Mendiola, Doris

Attachments: 10CFR37 NRC-2008-0120 Comments.docx

From: ERIC BOELDT [mailto:EJB6@psu.edu]
Sent: Wednesday, January 05, 2011 2:18 PM
To: Rulemaking Comments
Subject: Comment on Docket ID NRC–2008–0120 10CFR37 proposed

Attached are the comments pertaining to the NRC's proposed rule on the Physical Protection of Byproduct Material, 10CFR Part 37.

Docket NRC-2008-0120

Thank you,

Eric

Eric Boeldt
Radiation Safety Officer
The Pennsylvania State University
201 Academic Projects Building
University Park, PA 16802
www.ehs.psu.edu
ejb6@psu.edu

7/14/2010
75 FR 40756
12

RECEIVED
2011 JAN -7 AM 9:45
RULES AND DIRECTIVES BRANCH USNRC

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add = P. Goldberg (PFG)
M. Kern (MLK1)

PENNSTATE

Environmental Health and Safety
The Pennsylvania State University
6 Eisenhower Parking Deck
University Park, PA 16802-2116

(814) 865-6391
Fax: (814) 865-7225
Website: http://www.ehs.psu.edu

Secretary
U. S. Nuclear Regulatory Commission
Washington DC 20555-0001
Attn: Rulemakings and Adjudications Staff

Re: Docket ID NRC–2008– 0120 Email comments to *Rulemaking.Comments@nrc.gov*.

Subject: Public Comment on "Physical Protection of Byproduct Material; Proposed Rule" (75 FR 33902) and Draft Guidance for Implementation of 10 CFR Part 37 – Physical Protection of Byproduct Material -- Category 1 and Category 2 Quantities of Material (75 FR 40756); Docket Number NRC-2010-0194.

To Whom It May Concern:

I have reviewed the reviewed this document and the relevant guidance document on behalf of The Pennsylvania State University. PSU has been operating under the multiple Increased Controls since they were issued. The proposed rule appears to be overly prescriptive in some areas and I am concerned about the practicability of some of the proposed changes.

The Pennsylvania State University endorses the need to use the radioactive materials referred to in this Part in a secure and safe manner. PSU accepts our security responsibilities with regard to these kinds of sources and takes those responsibilities very seriously. The following comments are offered as constructive criticism to provide further information that will make Part 37 easier to implement while meeting the intent of providing the necessary security for these devices. In order to fully determine the extent of these regulations, I have tried to comply with many portions of the requirements published on June 15, 2010 as if the draft Part 37 were finalized as currently written. This has been very difficult in some areas.

1. **General comment.**
   Placing all of these security requirements in one chapter significantly enhances their clarity. Thank you. I have found having multiple Increased Control requirements confusing.

2. **General comment.**
   The NRC has to remain aware that the cost of implementation of these requirements (background checks, maintenance and testing of systems) will continue forever. Security measures and requirements are unlikely to be relaxed within the next couple decades. Costs for initial hardware and training, can be justified and bourn more easily than the time and effort required to document the written security plan, perform and document complete quarterly tests, annual reviews of the security program, annual training, reinvestigations, thorough annual audits of physical protection program, and the background check program. Some of these audits are dependent upon the number of devices present and some upon the number of individuals who require access. In either case a good annual audit will require about forty hours of work after the first few years which will be more time consuming.
   I think your estimate of the time for annual requirements is significantly underestimated. I will

not know by how much they have been underestimated until our programs and audits have been fully implemented.

3. General comment concerning the plain language requirement

The Presidential Memorandum, ''Plain Language in Government Writing'' published June 10, 1998 (63 FR 31883), directed that the Government's documents be in clear and accessible language. This memorandum in part says:

By January 1, 1999, use plain language in all proposed and final rulemaking documents published in the ***Federal Register,*** *unless you proposed the rule before that date.*

"Plain language requirements vary from one document to another, depending on the intended audience. Plain language documents have logical organization, easy-to-read design features, and use:

- *common, everyday words, except for necessary technical terms;*
- *''you'' and other pronouns;*
- *the active voice; and*
- *short sentences.*

The NRC did not use the word "you" in the proposed regulations. Obviously by this fact alone, this regulation does not in any way comply with the plain language memorandum and should be completely rewritten.

