

**Rulemaking Comments**

---

**From:** Sheetz, Michael A [msheetz@pitt.edu]  
**Sent:** Wednesday, January 12, 2011 3:53 PM  
**To:** Rulemaking Comments  
**Subject:** Docket ID NRC-2008-0120

DOCKETED  
USNRC

January 12, 2011 (4:45 pm)

**Docket ID NRC-2008-0120**

OFFICE OF SECRETARY  
RULEMAKINGS AND  
ADJUDICATIONS STAFF

The following comments are offered for consideration regarding proposed 10 CFR 37 "Physical Protection of Byproduct Material":

**37.5 Definitions**

In the definition of "Escorted Access", the term "line-of-sight" should be deleted as it is too prescriptive and creates compliance issues should someone "look away" or stand in an area of the security zone where the escorted individual's view may be blocked by some object or equipment in the zone. Surveillance can also be accomplished by remote video monitoring.

The definition of "Local law enforcement agency (LLEA)" should be revised. As currently written, it "means a government entity..." The LLEA for our large university is the university police department, which has full authority to make arrests and provides an armed response. It is not however, a government entity, but a private one. I note that in comment C 13, a university campus police force that is capable of providing an armed response and making arrests meets the proposed definition of LLEA: however, a change in the wording of the actual regulation would clarify this point. I would suggest that the wording "a government entity" be changed to "a law enforcement agency" or "licensed law enforcement agency".

**37.23 (b) Reviewing officials**

I agree that the reviewing officials should be evaluated as to their trustworthiness and reliability, and that their approval by an outside agency such as the NRC is a logical methodology.

The definition for "Reviewing official" is well worded. Their function is to make the trustworthiness and reliability determination. In 37.23 (b)(4) and 37.23 (b)(5) however, the wording suggests that they are also the individuals who permit unescorted access. I object to the additional wording with regard to permitting.

The function of the reviewing official is to determine an individual's trustworthiness and reliability and to thereby authorize that unescorted access privileges may be given to that individual. Access permissions may be controlled by others. The review of an individual to determine trustworthiness and reliability is basically a routine human resources department function. In our institution, our T & R official is a Human Resources employee. Once a positive determination is made, the actual permissions for unescorted access are controlled by, in our case, Radiation Safety personnel.

I suggest that 37.23 (b)(4) be terminated after the word "determinations", therefore reading "Reviewing officials nominated by the licensee and approved by the NRC are the only individuals who may make trustworthiness and reliability determinations."

I also suggest that 37.23 (b)(5) be modified to delete the words “or permit any individual to have unescorted access”. It would therefore read, “Reviewing officials may not make any trustworthiness and reliability determinations until they have been approved as a reviewing official by the NRC.”

Finally I suggest that 37.23 (e)(2) be modified by changing the word ‘permit” to “authorize”, thus reading “The reviewing official may not authorize any individual...”

### **37.25 (a)(6) Background investigations, Credit history**

I do not believe that a credit history check is necessary for the determination of whether an individual is trustworthy and reliable. In our initial response to the Increased Controls order, “recurring financial irresponsibility” was one item of fourteen suggested for inclusion in the background check process, and we opted not to include it into our program as it was considered too invasive for the purpose. Whether an individual can manage money is not a clear indicator of reliability. Negative report items such as bankruptcies, liens and judgments, foreclosures, and accounts in collection, without detailed explanations, do not constitute a lack of trustworthiness and corresponding security risk.

In our program we currently have 250 individuals who have been granted unescorted access. For the past three years, we have averaged 35 new applicants each year. Because we are a university, most are graduate students and post doctoral researchers. One third of our new applicants are foreign nationals. They come from a diverse number of countries, most recently including Korea, China, Japan, Denmark, Italy, Argentina, Russia, and India. We contacted our background investigation vendor and the fee for a foreign credit history check is currently \$170; however, Japan, Denmark and Russia are not on their country listing. Our vendor stressed that credit reporting from other countries is not comparable to the U.S. system and varies by country. Therefore, a credit history for a foreign national may be of little value in the trustworthy and reliability approval process.

Finally, 37.29 exempt several categories of individuals from background investigations prior to granting unescorted access. A Member of Congress or a law enforcement person may be just as likely to have a negative credit history report as is a research investigator wishing to utilize a device containing a category 1 or 2 quantity of radioactive material, but they will not be subject to the same scrutiny. This appears to be an inequity in the process.

For these reasons, I do not think a credit history should be mandated by the regulation.

### **37.33 Access authorization program review**

To simplify the overall review process, this section should be deleted and added as a component of the Security program review in section 37.55.

**Question C 6 (5)** Should background investigation elements for access to security information be the same as for determining physical access (reference to **37.43 (d)(3)(ii)**)?

