From: fejka <rotman@nmdhst.cc.nih.gov>
To: TWD2.TWP8(dac)
Date: 8/7/96 1:15pm
Subject: Comments for 8/21 security workshop

7 Aug 96
Mark Rotman
8585 Mansfield Court
Middletown, MD 21769
(301) 371-7651
(301) 496-1426 work

Dr. Cool;
Hello, forgive me for sending you this via E Mail. This time no allegations will be made. I will be unable to attend the workshop in RI on Part 20
Security Policy to be held 8/21/96. I will be on vacation, so I wish to send my generic comments, so that they may be included when the findings of that workshop are reviewed.

The NRC has a "one size fits all" policy on security. The problem with this policy is that the issues of security are multifaceted, the risks range from zero to significant. It is also clear that for certain types of criminal action the existing policy is inadequate, yet for other types of criminal activity the policy is excessive.

The NRC needs to develop a security policy that adapts to the risks and to the type of criminal activity the policy is designed to prevent. This new security policy should be developed in accordance with Presidential
Executive Order 12866, i.e., have a risk-risk, risk-benefit, benefit-cost analysis, so that the security measures created to conform to the new security policy provide a level of protection that is fiscally reasonable, achievable by the licensee, and accomplishes the goal of protecting the public health and safety. This new security policy will be impossible to create without first setting a threshold of risk. Below this threshold no security is required, above this threshold the level of security is commensurate with the risk. What level of risk creates the need for security? Above this level, what are the risk thresholds that induce additional security measures?

As a former Deputy Sheriff I have some comments on criminal activity. I will deliberately omit discussion of criminal activity (security) at power plants, fuel cycle, and other licensees (possessing rather large quantities of RAM). I will limit my discussion to licensees involved in fields of medicine, pharmacy, and biomedical research.

=B7 Inadvertent criminal activity: I am not sure this is criminal activity, but it could result in a violation of the current NRC security policy, thus creating a violation for licensee. If a worker accidentally picks up a package not destined for that person (wrong package pickup), or a package is mis-addressed, so that it is delivered to the wrong person. Also possible here are lost packages. In all these cases the package may not be secured or under surveillance at all times - thus a violation of the current security policy. However, this is the most frequent event in issues of security. Also, if the work area where RAM is contained is left open (door open) and a stranger walks in, no theft takes place, this is also a breach of security unless the authorized user stops/and or questions the stranger.

Attachment (6)

Even though no crime takes place this is also a security violation.
Question: Should the NRC security policy address inadvertent activities such as these? Does the current NRC security policy prevent these events?

=B7 Crimes of Opportunity: This is a very common type of criminal activity, and often does not involve the career criminal. It can occur in the work place where one worker steals the purse of another. In any case, whether it be the professional or amateur criminal, the target are items of value or desire that are easily obtained. Sneak thieves will steal what is available, they will usually only takes what has a retail value, and can be easily sold. This activity is usually not premeditated. It is premeditated only in as much as they will enter an area wanting to steal whatever is easily available, to produce currency for a need, such as drugs. These types of criminals often have favorite items to heist, as they can develop an outlet for them. These types of crimes do not require premeditation or tools. Question: !s RAM (type and quantity used by this subset of licensees) a target in crimes of this nature? Does the current NRC security policy prevent these events?

=B7 Breaking and Entering (B&E, or burglary). This is a planned and premeditated criminal activity, and usually requires tools. This type of criminal activity usually targets a certain type of facility, like a residence, or business. Secondarily, the target is often a specific type of material, like cash, jewelry guns, tools, cameras or whatever. However, the criminal will take what is of value in addition to or instead of what was originally targeted. Question: Is RAM (type and quantity used by this subset of licensees) a target of these types of criminals? Does the current
NRC security policy prevent this type of activity?

=B7 Armed Robbery: Although depending on definitions, this could include muggings. This is premeditated, in that the criminal plans to commit this crime. However, the victim could be pre-selected (liquor store just prior to closing or making a bank deposit), or the victim could be random (mug someone simply because they are walking alone on a dark secluded street). Armed robbers also develop preferences, thus we have bank robbers, convenience store robbers, muggers etc. Question: Is RAM (type and quantity used by this subset of licensees) the target of these types of criminals? Does the current NRC security policy prevent this type of=
activity?

=B7 Terrorist: This will usually involve multiple types of crimes to obtain the weapons of terror, then the terrorist act itself. For example B&E/and or armed robbery might be used to obtain guns or cash, then the cash is used to travel, the guns to commit more crimes obtain the weapon of choice for terror. Terrorism is premeditated. Question: Is RAM (type and quantity used by this subset of licensees) the target of these types of criminals?
Does the current NRC security policy prevent this type of activity?

=B7 Revenge/Jealousy: This seems to appear in the NRC regulated community every year or two. Someone, usually a authorized worker is internally contaminated with RAM. There appears to be no immediate fiscal reason for this, and since no one has been harmed (in a true physical way) the motives for such an act must be personal in nature. The regulatory response (for both the licensee and the NRC) to these acts, as well as the media attention given these events appear to make them useful for purposes of revenge. The victim is effectively taken out of the use of RAM for a period of time, often months. Question: Do the

actions of the regulators make this crime more attractive? Does the current NRC security policy prevent this type of activity?