The definition of "Person" is one sentence of 162 words. Paragraph 37.27(c)(1) is one sentence of 120 words. The first sentence in paragraph 37.29 contains 342 words. These are not necessarily the only sentences that could be shortened, just the ones I noticed in a quick review.

In paragraph 37.33(b), the sentence "The results of the reviews, along with any recommendations, must be documented." Is a good example of the regulations using the passive voice when an alternative active voice construction should be used. An alternative wording would be "You must retain documentation of these reviews." There are many other sentences that fail to follow the Presidential Memorandum that I could discuss. For example 37.1 should be rephrased to "This part establishes the physical protection program requirements for persons authorized to possess radioactive materials described in § 37.2. Implementation of these requirements provides reasonable assurance of protecting these materials from theft or diversion. No provision of this part authorizes possession of licensed material."

Clearly this draft regulation <u>does not comply</u> with the Presidential Memorandum and must be rewritten.

Note that the rest of my comments are written in the same incorrect and awkward style as the current draft version of Part 37 published in the Federal Register on June 15, 2010. My comments suggesting wording which are in the currently published style should not to be taken as approval of that style.

4. Comment § 37.1 Purpose

The NRC needs a clear concise statement that the requirements of Part 37 supersede the Increased Control Orders. I suggest adding a second paragraph to § 37.1

Suggested wording:

"§ 37.1 Purpose (b) As of the effective date of these regulations, the provisions in this part supersede the various security orders known as Increased Controls that were issued to licensees beginning in 2002 to which this part applies."

5. Comment §37.5 Definitions

The phrase "government entity" in the definition of "Local Law Enforcement Agency" is confusing and gives the impression that University Police may not be included in this definition even

though page 33915 indicates otherwise. In addition, page 123 of the guidance document specifically states that the University Police meet this definition.

Suggested rewording:

"Local law enforcement agency (LLEA) means a ~~government entity~~ a police organization that has authority to make arrests and the capability and the defined legal responsibility to provide an armed response in locations where licensed category 1 or category 2 quantities of radioactive material are used, stored, or transported."

Individuals within a LLEA may not wish to respond to a report of theft of nuclear material, but the local police still have the responsibility to respond to any criminal activity at the facility.

6. **Comment §37.11 Specific exemptions**

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

This exemption should be retained in the final draft of Part 37. An institution with a reactor and NRC audited physical protection plan and Category amounts of radioactive material stored in the same building and used by the same personnel should not require dual regulation. During the process of issuing Increased Controls, the Orders seemed to be issued to reactors then a few months later to licensees with devices. A security plan developed to protect the reactor fuel should meet the intent of Part 37 (background checks, alarms, police response). It would be a significant paperwork task to keep records showing compliance with both sets of controls without a real increase in the security of either material. It would also be an added inspection burden if the program required separate inspections by an Agreement state and the NRC.

In order to clarify who has inspection/security oversight, I suggest the following wording:

§37.11 "(b)Any licensee's activities are exempt from the requirements of this part to the extent that its activities are covered under the physical protection requirements of part 73 of this chapter. Although the NRC maintains primary oversight of these facilities, inspection by Agreement State representatives is permitted."

7. **Comment §37.21(a)(3) and §37.41(d) NRC notification of compliance**

What is the purpose of requiring licensees to report compliance with regulations within 30 days of the effective date if the rule is not to take effect until 270 days after publication? For Agreement States, compatible rules may not be issued for an additional three years.

The Increased Controls (ICs) were a new set of complicated regulations that required immediate attention, and thus notification to the NRC was justifiable. These Part 37 regulations, at a basic level, just codify the ICs. Each licensee should have been inspected by the NRC (or Agreement State) on these controls at least once and found in compliance or required to improve. Requiring licensees to report compliance is just an added burden on licensees, the NRC, and Agreement State programs.

The NRC (or Agreement States) should not approve receipt of this type of material unless the licensee is in compliance with the ICs or Part 37.

Deleting §37.21(a)(3) and §37.41(d) will in no way diminish the intent of these regulations but will reduce the regulatory burden.

