



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

AB46-1

MAY 08 1985

MEMORANDUM FOR: Victor Stello, Jr., Deputy Executive Director  
Regional Operations and Generic Requirements

FROM: Robert F. Burnett, Director  
Division of Safeguards, NMSS

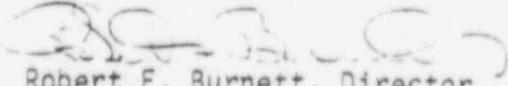
SUBJECT: CATEGORIZATION AND REPORTING OF EVENTS (10 CFR 73.71)

Please recall that a number of points were raised by the CRGR during the April 17, 1985 meeting which considered our proposed revision to 10 CFR 73.71. We have considered your suggestions and believe they will result in eliminating ambiguities and providing more meaningful guidance for implementing the provisions of the rule. Enclosure 1 proposes clarification to the examples listed in the proposed guidance for events to be reported within one hour and events to be logged.

We have also developed a chart (Enclosure 2) which provides a comparison of requirements for reporting of events under the present and proposed rules. This may answer some of the questions you raised concerning just what is and what isn't reportable.

Concern was also expressed that our proposed requirements for the reporting of lost or stolen badges would place an undue burden on licensees. We have surveyed the regions and find that only a negligible number of access badges which are not properly compensated (reportable) have occurred. See Enclosure 3 for the results of this survey.

Please let me know if any further information is needed prior to your further action on the proposed rule.

  
Robert F. Burnett, Director  
Division of Safeguards, NMSS

Enclosures:  
(3), as stated

cc: W. Schwink, DEDROGR Staff  
w/encls. (15 copies)

8510180330 851009  
PDR PR  
73 50FR34708 PDR

COMPARISON WITH CURRENT ONE HOUR REPORT

ONE HOUR REPORTS (CURRENT)	ONE HOUR REPORTS (PROPOSED)	LOG ONLY (PROPOSED)
a. Attempted or confirmed intrusions at vital, material access, protected, or controlled access areas.	(1) Purposefully attempted or confirmed intrusions into protected areas, material access areas, controlled access areas or vital areas. This includes tailgating by employees/contractors to gain access to an area to which they are not authorized. (Note: Any unauthorized entry through a required barrier must always be reported within one hour whether or not the breach has been properly compensated.)	(7) Tailgating by licensee employee/contractor to gain access to an area that he or she is authorized to be in.
b. Attempted intrusions into protected area by protesting groups.		
c. Discovery of or attempted introduction of unauthorized weapons, explosives, or incendiary devices inside the protected or controlled access areas./1	(2) Discovery of the actual or attempted introduction or possession of unauthorized weapons, explosives, or incendiary devices into or within the protected area, controlled access areas, material access areas, or vital areas.	
d. Bomb threats or extortion threats./1	(3) Substantiated bomb or extortion threats. In addition a telephonic follow-up report of the results of a bomb search should be made within one hour of completion. Unsubstantiated bomb threats need not be immediately reported unless a specific organization or group claims responsibility; in this case the threat must be reported within one hour.	(12) Unsubstantiated bomb or extortion threats received from individuals.
e. Mass demonstrations, picketing, or other job actions at the plant site./1	(19) Mass demonstration at plant site that may pose a threat to the facility.	
f. Civil disturbances near the plant site./1	(20) Civil disturbance within one mile of plant site that may pose a threat to the facility.	
g. Loss of both central and secondary alarm stations./2	(13) Uncompensated loss of both central and secondary alarm station ability to monitor or remotely assess alarms, or communicate with off site sources.	(3) Loss of a single alarm station ability to monitor or remotely assess alarms, but dual offsite communication capability remains.
h. Loss of all capability for offsite communication to the local law enforcement agency./2	(16) Complete loss of offsite communications. The licensee should report the complete loss of offsite communications within one hour if possible or immediately after restoration of communications. If communications to off-site are lost and cannot be restored within an hour, then the licensee should use communications located offsite to notify the NRC.	(8) Loss of intra-convoy communications ability.

1 These events should be evaluated and reported in accordance with contingency plans. If the threat is more potential in character than explicit, it can be reported within 24 hours from the time it has been estimated to be in existence.

2 These events do not have to be reported within one hour if properly compensated for in a timely manner; however, they have to be reported within 24 hours.

