) under protection, identifying and assessing the threats against which the facility is being protected, describing the security assessment methodology, and providing information on how the design of the security system achieves sufficient protection by using a graded approach and by employing the principles of defense in depth and balanced protection."*	Rec 9
D	*§37.71 Additional requirements for transfer of category 1 and category 2 quantities of radioactive material. A licensee transferring a category 1 or category 2 quantity of radioactive material to a licensee of the Commission or an Agreement State shall meet the license verification provisions listed below instead of those listed in § 30.41(d) of this chapter:* *(a) Any licensee transferring category 1 quantities of radioactive material to a licensee of the Commission or an Agreement State, prior to conducting such transfer, shall verify with the NRC's license verification system [emphasis added] or the license issuing authority that the transferee's license authorizes the receipt of the type, form, and quantity of radioactive material to be transferred and that the licensee is authorized to receive radioactive material at the location requested for delivery. If the verification is conducted by contacting the license issuing authority, the transferor shall document the verification. For transfers within the same organization, the licensee does not need to verify the transfer.* *(b) Any licensee transferring category 2 quantities of radioactive material to a licensee of the Commission or an Agreement State, prior to conducting such transfer, shall verify with the NRC's license verification system [emphasis added] or the license issuing authority that the transferee's license authorizes the receipt of the type, form, and quantity of radioactive material to be transferred. If the verification is conducted by contacting the license issuing authority, the transferor shall document the verification. For transfers within the same organization, the licensee does not need to verify the transfer.*	Rec 15