8. **Comment §37.23(b)(2) Reviewing Official**

The proposed regulation states: "Reviewing officials must be required to have unescorted access to category 1 or category 2 quantities of radioactive materials or access to safeguards information, if the licensee possesses safeguards information, as part of their job duties. "

The reviewing official must "be required to have unescorted access" but according to the

guidance document that person may be "someone from HR". Why would someone from HR need to have access to radioactive material, to the details of electronic response, or the details of police response? Obviously this is just a side step past some sort of regulation. If the individual has no real need for access, (s)he should not be issued a key nor allowed unescorted access. If (s)he does not need access to the details of how police respond to a violent assault on a device, why should that person be allowed access to the information. The Increased Controls were quite emphatic that no individual should be granted access unless that individual actually needed access. This change in regulation appears to reduce the security of the devices which this regulation is supposed to protect.

Depending upon how each institution is organized and who is appointed the "individual with overall responsibility for the security program" having unescorted access may or may not be justifiable. I can envision a situation in which the RSO of the facility is allowed unescorted access but does not have a key to the device or to the room in which the device is stored. (Leak tests are performed with the aid of the operators.) In this case the only individuals with unescorted access would be the few people that actually use the device. These individuals would be the only ones with the pass codes necessary to disarm the alarm systems required in §37.41.

Even the "individual with overall responsibility for the security program" may not need unescorted access to the device, but may be limited to understanding the alarms, communication system, directing the police response, auditing the reviewing official's implementation of the background check process, and auditing the implementation of the alarm maintenance program.

For the NRC to arbitrarily require a person who is, or must become, an expert at performing background checks to have access to radioactive devices implies an oversimplification of the complexities of the T&R process. It is not impossible that the T&R official may never see the devices, be told about the types of alarms present, or learn the details regarding the police response.

The NRC needs to focus on performance based regulations that allow for flexibility while providing the necessary security. It is generally understood that the best security is obtained when the fewest people are allowed access.

I suggest that 37.23(b)(2) be deleted in its entirety.

In answer to the NRC's specific questions:

(1) Does the reviewing official need to be fingerprinted? Yes

(2) Are other aspects adequate? No, the reviewing official needs to be reviewed if for no other reason so he or she is required to complete the paperwork involved in applying for access. Some other individual within the organization should be required to perform the background check of the reviewing official unless the NRC will be performing all of the checks required by Part 37 for that person.

(3) Is the burden too high on licensees to T&R the reviewing official? No. Since a process for performing the review must be established, one extra person should not pose an undue burden. If there are institutions with only one individual with unescorted access, and if that person is the reviewing official then the NRC should perform the review.

9. Comment §37.23(f) Part 73 plans should meet the Part 37 requirements.

For licensees subject to a Part 73 plan that have additional radioactive materials not covered by Part 73, the procedures used for Part 73 background investigations, updating of background investigations, etc. should be considered adequate to meet the intent of Part 37. I suggest adding new paragraph (5):

37.23(f)(5) "Procedures and policies meeting the requirements of the security plans required by Part 73 meet the requirements of this Subpart B of this chapter."

10. Comment §37.25 Background investigations – credit check

I am unaware of how the current level of background investigation came to be considered

inadequate. Is there any documented evidence that indicates that someone "slipped through" a background check? Would the credit check have found this individual?

In reading the Atomic Energy Act of 1954 as amended I was unable to find any reference to a credit history check. If congress, in consultation with the NRC, had deemed credit history checks significantly useful to provide for the common defense, these checks would have been included within the most recent amendments in Section 149 along with the fingerprinting requirements.

I strongly urge that the NRC follow the wishes of Congress and remove the whole credit check provision from Part 37.

11. Comment §37.25 and §37.27 Background and criminal history checks.

When the Increased Controls were first implemented, current employees were grandfathered and thus there was motivation for a licensee to allow for a not completely clean criminal history or credit evaluation. When reviewing job applications at the present time, why should a licensee go to the trouble of looking closer at anyone with a not-perfect background check?

"The Equal Employment Opportunity Commission has been cracking down on efforts to disqualify potential hires with criminal records or bad credit history, arguing that the practice can be tantamount to discrimination, as such applicants are disproportionately black or Latin." Wall Street Journal 8/12/10.

Credit history evaluation may be even more difficult to judge as a way of determining the trustworthiness of an employee. An individual without health insurance can be driven to bankruptcy and multiple bounced checks in short order.

