UCRL 15265

Master

INSPECTION METHODS FOR PHYSICAL PROTECTION

TASK II

Review of Research Reactor Licensees' Physical Security Practices

July 3, 1980

Submitted to:

Lawrence Livermore Laboratory
P.O. Box 808
Livermore, California 94550

Submitted by:

Teknekron Research, Inc.
1483 Chain Bridge Road
McLean, Virginia 22101
(703) 734-0800

Under Contract No. 9440309

TASK II BACKGROUND

Introduction

On May 24, 1978, the Nuclear Regulatory Commission issued for public comment proposed amendments to 10 CFR Parts 70, 73, and 150. These amendments required physical protection measures to detect theft of special nuclear material of moderate and low strategic significance and applied to non-power reactor facilities. Interested persons were given 30 days to comment on the proposed amendments.

Many of the commenters questioned the need for the new requirements. They complained that detailed information regarding the threat was lacking, that the costs of complying with the regulations would be incommensurate with the marginal improvements in physical protection, and that the regulations could have an adverse affect on the licensees' educational and research programs. Underlying all these comments was the feeling that the requirements were not technically justified. Because of this general feeling that the requirements are unnecessary, attitude is a key factor in licensee compliance.

On July 24, 1979, the NRC published the revised amendments. The amendments became effective on November 21, 1979. The licensees were originally required to submit new physical security plans (PSPs) by March 20, 1980, but because of intra-Commission confusion, they received an extension until May 19, 1980. As of late June 1980, not all of the licensees had submitted new PSPs. The NRC staff did not plan any immediate follow-up action because it was already overburdened and wouldn't be able to review the plans for some time.

To assist Lawrence Livermore Laboratory in its development of research reactor inspection modules for the NRC, Teknekron Research, Inc. (TRI), examined a sample of the the reactor licensees' responses to the new physical security requirements. Our primary objective was to provide an overall picture of the

security practices and attitudes at research reactor facilities. The following sections present our findings for the three facilities examined and draw conclusions about how these findings apply to the entire research reactor community.

TASK II FINDINGS

To perform Task II, we reviewed the security plans for and visited three local research reactors. On June 17, 1980, we toured the Armed Forces Radiobiology Research Institute (AFRRI) in Bethesda, Maryland. Two days later, we visited the research reactor facility at the University of Maryland in College Park, and on June 23 we toured the University of Virginia's facility in Charlottesville.

In the following sections, we describe our impressions of the scope, stringency, and specificity of the physical security plans for each facility. (We reviewed AFRRI's new security plan, which had not yet been approved; for the Universities of Maryland and Virginia, we reviewed the old PSPs because they had not yet submitted revised plans.) We then present our observations of the security procedures and equipment at the facilities and comment on how closely they match the procedures described in the PSPs. Finally, we describe the facility staffs' attitudes toward compliance with the security requirements.

We caution readers of this report that the facilities may have physical protection procedures or equipment that they were unwilling to disclose to us for security reasons. Readers should also be aware that impressions of licensee attitudes are strictly subjective. In addition, the attitudes of the few people we interviewed at the facilities may not be representative of the attitudes of the staffs as a whole.

ARMED FORCES RADIOBIOLOGY RESEARCH INSTITUTE (AFRRI)

The AFRRI reactor facility in Bethesda, Maryland, houses a TRIGA reactor with an authorized power level of 1,000 kilowatts.

Review of Security Plan

We found the revised physical security plan for this Category III facility adequate to meet the requirements of 10 CFR 73,.67(f)(1)-(4). The plan is quite specific in that it:

- Names the persons responsible for control of security in both normal and emergency situations
- States the number of rounds to be made by the security watchman within a specified time period
- Gives specific dates for plan review and inventory of keys

The plan does not list brand names of the detection equipment used, but this is not a requirement. In contrast to its generally high level of specificity, the plan fails to state that detection devices will be checked for operability either periodically or before being placed in operation. Nor does it state who will activate the alarm system at the end of regular hours.

We found the plan to be sufficiently stringent, except in the area of control of master keys. This requirement could be made stronger, perhaps by reducing the number of people who are allowed to have keys.

Observations of Security Practices

The security procedures and equipment at the AFRRI facility generally match those described in the security plan. Unauthorized persons (i.e., visitors) are admitted only with the approval of an authorized person and are escorted

at all times. The visitors are approved for entry and registered within the reception area. A series of locked doors opened by electromagnetic cards and color-coded security badges bars entry to the controlled access area (CAA). All doors have alarms and are monitored by either security personnel or closed-circuit video camera.

