APR 30 1984

DISTRIBUTION:
NMSS r/f
SGPR r/f
Case File
PStarcher
DKasun ✓
CGaskin
RSkelton
SBrown
RManili
TAllen
RDiggs

MEMORANDUM FOR: Kenneth P. Barr, Chief
Safeguards Branch, RII

FROM: George W. McCorkle, Chief
Power Reactor SG Licensing Branch
Division of Safeguards, NMSS

SUBJECT: RELAXATION OF ACCESS CONTROLS DURING EMERGENCY DRILLS

During the March 13, 1984 site visit to Catawba, several questions were raised regarding the relaxation of access controls for emergency vehicles and personnel during drills or exercises. The enclosure sets forth the current Headquarters staff position on this matter.

George W. McCorkle, Chief
Power Reactor SG Licensing Branch
Division of Safeguards, NMSS

Enclosure:
As stated

cc: J. Joyner, RI
W. Axelson, RIII
R. Hall, RIV
L. Norderhaug, RV
C. Thomas, NRR

CONTACT:
D. J. Kasun, NMSS
42-74383



A8

| OFFICE | SGPR | SGPR | SGPR | SGPR | SGPR | SGPR | SGPR |
|---|---|---|---|---|---|---|---|
| SURNAME | DKasun/cw | CGaskin | RSkelton | BManili | SBrown | TAllen | GMcCorkle |
| DATE | 4/30/84 | 4/30/84 | 4/30/84 | 4/30/84 | 4/30/84 | 4/30/84 | 5/2/84 |

NRC FORM 318 (10-80) NRCM 0240 OFFICIAL RECORD COPY ☆ U.S. GPO 1983—400-24

STAFF POSITION ON ACCESS CONTROLS
DURING EMERGENCY DRILLS OR EXERCISES APRIL , 1984

Background

The matter of protected area access for vehicles under emergency conditions (life threatening or plant safety related) is addressed in 10 CFR 73.55(d)(4). The general authority for departure from any security plan commitment when needed to protect the public health and safety (i.e., for safe operation of the reactor) is contained in 10 CFR 50.54(x) and (y). Various staff guidance documents have been prepared in support of these regulatory provisions. However, the subject of safeguards during emergency drills and exercises is not covered in any of the current security regulations and no staff position has been heretofore available to indicate what relaxations, if any, would be acceptable.

Staff Position

In regard to access into protected areas, it would seem reasonable to practice an operating procedure that is authorized by the regulations and which most likely would be put into use at some time. On the other hand, there should be no reduction in overall site protection in order to prevent the drill from being used as a means of penetrating the facilities perimeter safeguards. Accordingly, we conclude that during a pre-planned authorized drill or exercise the licensee may waive: (for the offsite emergency response forces)

- search of the emergency vehicles,
- search of the drivers and emergency response personnel,
- search of hand carried packages and equipment,
- badging and registration of the response personnel, and
- individual identification of the response personnel,

provided that:

- each vehicle is escorted by a member of the licensee's security organization equipped with two-way radio communication to the alarm stations,
- all response personnel remain within view of an escort at all times, and
- the licensee positively identifies at least one member of the response team who verfies that the other personnel are bona fide members of the responding organization.

In regard to access into vital areas, there is no regulatory authority for relaxation of controls during any non-emergency situation. Accordingly, the drill must stop at the vital boundary.

If it is considered necessary to familiarize the response team with plant layout (including vital areas), the full security plan measures must first be applied.

73.67(d)(1) Use the material only within a CAA which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.

1. USE OF SNM

Identify the CAA(s). Outline the CAA(s) on a floor diagram. All SNM must be used only within a Controlled Access Area (CAA) which is illuminated sufficiently to allow detection and surrveillance of unauthorized penetration or activities.

1.1 Isolation

Describe the physical barriers (i.e., fences, gates, free standing walls, building walls, locked doors, windows, etc.) which define the area within which SNM is being used. On the floor diagram identify the access doors into the CAA(s). Indicate if the CAA is Permanent or Temporary. Temporary CAA(s) should be established only when authorized personnel maintain continuous control over the SNM and supervision of the uses thereof.

1.2 Access

Describe how access into the CAA is controlled. Access control may be accomplished through the use of an appropriate combination of:

(a) An access control roster which identifies persons authorized to use the SNM and which has been validated by signature of the individual who has overall responsibility of the SNM;

(b) A system which controls and limits the distribution of keys, keycards, and/or combinations to locks on doors and gates which lead to a CAA;

(c) Personal recognition of individuals entering or within the CAA by an authorized individual;

(d) A badging system established at CAA access control points which identifies personnel authorized to use SNM within the CAA.