The proposed regulations indicate that criminal and credit history are not necessarily sufficient to stop a clean T&R report, but it is obvious that a reviewing official has the authorization to prohibit anyone with a criminal history or a poor credit score from being considered trustworthy. This is not the intent of these regulations, but it may be an unintended consequence. At the very least, the NRC needs to enhance their guidance for this section. There is little to no information in the guidance Q&A document as to what constitutes acceptable attempts to obtain credit history information, just that we are required "document all attempts."

In August 2010, Illinois Gov. Pat Quinn signed into law a bill that prohibits employers from discriminating against employees on the basis of their credit history. H.B. 4658, the Employee Credit Privacy Act, takes effect January 1, 2011. It says employers can neither inquire about nor refuse to hire, discharge or otherwise discriminate against workers on the basis of their credit reports. Pennsylvania has a similar law moving through the process of being enacted. Although NRC regs may trump PA law in this particular case, it would be best to not have this conflict. A brief internet search found other states with similar laws.

Although I have not tried to obtain a credit history check of a foreign national, I expect it will be a frustrating and expensive procedure with no guarantee that the information obtained is correct. I suggest that the whole "credit history" requirement be dropped from this rule.

12. Comment §37.29 Relief from background checks for designated categories of individuals

Page 33908 and 33912 in the Federal Register discusses categories of individuals for whom T&R determination is not required. Although the discussion clearly states that licensees have the option to escort these individuals, the proposed regulation must clearly state this fact. Please clarify that the licensee **may** give unescorted access to multiple types of individuals in §37.29 (a – m), but that it is in no way required. I realize that the Implementation Guidance makes this clear, but the clarity should be built into the regulations rather than into the Guidance which will be difficult to find in a decade.

In addition, it should be made clear that the training required by 37.43(c) must be obtained prior to being allowed non-emergency access.

Suggested wording:

§37.29 "Fingerprinting, and the identification and criminal history records checks required by

section 149 of the Atomic Energy Act of 1954, as amended, and other elements of the background investigation are not required for the following individuals and they may be granted ~~prior to granting~~ unescorted access to category 1 or category 2 quantities of radioactive materials after having been trained in accordance with 37.43(c):"

13. Comment §37.33 (a) Access authorization program review frequency

Why require that the licensee audit the security program "at a frequency not to exceed 12 months?" In accordance with 10CFR20.1101 the licensee must "periodically (at least annually) review the radiation protection program content and implementation." I think it is appropriate to allow the same flexibility for the access authorization program review that is used for the radiation protection program. The terminology from §20.1101 allows a bit of flexibility that is not present in the proposed §37.55. Organizations with few staff require flexibility to allow for circumstances beyond the control of the work force (staff illness, staff reductions, major contamination events, etc.). Being a couple weeks late on an annual review should not be seen as a security threat or as a significant violation of regulations.

Suggested rewording of last sentence: "Each licensee shall ensure that its entire access program is reviewed once every calendar year at a frequency of 8 to ~~not to exceed 12~~ 15 months.

14. Comment §37.33 Access authorization program review.

Since §37.43(2) requires that the licensee appoint a person with "overall responsibility for the security program", it is only logical that the NRC require that individual to review the results of the annual audit. Half the overall security program required in this Part is based upon allowing access to individuals with good backgrounds. To have the "the individual with overall responsibility for the security program" not involved with the access portion of this program leads to split responsibility. Note that having the reviewing official separate from the "overall responsibility" person is not inappropriate. The "overall responsibility" person may be corporate president, head of security, or the radiation safety officer while the reviewing official may be in the Human Resources department. Still, the "overall responsibility" must include responsibility for the access authorization program.

Suggested rewording of the last sentence:

§37.33(b) The reviewing official and the individual with overall responsibility for the security program for the licensee shall review the findings and take any additional corrective actions necessary to preclude repetition of the condition, including reassessment of the deficient areas where indicated.

15. Comment §37.43(a) General security program requirements.

The wording of §37.43(a)(2) implies the appointment of an "individual with overall responsibility for the security program." An upfront requirement for the licensee to appoint such a person would clarify the responsibilities and authority and make this requirement easier and more direct.