ONE HOUR REPORTS (con't)  
(CURRENT)

ONE HOUR REPORTS (con't)  
(PROPOSED)

LOG ONLY (con't)  
(PROPOSED)

i. Loss or degradation of power for the physical security system (below that level required to keep the security system operating at rated capacity)./2

(15) Uncompensated loss of all electrical power supply to security systems that would allow unauthorized or undetected access.

(11) Properly compensated loss of all electrical power supply to security systems that if uncompensated would allow unauthorized or undetected access.

j. Failure or loss of operability of any alarm or intrusion detection system or portion thereof that could be directly exploited to allow undetected access to vital or material access areas such as  
(1) card reader access control system malfunction so that unauthorized personnel could gain access to vital areas or  
(2) simultaneous failure of vital or material access area intrusion detection and threat assessment equipment./2

(6) Discovery of intentionally falsified identification badges or key cards

(7) Discovery of uncompensated and unaccounted for, lost or stolen key cards, ID card blanks, keys, or any access device that could allow unauthorized or undetected access to protected areas, material access areas, controlled access areas, or vital area if use of MRC approved facility procedures cannot account for the loss.

(17) Uncompensated loss of a single intrusion detection system zone.

(18) Member of security force found asleep at post.

(1) Properly compensated security computer failures or security computer failures that do not assist in allowing unescorted or undetected access.

(2) Properly compensated card reader failures.

(4) CCTV camera failure in a single zone if intrusion detection system remains operational.

(5) Failure of a single perimeter lighting zone if intrusion detection system remains operational.

(6) Properly compensated loss of a single intrusion detection system zone.

k. Unavailability of minimum number of security personnel./2

(14) Unavailability of minimum number of security personnel or an actual or imminent strike by the security force.

1 These events should be evaluated and reported in accordance with contingency plans. If the threat is more potential in character than explicit, it can be reported within 24 hours from the time it has been estimated to be in existence.

2 These events do not have to be reported within one hour if properly compensated for in a timely manner; however, they have to be reported within 24 hours.

AB46-1

COMPARISON WITH CURRENT 24 HOUR REPORT

24 HOUR REPORT (CURRENT)	ONE HOUR REPORT (PROPOSED)	LOG ONLY (PROPOSED)
a. Theft of security weapon at the site.		(14) Theft of security weapon at the site.
b. Confirmed tampering with security equipment.	(22) Confirmed security equipment tampering of suspicious origin.	(13) Confirmed security equipment tampering of non-suspicious origin.
c. Discovery of spurious identification badges, key cards, or security locks and keys.	(6) See #6 under one hour report.  (7) See #7 under one hour report	(10) Properly compensated accidental removal offsite or loss of badge by employee, i.e., badge is promptly cancelled, or use of NRC-approved procedures account for the loss.
d. Theft of documents containing proprietary or classified security information.	(9) Theft or loss of classified documents pertaining to facility or transport safeguards. (Note: Also reportable under 10 CFR 95.57.)  (21) Compromise of safeguards information (including loss or theft) which would significantly assist an individual in an act of radiological sabotage or theft of special nuclear material.	
e. Unexplained fire or explosion within the isolation zone, protected area, or controlled access area that could affect plant security.	(10) Fire or explosion of suspicious or unknown origin within the isolation zone, protected area, material access area, controlled access area, or vital area.	
f. Sudden retirement, discharge, or resignation of key security personnel if the event results in a moderate loss of physical security effectiveness./3		
g. Security-related injury to a member of the security organization such as that caused by malfunctioning security equipment.		
h. Sickouts or other labor problems affecting the readiness of the security forces.	(14) See #14 under one hour report.	

3 These events do not have to be reported if properly compensated for in a timely manner; however, they do have to be recorded in the licensee's records.