The only instance where security procedures described in the plan were not in effect was the final barrier leading to the reactor room. Although the plan describes this barrier as locked, the door was blocked open. However, the reactor was not in operation at the time and, to reach this point, one must have already passed through two barriers.

In the only other deviation from the plan, we found the overhead crane in the reactor room to be secured although this was not mentioned in the security plan.

The only SNM at the facility is in the reactor core or stored in the reactor pool. Visual accounting of the stored fuel, visual inspection of the core, and testing the reactivity of the core before start-up should be sufficient to detect any theft or mishandling of SNM. The closed-circuit video cameras and motion detectors used to monitor the reactor room, along with the alarm system, should be adequate to alert security personnel of an attempt to remove SNM. We did not observe shipping and receiving procedures and cannot comment on them.

We noted the following equipment in use at the facility:

- Russco card readers
- Exide Lightguard emergency lamps
- Scovill speakers at access points
- Honeywell computer
- Closed-circuit TV monitors (two in reactor room, one monitoring door to CAA)

Attitude of Staff

Based on the comments of the facility's director, we believe that the staff has a positive attitude towards security procedures. Although they perceive the threat of sabotage or theft as greatly exaggerated, they appear willing and able to carry out the required security functions. The staff does not consider the 10 CFR 73.67 requirements to be a burden, although spending time to produce and submit a revised security plan is felt to be a nuisance. One explanation for the staff's generally positive attitude toward security requirements is that the facility is under military control, and the military orientation towards security contributes to compliance with NRC requirements.

UNIVERSITY OF MARYLAND

The Maryland University TRIGA Reactor (MUTR) in College Park is a pool-type, conversion research reactor with a power rating of 250 kilowatts steady state (no pulsing capability).

Review of Security Plan

The University of Maryland is a Category III facility. Its first physical security plan was submitted in 1974, and this 1974 plan appears generally adequate to meet the new Category III requirements. The plan may need some elaboration to meet 10 CFR 73.67(f)(4), which requires the licensee to establish and maintain response procedures to deal with theft or threat of theft of SNM. The 1974 plan states only that the response procedures are standard university practices. This statement may be too general to indicate compliance with the new regulations. The 1974 plan must also be updated to include the ultrasonic detectors added in the last six years (only one detector had been installed in 1974).

The plan describes very specifically the alarm systems in use and their arrangement. Far more protection is provided for in the plan than is actually required. The new Category III requirements will have little affect on this facility since its security arrangements are already adequate to meet

these requirements. The only effort needed for compliance will be the completion of the associated paperwork.

Observations of Security Practices

Security practices observed at the University of Maryland research reactor facility correspond to those described in the 1974 PSP. The security system was built in stages with a total material cost of about $6,000.

Entry to the controlled access area (CAA) is governed by a series of locked doors with either combination locks or locks of 6-pin locksmith quality. The facility's procedures for key control appear to be adequate. There are alarms on the access barriers to the reactor room and control room, and area motion detectors and infra-red presence detectors are used to detect unauthorized entry into the CAA. The alarms are connected to four independent tamper-indicating circuits, thus requiring extensive disarming before the entire system can be defeated. The alarms also signal the campus police (a branch of the Maryland State Police) to check the facility. Procedural requirements, such as the supervision of students during training sessions, appear to be sufficient to minimize risks during working hours.

The only SNM at the facility is stored in the reactor pool, either as stored fuel or in the reactor core. Radiation detectors at the bridge of the pool monitor radiation levels and would detect the increase in activity that would result from an attempt to remove fuel from the pool.

We observed that the security system relies to some degree on the mutual trust of the people who work at the facility. This human element is a part of any security system but seems to be more important here than at the AFFRI facility, for example. However, despite this dependence on people's trustworthiness, the detection system is quite thorough. It is ingeniously designed to provide general overlapping levels of protection at modest cost. Cleverness of design has eliminated the need for sophisticated and costly equipment.

We noted the following equipment in use at the facility:

- Simplex five-button combination locks
- "Best" cylinder locks
- Alarm system (manufactured by Luddeke Labs)
- Ademco contacts on doors, exhausts
- Ultrasonics (two kinds, no brand name)

Attitude of Staff

We interviewed only one member of the staff, but from his comments, it was evident that the staff feels the threat of theft or sabotage is extremely remote. Nonetheless, the general attitude towards intrusion detection and prevention is very positive. The 10 CFR 73.67 requirements are not considered a great burden on the facility. The staff member whom we interviewed felt that the University had anticipated many of the requirements of the new regulations. Thus, compliance would be merely a matter of completing some additional paperwork rather than purchasing new hardware.