Let me add that I personally know of a three institutions in which no one individual has been given the responsibility to handle background checks, motion detectors, backup power, secure communications, and coordinate police response. If the RSO is in this position by default, (s)he may not have the authority or ability to require appropriate prompt and armed police response or to ensure that the communications systems are always secure and dependable. Having the licensee specifically designate the correct individual will clarify responsibility and provide some authority.

Suggested wording:

New paragraph inserted before §37.43(a)(1) to read

"Each licensee subject to the requirements of this part shall appoint an individual with overall responsibility for the security program and ensure that individual has the authority and resources to ensure implementation of the program."

Alternatively this appointment requirement could be inserted in Subpart B to make it clear that the individual in 37.33 and 37.55 are the same person as listed here in 37.43.

16. Comment §37.43(a)(2) and (3) General security program requirements.

Paragraph (2) requires that the plan be reviewed and approved by "the individual with overall responsibility for the security program", however when the plan is revised the licensee must ensure that the " (i) The revision has been reviewed and approved by the individual with overall responsibility for the security program **and licensee management** {emphasis added}.

Why are there separate requirements for revision "0" and future revisions? Including another person in the approval path just adds additional complications. In addition, the Guidance Document does not include a reference to licensee management.

Paragraph §37.43(d)(3) requires that anyone with access to the plan have a need to know and have had a complete background check (except fingerprinting and criminal history) prior to seeing this information. It is quite possible that licensee management may not wish to go through this process in order to review a plan, particularly if he has delegated the responsibility and authority to other individuals.

Suggested wording:

37.43(a)(3)(i) should be revised by deleting the phrase "and licensee management".

17. Comment §37.43(c)(3) General security program requirements. Training.

Why require that the refresher training must be performed "at a frequency not to exceed 12 months"? In accordance with 10CFR20.1101 the licensee must "periodically (at least annually) review the radiation protection program content and implementation." I think it is appropriate to allow the same flexibility for the access authorization program review that is used for the radiation protection program. The terminology from §20.1101 allows a bit of flexibility that is not present in the proposed §37.43. Organizations with few staff require flexibility to allow for circumstances beyond the control of the work force (staff illness, staff reductions, major contamination events, etc.). Being a couple weeks late on an annual review should not be seen as a security threat or as a significant violation of regulations.

Suggested rewording of 37.43(c)(3)

"Refresher training must be provided <u>every calendar year</u> at a frequency <u>of 8 to</u> ~~not to exceed 12~~ <u>15</u> months and when significant changes have been made to the security program."

18. Comment §37.45 (a-c) LLEA coordination.

The requirements detailed in this section assume that the LLEA is not part of the same organization that owns the radioactive material. In the cases in which coordination is smooth and flawless documentation of good news is a waste of time, effort, and paper. An inspector that finds LLEA response training, LLEA response, and LLEA detailed knowledge of the process should not be able to cite the institution of lack of paperwork. Lack of documentation of coordination activities should be seen as good news unless the LLEA refuses to respond to appropriate requests for assistance.

My institution has excellent coordination between the Environmental Health and Safety Office (including the radiation protection group) and the University Police. A polite and professional relationship between the entities allows for a minimum of paperwork and a maximum response. The officers know that it is their responsibility to protect sources of interest and they are aware of the institutional damage that would result if they failed in their responsibility. To burden the police with specific detailed paperwork is an insult to their understanding of the risks inherent to their mission.

Suggested rewording: Insert a new (1) prior to the current 37.45(a)(1) as follows.

"When the LLEA is part of the organization that owns and controls the Category sources, the documentation in paragraph 37.45(a)(2 {was 1}) is not required provided all the elements of good willful coordination are clear"

19. Comment §37.49(d) Monitoring, detection, and assessment. Response

"Licensees shall immediately respond to any actual or attempted unauthorized access to the

security zones . . . ."

This requirement is too broad. A wondering student who tries the doorknob of a secured area because he was "sort of curious what was in there" is an "attempted unauthorized access to the security zone." There is no point in responding to this sort of challenge to the system as long as the door remains locked. There is no security benefit gained by responding to this type of situation. To prevent and reduce unnecessary responses to this sort of trivial challenge a continuous watchman would be needed or a locked door outside the security zone to prevent access to the boundary of the security zone to keep the tourists away from the security zone. An unescorted NRC inspector who could not gain access but tried to turn the doorknob without success or licensee response could still issue a citation because there was no response by the licensee.