AB46-1

24 HOUR REPORT (con't) (CURRENT)	ONE HOUR REPORT (con't) (PROPOSED)	LOG ONLY (con't) (PROPOSED)
i. Any event that reduces the capability for offsite communication to the local law enforcement agencies. (This would not include loss of service of any one regular telephone, even from an alarm station. However, it would include loss or malfunction of an alarm station radio or hotline equipment./3	See #13 under one hour report  See #16 under one hour report	(3) Loss of a single alarm station ability to monitor or remotely assess alarms, but dual offsite communication capability remains.  See #8 under log only
j. Failure or loss of operability of any alarm or intrusion detection system or portion thereof that could be directly exploited to allow undetected access to the protected area such as (1) simultaneous failure of any one perimeter intrusion alarm segment and threat assessment equipment or (2) undetected failure of any one perimeter intrusion alarm segment./1	See #6 under one hour report See #7 under one hour report  See #17 under one hour report See #18 under one hour report	See #1 under log only See #2 under log only  See #4 under log only See #5 under log only See #6 under log only
k. Failure of perimeter lighting to an extent that would impair threat assessment./3		See #5 under log only
l. Loss of either the central or secondary alarm station./3	See #13 under one hour report	See #3 under log only
m. Number of guards at transfer points of a shipment fewer than that required by the regulation or security plan./3	See #14 under one hour report	

3 These events do not have to be reported if properly compensated for in a timely manner; however, they do have to be recorded in the licensee's records.

AB46-1

24 HOUR REPORT (con't)  
(CURRENT)

ONE HOUR REPORT (con't)  
(PROPOSED)

n. Unexplainable security situations impeding the effectiveness of security to the limit defined in the physical security plan.

(5) Discovery of a criminal act involving licensee personnel or contractors with the potential to impact facility operation or an individual's trustworthiness or reliability in the nuclear setting (i.e., discovery of a conspiracy to bomb the facility or disturb its vital components, falsification of background screening certificates, etc.)

(11) Discovery of a suspicious vehicle following a licensed carrier transporting SSNM.

(12) Mechanical breakdown of transport vehicle carrying SSNM.

(4) Uncompensated suspension of safeguards controls during emergency conditions which could allow undetected and unauthorized access.

3 These events do not have to be reported if properly compensated for in a timely manner; however, they do have to be recorded in the licensee's records.

PROPOSED REVISIONS TO GUIDANCE

II. g. Examples of Safeguards Events That Should be Reported Within One Hour

- (1) Attempted or confirmed intrusions into protected areas, material access areas, controlled access areas or vital areas. This includes tailgating by employees/contractors to gain access to an area to which they are not authorized. (Note: Any unauthorized entry through a required barrier must always be reported within one hour whether or not the breach has been properly compensated.)

Clarification:

- (1) Purposefully attempted or confirmed intrusions into protected areas, material access areas, controlled access areas or vital areas. This includes tailgating by employees/contractors to gain access to an area to which they are not authorized. (Note: Any unauthorized entry through a required barrier must always be reported within one hour whether or not the breach has been properly compensated.)
- (2) Discovery of an introduction or attempted introduction of unauthorized weapons, explosives, or incendiary devices into the protected area, controlled access areas, material access areas, or vital areas.

Clarification:

- (2) Discovery of the actual or attempted introduction or possession of unauthorized weapons, explosives, or incendiary devices into or within the protected area, controlled access areas, material access areas, or vital areas.
- (3) Credible bomb threats or extortion threats. In addition, a telephonic follow-up report of the results of a bomb search should be made within one hour of completion. If a bomb threat is made where evidence suggests that it is not credible, it need not be reported.

Clarification:

- (3) Substantiated bomb or extortion threats. In addition a telephonic follow-up report of the results of a bomb search should be made within one hour of completion. Unsubstantiated bomb threats need not be immediately reported unless a specific organization or group claims responsibility; in this case the threat must be reported within one hour.
- (4) Uncompensated suspension of safeguards controls during emergency conditions which could allow undetected or unauthorized access.

Clarification:

- (4) Uncompensated suspension of safeguards controls during emergency conditions which could allow undetected or unauthorized access. (Note: Events reportable under 10 CFR 50.72 do not require duplicate reports under 10 CFR 73.71.)
- (5) Discovery of a criminal act involving licensee personnel or contractors (e.g. discovery of a conspiracy to bomb the facility or disturb its vital components, falsification of background screening certificates, etc.)

Clarification:

- (5) Discovery of a criminal act involving licensee personnel or contractors with the potential to impact facility operation or an individual's trustworthiness or reliability in the nuclear setting (i.e., discovery of a conspiracy to bomb the facility or disturb its vital components, falsification of background screening certificates, etc.)

(6) Discovery of falsified identification badges, key cards and keys.

Clarification:

(6) Discovery of intentionally falsified identification badges or key cards.