1.3 Illumination

Describe the illumination of the CAA. The CAA should have an illumination level which is sufficiently uniform and bright enough to detect unauthorized penetration or activities within the CAA. Generally, a minimum of 0.2 foot candles measured horizontally at ground level should be maintained.

A9

73.67(d)(2) Store the material only within a controlled access area such as a vault-type room or approved security cabinet or their equivalent which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.

## 2. STORAGE OF SNM

Describe the area where SNM is stored. Show the area(s) on the floor diagram.

### 2.1 Isolation

Describe the physical barriers which define the area within which SNM is stored. SNM must be stored in a vault-type room, approved security cabinet or the equivalent. On the floor diagram, identify access doors into the area.

### 2.2 Access

Describe how access into the area for storage is controlled. Access control may be accomplished by:

(a) An access roster which identifies persons authorized to have access to CAA's where SNM is stored and which has been validated by signature of the individual who has overall responsibility for the SNM; and

(b) A system which provides for limiting to authorized individuals the distribution of keys, keycards, and/or combinations to locks on doors and gates leading to the CAA.

### 2.3 Illumination

Describe the illumination of the area where SNM is to be stored. The area should have an illumination level which is sufficiently uniform and bright enough to detect unauthorized penetration or activities within the area. Generally, a minimum of 0.2 foot candles measured horizontally at ground level should be maintained.

73.67(d)(3) Monitor with an intrusion alarm or other device or procedures the CAA to detect unauthorized penetration or activities.

## 3. DETECTION

### 3.1 Intrusion Detection

Describe the intrusion detection system. The intrusion detection system may include but is not limited to:

(a) Motion detection system for CAAs or portions of CAAs; or

(b) Perimeter detection systems at the CAA boundaries.

In the description of each system indicate:

(a) if the system is line supervised (open, short, loss of power) and/or tamper indicating;

(b) if there is an emergency power source;

(c) if there is a weekly testing program.

Describe when the system is in service, how the system is turned on and off, and who is responsible for turning the system on and off. Indicate where the system alarms.

Describe any other devices which are not normally considered security related systems which are employed. Such a device may consist of radiation detectors which could be used to detect unauthorized removal of irradiated SNM from a facility.

### 3.2 Procedures

Describe procedures which are used to detect theft of SNM. Procedures should include the following:

(a) Directing authorized individuals to be aware of unauthorized persons in their work areas, and to report the presence of such persons to supervisory or security personnel;

(b) Escorting of unscreened persons (visitors) within the CAA;

(c) Surveillance (e.g., escorting) or inspection of non-licensee vehicles capable of transporting large quantities of SNM away from the site;

(d) Continuous or periodic surveillance of the CAA, or a given portion of the CAA by designated supervisory or other authorized individuals or by CCTV;

(e) Random exit searches of packages.

Other procedures may include but are not limited to:

(a) Administrative control of materials removed from the CAA;

(b) Frequent inventories of SNM;

(c) Periodic inspections to confirm continued integrity of barriers, gates, loading bay doors, etc., through which unauthorized removal of SNM could be effected.

Indicate if periodic patrols are made by watchman of CAA perimeters and areas. If so, indicate how often.

73.67(d)(4) Conduct screening prior to granting an individual unescorted access to the CAA where the material is used or stored, in order to obtain information on which to base a decision to permit such access.

## 4. PREAUTHORIZATION SCREENING

All personnel granted unescorted access (authorized individuals) to the CAA shall be screened.

### 4.1 Screening

Describe the measures taken to determine the trustworthiness and reliability of an individual before granting them unescorted access to CAA(s) where SNM is used or stored. Indicate who is responsible for this determination.

Unescorted access is usually granted by a member of the Facility Management such as the Facility Director. Unescorted access is based on an individual's need for access and a favorable review of information obtained on the individual for trustworthiness and reliability. For Facility Staff/Students (US Citizens) this should be done by selecting two of the three measures identifies below:

(1) Examination of past employment and education records;

(2) Endorsements or references from previous employers;

(3) Consideration of the individual's present employment record.

For Foreign Students:

(1) Admissions file, and

(2) Academic records for last one year, if available, and

(3) Personal reference letters from two nonrelated individuals, if possible.

The Facility Director may authorize the following individuals unescorted access to the CAA without review of the above information:

(1) Facility Staff/Students granted unescorted access to the facility for at least the previous one year prior to the implementation of this security plan.

(2) Facility Staff/Students holding or having held a government sanctioned clearance within the last one year.

It should be noted that the screening process should be consistent with local, state, and federal laws and regulations regarding the protection of the privacy and other rights of the individual.

73.67(d)(5) Develop and maintain a controlled badging and lock system to identify and limit access to the CAA to authorized individuals.