Repeated attempts to enter would be suspicious and reports are required by 37.55(b).

Suggested rewording:

"The licensee shall immediately respond to any action that breaches the perimeter of the Security Zone." {37.57 (b) requires LLEA and NRC notification of any suspicion of attempt to gain access. See relevant comments below. }

20. Comment §37.51(a) Maintenance, testing, and calibration.

In a review of other comments submitted prior to January 1, 2011, to the NRC concerning Part 37, I did not see anyone commenting upon the requirements in this section. On the surface, the background and credit check requirements appear to be more time consuming and aggravating than the requirements in this section. Although I have commented on those sections, I believe that this section will cause more work and headaches than the background check requirements. In particular, I have had difficulty writing procedures that cover all aspects of the requirements in this section. Complying and implementing my own procedures has been **very time consuming** and awkward. Let me add, that the security company hired by NNSA-GTRI that was hired to install the security system was unable, or unwilling, to provide workable procedures that meet this requirement.

The Guidance document for this paragraph states {emphasis added}

- "Identify **all alarms, communication systems, and other physical components** used to secure or detect unauthorized access to radioactive material;
- Specify the **test(s) to be conducted on each component**, and the minimum quantitative or qualitative results of the test(s) required for the component to be found operable and capable of performing its intended function;"

The Guidance and the Regulation should allow licensees to limit testing and recordkeeping to those alarms, systems, and components **necessary** to meet the performance based requirements. The discussion in the Federal Register (page 33914 -5) answers two questions:

"9. What would be required to monitor and detect an unauthorized entry into a security zone?

"A licensee would be required to establish and maintain the capability to continuously monitor and detect all unauthorized entries into its security zone(s). Monitoring and detection would be performed by either a monitored intrusion detection system that is linked to an onsite or offsite central monitoring facility; electronic devices for intrusion detection alarms that would alert nearby facility personnel; visual monitoring by video surveillance cameras; or visual inspection by approved individuals.

"The rule language was clarified in response to comments on the preliminary rule language.

"A licensee would also need the capability to detect unauthorized removal of the radioactive material. For category 1 quantities of radioactive material, a licensee would need to immediately detect any attempted unauthorized removal through the use of electronic sensors linked to an alarm or continuous visual surveillance. For category 2 quantities of radioactive

material, a licensee would need to verify the presence of the radioactive material through weekly physical checks, tamper indicating devices, actual usage of the material, or other means.

"10. What are the requirements for personnel communications and data transmission?

"Licensees would be required to maintain continuous capability for personnel communication and electronic data transmission and processing among site security systems for any personnel and automated or electronic systems used to support the site security systems. Licensees would be required to have alternative capability for any system in the event of loss of the primary means of communication or data transmission and processing. The alternative means could not be subject to the same failure mode as the primary systems. "

Again, the Guidance and the Regulation should allow licensees to limit testing and recordkeeping to those alarms, systems, and components **necessary** to meet the performance based requirements as listed above.

Testing all alarms, systems, and components quarterly is a long term financial burden that can best be mitigated by licensees now by removing all unnecessary alarms, systems, and components. For example if a licensee installed four motion detectors in an area because it was financially prudent to have installed spares, this proposed regulation would punish the institution by requiring testing of all four detectors and their tamper alarms quarterly. Under these regulations it would be financially prudent to disconnect three of the detectors to eliminate the burden of quarterly testing three motion detectors and three tamper indicators.

Another example is a licensee who installs a motion detector inside the room but no actual alarm on the door. Only the motion detector needs regular testing and documentation. The self-locking doorknob is tested during each use and requires no alarms, testing, or documentation. Should the licensee disengage security devices designed to prevent inadvertent access to avoid the burden of testing? Is it the NRC's desire to discourage biometric readers?

Testing extra alarms and tamper indicators upon installation is appropriate. But establishing a regulatory system that requires testing and maintaining records of quarterly testing for extra devices is an unnecessary burden on licensees.

A security system of which I am aware has "door opening" indicators/alarms. The indicators themselves have "tamper alarms" associated with them. Testing the "door opening" mechanism is performed by ensuring that the door cannot be opened without the proper pass code. Testing the tamper alarm on this mechanism involves partial disassembly of the door opening mechanism. Opening the door does not affect the status of the motion alarms which are the real security alarm. Thus, testing the tamper alarm on these door opening devices provides no additional security and is a waste of time.