What exists in terms of quantity of RAM in this subset of licensees is a broad range. At the high end, in therapy centers, RAM in quantity that could cause real and immediate harm if used improperly. At the other extreme, in biomedical research facilities, the amount of RAM often used would not even trigger the part 20 exposure limits for the general public. Thus, it is clear there is a range of risk from these various quantities of RAM, from real risk of harm to no risk at all. =20

At one extreme, the current NRC security policy is inadequate to prevent most premeditated criminals from obtaining RAM. At the other extreme the current NRC security policy is excessive, and may in some cases cause an inadvertent risk to public health and safety (locking doors, and restricting access to provide security for a few microcuries could delay or prevent emergency services from acting in a timely manner). Economically the current NRC security policy, as applied to medicine, pharmacy, and biomedical research, forces a considerable expenditure of funds and manpower, to protect the public from material that is relatively harmless compared to many other items in everyday use. An example of the impact of excessive regulation is current policy on the use of RAM at the National Institutes Health. NIH has moved to minimize the use of RAM wherever and whenever possible, this was done as direct result of the current NRC security policy. The current policy is expensive to implement, and does not foster a collegiate like atmosphere for research. Question: Does the NRC want its regulations to have such a profoundly negative impact on biomedical research?

I have deliberately not answered the questions I have asked, I know what I think, but I also think it is important for these questions to be asked and discussed by the group. Perhaps in this way the NRC can refocus its security policy, a craft a policy that provides security commensurate with risk and at a price the American public can afford. Thanks for letting me provide my thoughts on this very important issue=85

Sincerely,

Mark Rotman
Mark Rotman
Chief, Radiolabeling Unit
Monoclonal Antibody Section
Dept of Nuclear Medicine
NIH, Bethesda MD 20892-1180
(301)496-1426
(301)496-3544 FAX
(301)402-4548 FAX rotman@nmdhst.cc.nih.gov E Mail

CC: TWD2.TWP8(lwc)

ACURI Association Inc.
820 North University Drive
University Support Building 1, Suite B
University Park , PA 16802-1003
814-863-2348
814-863-2347 fax
jrv2@email.psu.edu

ACURI Position Statement on Radioactive Materials Security

Position: ACURI's Technical and Regulatory Advisory Committee (TRAC) supports the Conclusions (pages 18 and 19 and Table 1. and Table 2.) of the Howard Hughes Medical Institute Workshop Summary draft report dated August 12, 1996. The report is entitled, "Effective Security of Radioactive Materials in Biomedical Research Laboratories". The document states:

Conclusions

• There is a need to revise NRC compliance standards as they pertain to the enforcement of 10 CFR 20.1801 and 10 CFR 20.1802 in biomedical research laboratories. This need is based on inconsistencies in NRC regulatory standards and guidelines, and the substantial range of potential public health risks that exist between the types of NRC licensees (e.g., biomedical research institution vs. nuclear power reactor).

• The preferred strategy for defining relevant compliance standards is to encourage NRC enforcement officials to reassess and revise existing enforcement guidelines to ensure the guidelines correspond to the risks associated with the handling, storage, and loss of RAM in biomedical research laboratories. A collective assessment involving scientists, radiation safety officers, and NRC enforcement officials would be beneficial.

• COMPLIANCE STANDARDS SHOULD BE BASED ON THE FOLLOWING THREE PRINCIPLES:

> The responsibility of an institution to secure and control RAM should be applicable to all quantities of RAM.

> Practices for securing and controlling RAM will vary depending upon the risk associated with the use and storage of RAM, and the general security experience of the institution's local community.

> A determination of "in compliance" should be achievable at some level of performance less than perfection.

• ACCEPTED PRACTICES FOR SECURING AND CONTROLLING RAM IN BIOMEDICAL RESEARCH LABORATORIES INCLUDE:

> The ways in which an institution controls building security risks associated with local community security experience.

> The oversight provided by the radiation safety committee of the institution's radiation protection program.

> Training that ensures users are informed of their responsibilities to secure and control RAM and provides appropriate instructions.

> Using RAM in designated laboratories.

> Posting the universal radiation symbol outside of the designated laboratories where RAM is used.

> Accounting for quantities of RAM removed from stock source containers kept in storage.

> *Locking containers or rooms used to store stock source containers of RAM.*
> *Providing constant surveillance of research protocols involving quantities of RAM that exceed a determined risk level.*

Table 1 provides guidance for the selection of security and control practices identified above. Constant surveillance was determined to be appropriate when research protocols require quantities of RAM equal to or greater than 100 x Appendix C quantities. Table 2 identifies the 100 x Appendix C quantities for radionuclides commonly used in biomedical research laboratories.

Table 1. Security and Control Practices for RAM Used in Biomedical Research Laboratories Based on Relative Risk Indices.

SECURITY AND CONTROL PRACTICES	RELATIVE RISK INDICES		
	RAM Quantities Used in Research Protocols		RAM in Storage
	<100 x Appendix C	≥100 x Appendix C	Stock Source Quantities
Local Building Security Practices	√	√	√
Radiation Committee Oversight	√	√	√
Training	√	√	√
Designated Laboratory	√	√	√
Accountability			√
Posting of Laboratory	√	√	√
Locked Containers or Storage Rooms			√
Constant Surveillance or Locked Laboratory Doors		√	

Table 2. The 100 x Appendix C Quantities for Radionuclides Commonly Used in Biomedical Research Laboratories.

Radionuclide	100 x Appendix C Quantities
^{3}H	100 mCi
^{14}C	10 mCi
^{32}P	1 mCi
^{35}S	10 mCi
^{125}I	100 uCi
^{131}I	100 uCi