Regarding the background check for individuals who are granted access to the security plan, I feel the elements of the background check should be the same as for unescorted access, including the fingerprinting and FBI criminal history check. This would make all background checks consider equal factors. It is important to know whether an individual has a federal criminal history.

### **37.43 (b) General security program requirements, Implementing procedures**

The requirement to have separate procedures for the implementation of the security program is unnecessary since they should be incorporated into the security procedures. This section should be deleted.

### **37.51 (a)**

I agree that security systems should be maintained, tested and calibrated on a periodic basis such as quarterly. However, certain detection devices, such as tamper indicators, may be internal to a piece of equipment (i.e. a gamma irradiator), therefore requiring partial disassembly of the equipment for testing. Repeated disassembly and reassembly for testing purposes could lead to premature failure or wear on components. It is suggested that internally installed detection devices be allowed to be tested on an annual basis, which could coincide with an annual preventative maintenance of the equipment.

**Question B 8 (6)** how much time does a licensee typically spend on conducting the background investigation for an individual?

Our approval process involves multiple individuals. Initial processing of the application for access is handled by an individual in the safety office. Human Resources conducts reference checks, department review, and payroll checks. A third party background investigation firm is contracted for previous employment, local criminal history, and education confirmation. The LLEA takes the fingerprints.

Average time spent for each applicant is approximately 2.5 hours. In addition, the average fee charged by the outside contractor is \$100 (without credit history.) Overall administration of the program involves a 0.2 FTE.

### **37.49 (a) Monitoring, detection and assessment**

Allowing monitoring and detection to be performed only by visual inspection [(a)(2)(iv)] or direct visual surveillance [(a)(3)(i)(C)] is not adequate for non-mobile devices. The concepts of detection, delay and deterrence are best implemented through multiple tiers of security.

I believe that the monitoring and detection aspect of the security program needs to be more prescriptive, with a minimum requirement for electronic sensors and a detection system linked to an on-site or off-site monitoring facility. As a case in point, in several of our facilities there are category 1 sources controlled by two different licensees (the blood bank operations are independent.) This has resulted in two separate and different Increased Controls programs. One program utilizes security measures promoted by NNSA, the other depends on 24 hour staffing alone. The responding LLEA is not the same for the two programs, though the buildings are physically connected. Certainly in the scenario of armed terrorists with explosives attacking a facility, reliance on individuals to be the sentinels allows the security program to be defeated rather easily.

Michael Sheetz, MS, CHP, DABMP  
Director, Radiation Safety Office  
Radiation Safety Officer  
Clinical Assistant Professor of Radiology  
University of Pittsburgh  
G-7 Parran Hall, 130 DeSoto St.  
Pittsburgh, PA 15261

Received: from mail1.nrc.gov (148.184.176.41) by OWMS01.nrc.gov  
(148.184.100.43) with Microsoft SMTP Server id 8.2.247.2; Wed, 12 Jan 2011  
15:52:49 -0500

X-Ironport-ID: mail1

X-SBRS: 4.5

X-MID: 29443138

X-IronPort-Anti-Spam-Filtered: true

X-IronPort-Anti-Spam-Result:

AocAAD+jLU1AEgKjkWdsb2JhbACCOqEtbQEBAQEJCwoHEQUftgKGGIJsgmAehGg

X-IronPort-AV: E=Sophos;i="4.60,314,1291611600";

d="scan'208,217";a="29443138"

Received: from exprod7og105.obsmtm.com ([64.18.2.163]) by mail1.nrc.gov with  
SMTP; 12 Jan 2011 15:52:48 -0500

Received: from source ([136.142.251.60]) (using TLSv1) by  
exprod7ob105.postini.com ([64.18.6.12]) with SMTP ID

DSNKTS4Un047gtvfM/K/kPyMvFqxaaZcyP8H@postini.com; Wed, 12 Jan 2011 12:52:48  
PST

Received: from pitt-exch-10.univ.pitt.edu ([169.254.1.107]) by  
pitt-ht-03.univ.pitt.edu ([136.142.251.60]) with mapi; Wed, 12 Jan 2011  
15:52:46 -0500

From: "Sheetz, Michael A" <msheetz@pitt.edu>

To: "Rulemaking.Comments@nrc.gov" <Rulemaking.Comments@nrc.gov>

Date: Wed, 12 Jan 2011 15:52:45 -0500

Subject: Docket ID NRC-2008-0120

Thread-Topic: Docket ID NRC-2008-0120

Thread-Index: Acuymqnf6UV+kEwWStqyYiyWUm1ROw==

Message-ID:

<15D7EBBD5E43C34D92857D3EEDBC45F005266F1314@PITT-EXCH-10.univ.pitt.edu>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

acceptlanguage: en-US

Content-Type: multipart/alternative;

boundary="\_000\_15D7EBBD5E43C34D92857D3EEDBC45F005266F1314PITTEXCH10uni\_"

MIME-Version: 1.0

Return-Path: msheetz@pitt.edu