I submit that the necessary components of a properly maintained security system that meet the requirements are detailed in the Federal Register and no further alarms should require regular testing. Any mechanical or monitoring devices beyond that list is not installed to prevent unauthorized access but rather to provide additional information to the responders and are thus not necessary to maintaining security. A wire mesh grid to keep squirrels out of the facility is not necessary for security but is desirable to reduce false alarms and increase the likelihood of prompt response. A camera to allow individuals to view the area prior to responders entering is desirable to increase the safety of responders and reduce the assessment time of LLEA but is not necessary in all regulated locations. A radiation detector is not necessary for category 2 sources to indicate the presence of unauthorized access but will give responders valuable information as to the device's situation prior to entering the area.

Based on this list, NRC inspectors can work with licensees to determine "necessary" alarms and components. I am aware that this leaves this requirement open for interpretation, but performance based regulations should allow for a risk based analysis. If a facility meets the Increased Control security requirement with fewer security devices, why should the licensee be required to quarterly test other alarms that provide information above and beyond those necessary to maintain security?

In addition, if licensees are required to test all installed alarms and components instead of those just necessary, the individuals monitoring the alarms begin to think all alarms are tests. Under these circumstances I believe most licensees would test more alarms than strictly necessary but fewer than all

available alarms.

One more example, if an institution has more radiation detection meters than it actually needs at a particular time, they are often "withdrawn from service" to avoid the task of annual calibrations. This does not mean these meters are non-functioning, just that they do not need to be calibrated and should not be used for regulatory requirements. If an institution has more security measures than needed, they should be complimented not punished by requiring calibration of extra devices. If a device is not regularly tested the licensee would not be able to take credit for its presence during an inspection. If the licensee has two motion alarms but only takes credit for and tests one alarm the licensee meets the intent of the regulation. If the tested one fails, the backup would automatically meet the needs of the regulation until the primary device is repaired.

Testing of all alarms places an unnecessary burden on licensees and will encourage licensees to minimize the number of alarm points in a system which is counter to the intent of this regulation. Testing of necessary alarms will show that the system is functioning appropriately.

In addition, testing of alarms "not to exceed 3 months" unnecessarily limits licensees without an added benefit. Changing the interval to "every calendar quarter not to exceed 5 months" provides an extra degree of flexibility while still adequately verifying the system.

An institution in which I was employed was once cited by the NRC because a contamination survey meter with an "annual" calibration requirement went 369 days between calibrations. This possibility makes many individuals in the regulated community wary of very detailed calibration frequencies.

The test frequency for an device should have a relationship to the device's known failure rate. If a tamper switch has no known failure rate as long as it remains safely behind its plastic cover, why should the cover be removed quarterly to test the switch? Obviously we should not need to test a concrete wall, nor should a test be required for something that is most likely to fail due to too frequent testing. For example, a limit-switch of which I have knowledge is tested monthly because it needs to be adjusted frequently due to being exercised multiple times per day. So it is tested after 30 – 150 cycles. A tamper switch inside the plastic cover of a motion detector would only be exercised whenever it is tested. A test frequency of 1 per 100 cycles would imply that no tests would ever be necessary. I suggest a test frequency similar to the leak test frequency of sealed radioactive sources that are in storage which is normally once per decade.

Suggested wording

§37.51(a) Each licensee subject to this subpart shall implement a maintenance, testing, and calibration program to ensure that intrusion alarms, associated communication systems, and other physical components of the systems ~~used~~ <u>necessary</u> to secure or detect unauthorized access to radioactive material are maintained in operable condition, are capable of performing their intended function when needed, and are inspected and tested for operability and performance <u>every calendar quarter</u> at intervals not to exceed ~~3~~ 5 months. <u>Equipment without a known failure mechanism shall be tested after initial installation and at a frequency not to exceed 10 years.</u>

A question that should be answered in the discussion at the publication of the final rule:

If an alarm system/device is removed/de-energized from service because the "individual with overall responsibility for the security program" deemed the device unnecessary, obviously there are no testing/maintenance requirements, however if the device is deemed unnecessary but remains energized, must testing/maintenance be performed and documented?