UNIVERSITY OF VIRGINIA

The University of Virginia in Charlottesville operates two research reactors. The Cooperatively Assembled Virginia Low-Intensity Educational Reactor (CAVALIER) is a pool-type training facility with a power rating of 100 watts. The University of Virginia Reactor (UVAR) is a pool-type reactor with a power rating of 2 megawatts. This facility is a Class II facility and may be subject to the more stringent requirements of 10 CFR 73.60 in addition to those of 73.67(d). However, the university will maintain that it is not subject to 73.60 because the nuclear material is not readily separable from other radioactive material and is self-protecting.

Review of Security Plan

The University of Virginia's 1974 plan is less detailed and less stringent than the plan submitted by the University of Maryland. However, if the NRC accepts the University's contention that only the reactor pools and fuel storage room are controlled access areas, then the 1974 plan could be used as a basis for a new plan to meet the requirements of 10 CFR 73.67(d). If this definition of controlled access areas is accepted, the level of protection in the reactor room, for example, need not be increased. The plan offers no information on screening procedures before unescorted access is granted.

Observation of Security Practices

The presentation of the security system was somewhat vague, and the staff members who guided us on the tour explained that they could not show us all of the system's features for security reasons. As far as we could discern, physical security at the facility is minimal, consisting primarily of (1) a locked front door with electrical release, (2) a grilled metal door with an electrical interlock barring access to the reactor room, and (3) a wooden door (also with an electric interlock) behind the grilled metal door. These locked doors are all on the level of the larger (2 mega-watt) pool reactor. Access to the ground level of the facility, where the smaller (100-watt) CAVALIER reactor is located, is restricted only by minimal locks on overhead, garage-type doors. We saw no infra-red presence or motion detectors.

Approximately 100 individuals have access to the facility during working hours. Possession of keys is relatively uncontrolled - all 100 individuals have a key - but the facility's administrator recognizes the need for better key control.

The University of Virginia police (a branch of the Virginia State Police) are the first-response force for protection of the facility. Periodically, the police are invited to the facility so they will understand its security needs. They also patrol the area when making their rounds.

The security system does not depend heavily on protective equipment. We observed only the following devices:

- Simplex combination push-button locks on three doors
- Ademco contacts on same doors
- Locks (type unknown)

Attitude of Staff

The University of Virginia nuclear engineering staff feels that the SNM is self-protecting and very little additional security is needed. In fact, the University questioned the level of radiation established by the amendments as self-protecting as far back as the public comment period in 1978. They also feel protected by their isolation from the campus and the general lack of student interest in the facility. Because they see the threat of theft or sabotage as extremely small, the NRC requirements are taken as a sort of game in which you do the least possible while still gaining NRC approval. While the University does not "fight" the requirements, it is careful to commit itself to meeting only the intent of the regulations and no more. This attitude is common among power reactors but is not typical of research facilities. Unlike the University of Maryland's file, the University of Virginia's file is filled with requests for exemptions from certain requirements. These requests for exemptions were usually based on logical grounds and were generally granted, but this contentiousness indicates some reluctance to cooperate with NRC.

The facility personnel felt that they could meet Category II requirements by spending about $5,000 on equipment and revising a few procedures. This expenditure will not be a financial burden because they have funds from several outside research contracts. However, two years ago they would have been hard-pressed to meet the requirements and feel that many universities are in a similar position today. Although they felt the paperwork associated with preparing and filing a new PSP is substantial, the director of the facility is primarily an administrator rather than a teacher or researcher, and this paperwork is an accepted part of his job.

CONCLUSIONS

Although our sample is small (three licensees out of seventy-three), we feel it is representative of the spectrum of attitudes toward compliance that can be found among licensees. All felt that theft and sabotage are extremely unlikely and thus the new requirements are unnecessary; however, willingness to comply with the requirements varies considerably. As we suspected, the academic licensees interviewed find the requirements more burdensome than the government licensee whom we contacted. But even between the two universities there were differences in attitude. The University of Maryland is willingly complying with the requirements, complaining only slightly about the paperwork involved. The University of Virginia, on the other hand, is complying grudgingly with the regulations, looking for loop-holes and resisting whenever possible, in spite of the University's admission that it has the funds to purchase the additional equipment and implement new procedures.

The director of the University of Virginia facility warned that other universities not in Virginia's enviable financial position might close down their research reactors rather than try to raise funds to comply with the regulations. He further felt that a curtailment of research and education activities in the United States could be the unfortunate outcome of NRC's attempts to upgrade the physical security practices at these facilities.