## 5. BADGING AND LOCK SYSTEMS

### 5.1 Badging

Describe the badging system used to identify individuals having unescorted access (authorized individuals). The badging system should utilize a personalized badge, or a badge displaying some other personal characteristic which identifies an individual (e.g., signature, etc.).

Describe how the badges are used in controlling access into the CAA.

Describe an accountability and control program for the badges. Identify the individual responsible for monitoring the issuances of badges. Indicate how often badges are inventoried. Give procedures for dealing with lost and forgotten badges.

### 5.2 Locks

Describe the lock system used to control access into the CAA and into storage areas. The lock system may consist of:

(a) 3 or 4 position dial-type or cipher combination locks
(b) six-pin tumbler key locks
(c) card-key lock system
(d) a combination of the above

Describe the control and accountability program for the keys/combination. This program should:

1. ensure that only authorized individuals have access to keys/combinations;
2. indicate who is responsible for monitoring the issuance of keys and combinations;
3. ensure that spare keys are secured;
4. indicate when and under what conditions key/combinations are changed.

73.67(d)(7) Assure that all visitors to the CAA are under the constant escort of an individual who has been authorized access to the area.

## 7. VISITORS

### 7.1 Visitor Access Determination

Indicate who is responsible for determining visitor need for temporary access to the CAA.

### 7.2 Escort

Indicate who is authorized to escort visitors within the CAA. All visitors (individuals with escorted access) should be escorted by authorized individuals (individuals with unescorted access). Describe the responsibilities of the escort. Escorts should have constant control and surveillance of visitors within the CAA Indicate the ratio of visitor to escort. This ratio should not be more than 15 to 1.

73.67(d)(8) Establish a security organization or modify the current security organization to consist at least one watchman per shift able to assess and respond to any unauthorized penetrations or activities in the CAA.

## 8. SECURITY ORGANIZATION

### 8.1 Response Organization

Describe the security organization that will be responsible for assessing and responding to security incidents. In this description:

(1) indicate who the immediate response force will be;
(2) indicate who is responsible for notifying the response force for both working and non-working hours. The senior authorized individual at the facility is usually responsible during working hours. If, during non-working hours, an intrusion detection system is used, indicate where the system alarms and assure that the system is monitored and can be responded to at all times;
(3) indicate who is to be notified (management, campus police, local law enforcement agency, NRC, etc.).

### 8.2 Local Law Enforcement Agency (LLEA)

Identify the LLEA. Describe any training or familiarization of security the LLea has with the facility.

### 8.3 Training

Describe any training with regard to security procedures and facility familiarization given to authorized individuals or campus police. Authorized individuals and campus police should be familiar with security procedures and the facility physical layout.

73.67(d)(9) Provide a communication capability between the security organization and appropriate response force

9. COMMUNICATIONS

Describe the communication capability between the security organization and the appropriate response force. In this description, inciate the type of system used, the reliability of the system, the accessibility of the system and the testing program of the system. A duplex voice communication system should be used. The system should be accessible on a 24 hour basis and tested weekly. Commercial telephone is acceptable if procedures assure availability of an alternate.

73.67(d)(10) Search on a random basis vehicles and packages leaving the CAA.

10. SEARCH

Give the ratio for conducting searches for both packages and vehicles. Searches should be conducted to include at least 1 out of every 5 for both packages and vehicles.

Describe the type of search to be performed for both packages and vehicles. Vehicle searches should include a general examination of the vehicles's compartment, the cargo area and the undercarriage. Searches of packages should include packages that equal or exceed the size of the SNM being used or stored, which are removed from the CAA by other than authorized individuals. Searches of packages may involve opening the packages and may be conducted by the use of appropriate instrumentation (e.g., radiation detectors, metal detectors, etc.). Packages entering the CAA should be restricted to those carried by or under the supervision of an authorized individual(s).

Specify who will conduct searches. Searches should be conducted by authorized individuals or other specifically designated personnel.

73.67(d)(11) Establish and maintain response procedures for dealing with threats of thefts and thefts of such material.

11. RESPONSE PROCEDURES

Identify which security events response procedures have been developed for. Response procedures should be developed for the following events:

(1) Situation that could possibly lead to theft of SNM (e.g., civil disturbance, fire, intrusion alarm annunication, etc.);

(2) Discovery that the security system has been breached; and

(3) Discovery that SNM is missing.

Describe the response procedures or describe what is contained in the response procedures concerning the response for each event:

(1) the duties and responsibilities of the response organization;

(2) designation of command and control functions between onsite and offsite forces;

(3) the duties and responsibilities of the management involved in the response.

Assure that the NRC shall be notified in accordance with 10 CFR 73.71.

Describe what local law enforcement assistance is available. Describe the response capabilities, includeing number of officers, and response time. Describe any agreements between the facility and the local law enforcement agency.