21. Comment §37.55 (a) Security program review.

Why require that the licensee audit the security program "at a frequency not to exceed 12 months?" The licensee must "periodically (at least annually) review the radiation protection program content and implementation." I think it is appropriate to allow the same flexibility for the security audit that is used for the radiation protection program review. The terminology from §20.1101 allows a bit of

flexibility that is not present in the proposed §37.55. Radiation safety offices with few staff require some flexibility to allow for circumstances beyond the control of the work force. Being a couple weeks late on an annual review should not be seen as a security threat or as a significant violation of regulations.

Suggested rewording of last sentence:

"Each licensee shall ensure that the security program is reviewed every calendar year at a frequency not less than 8 months nor to exceed ~~12~~ 15 months.

22. Comment §37.57(b) Reporting of events. Suspicious activity

The annex in the Guidance document provides a long list of suspicious activities which, upon discovery, require reporting to LLEA and to the NRC. How is this paragraph to be enforced? If the "suspicious" activity is not reported to the RSO and thus not reported to the NRC upon discovery is the institution in violation? What if a staff member thinks *everything* is suspicious and reports suspicious activities to the RSO on a weekly basis? Should institution and NRC go to heightened security or fire the employee?

Changing "shall" to "should" or adding a phrase that "notification to the NRC shall be at the discretion of the individual with overall responsibility for the security program" would make this section less confusing.

In addition, describing the types of suspicious in the regulation as opposed to the guidance document increases the clarity of the regulation.

Suggested rewording:

(a) The licensee shall notify the LLEA upon the discovery of any suspicious activity that may indicate preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees, or their facilities related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material. As soon as possible but not later than 4 hours after notifying the LLEA, the licensee ~~shall~~ should notify the NRC Operations Center ((301) 816–5100) if the situation warrents.

It is far better to put the "preoperational surveillance . . ." clause in the regulations rather than in the guidance document. The guidance document description may well be hard to access in fifteen years.

23. Comment §37.57(b) Reporting of events. Suspicious activity

When does the number of nuisance alarms generated by an automated system rise to the level of a suspicious activity? Although this seems like a flippant question, it is important for the NRC to determine the number of calls that are directed to the NRC. One alarm can be a power glitch, a second alarm three days later can be an electric storm. Is a system error three days later suspicious? What if all three happen at 8:27 in the morning? Obviously, analysis of these incidents requires a judgment call on the part of the person in charge of overall security.

24. Comment §37.57(b) Reporting of events. Suspicious activity

If the LLEA provides an immediate assessment and determines that the event is completely harmless, why must the NRC still be notified? Notification is not always necessary even in cases where the LLEA was contacted. Here are two real examples of what my notification to the NRC would have been under the requirements of this regulation.

("I am calling you in compliance with 10CFR37.57(b) because an employee at my institution was taking pictures of all University buildings which they do every ten years. Based on the body language of the photographer and number of pictures being taken I called University Police who immediately responded to the suspicious event. We all had a good laugh at my expense.")

("I am calling you in compliance with 10CFR37.57(b) because an armed State Police Captain requested a tour of the facility. The Captain was in uniform but driving his personal car.

He was unknown to all available personnel. The LLEA were called and a police Supervisor immediately responded. The State Police Captain and the LLEA Supervisor were well known to each other even though they hadn't seen each other in couple weeks. They determined that calling LLEA was the correct action on my part. Moreover in order to prevent heart palpitations, the State Police Captain really should in the future call ahead and make an appointment for a tour. The State Police Captain indicated that he would try to remember next time.")

Adding the phrase "in the judgment of the individual with overall responsibility" or "in the judgment of the LLEA" allows some local interpretation to this notification.

Suggested wording:

(a) The licensee shall notify the LLEA upon the discovery, of any security-related events involving suspicious activity that may indicate preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees, or their facilities related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material. If the event is not found to be harmless ~~by the LLEA~~, the licensee should notify the NRC Operations Center ((301) 816–5100) as soon as possible, but not later than 4 hours, after notifying the LLEA.

I hope the information above is properly responsive to your request and I will be happy to furnish further information if necessary.

Sincerely,

Eric Boeldt, CHP
The Pennsylvania State University
Radiation Safety Officer
Ejb6@psu.edu