(7) Discovery of unaccounted for or unassigned key cards, and ID card blanks, keys and lock sets, or any access device that could allow unauthorized and undetected access to protected areas, material access areas, controlled access areas, or vital areas if not properly compensated.

Clarification:

(7) Discovery of uncompensated and unaccounted for, lost, or stolen key cards, ID card blanks, keys, or any access device that could allow unauthorized or undetected access to protected areas, material access areas, controlled access areas, or vital area if use of NRC approved facility procedures cannot account for the loss.

(8) Theft or loss of documents containing Safeguards Information.

Clarification: Delete, see item (21)

(9) Theft or loss of classified documents pertaining to facility or transport safeguards. (Note: Also reportable under 10 CFR 95.97.)

Clarification: None

(10) Fire or explosion of suspicious or unknown origin within the isolation zone, protected area, material access area, controlled access area, or vital area.

Clarification:

(10) Fire or explosion of suspicious or unknown origin within the isolation zone, protected area, material access area, controlled access area, or vital area. (Note: Events reportable under 10 CFR 50.72 do not require duplicate reports under 10 CFR 73.71.)

(11) Discovery of a suspicious vehicle following a licensed carrier.

Clarification:

(11) Discovery of a suspicious vehicle following a licensed carrier transporting SSNM.

(12) Mechanical breakdown of transport vehicle carrying SSNM.

Clarification: None

(13) Uncompensated loss of both central and secondary alarm station ability to monitor or remotely assess alarms, or communicate with offsite sources.

Clarification: None

(14) Unavailability of minimum number of security personnel or an actual or imminent strike by the security force.

Clarification: None

(15) Uncompensated loss of all electrical power supply to security systems that would allow unauthorized or undetected access.

Clarification: None

- (16) Complete loss of offsite communications. The licensee should report the complete loss of offsite communications within one hour if possible or immediately after restoration of communications. If communications to offsite are lost and cannot be restored within an hour, then the licensee should use communications located offsite to notify the NRC.

Clarification: None

- (17) Uncompensated loss of a single intrusion detection system zone.

Clarification: None

- (18) Member of security force found asleep at post, uncompensated.

Clarification:

- (18) Member of security force found asleep at post.

- (19) Mass demonstration at plant site.

Clarification:

- (19) Mass demonstration at plant site that may pose a threat to the facility.

- (20) Civil disturbance within one mile of plant site if it is a threat to the facility.

Clarification:

- (20) Civil disturbance within one mile of plant site that may pose a threat to the facility.

- (21) Compromise of safeguards information which would significantly assist an individual in an act of radiological sabotage or theft of special nuclear material.

Clarification:

- (21) Compromise of safeguards information (including loss or theft) which would significantly assist an individual in an act of radiological sabotage or theft of special nuclear material.

Add:

- (22) Confirmed security equipment tampering of suspicious origin.

III. c. Examples of Events Required to be Recorded in the Licensee's Log (p. 10)

- (1) Security computer failures that do not assist in allowing unauthorized or undetected access, or are properly compensated

Clarification:

- (1) Properly compensated security computer failures or security computer failures that do not assist in allowing unescorted or undetected access.

- (2) Card reader failures that have been properly compensated.

Clarification:

- (2) Properly compensated card reader failures.

- (3) Loss of a single alarm station capability to monitor or remotely assess alarms but dual offsite communication capability remains.

Clarification: None

- (4) CCTV camera failure in a single zone if intrusion detection system remains operational.

Clarification: None

- (5) Failure of a single perimeter lighting zone if intrusion detection system remains operational.

Clarification: None

- (6) Loss of a single intrusion detection system zone that has been properly compensated.

Clarification:

- (6) Properly compensated loss of a single intrusion detection system zone.

- (7) Tailgating by a licensee employee/contractor to gain access to an area that he or she is authorized to be in.

Clarification: None

- (8) Loss of inter-convoy communications ability.

Clarification:

- (8) Loss of intra-convoy communications ability.

- (9) Compromise of safeguards information which would not significantly assist an individual in an act of radiological sabotage or theft of special nuclear material.

Clarification: Delete

- (10) Accidental removal offsite or loss of badge by employee, if badge is promptly cancelled.

Clarification:

- (10) Properly compensated accidental removal offsite or loss of badge by employee, i.e., badge is promptly cancelled, or use of NRC-approved procedures account for the loss.

Add:

- (11) Properly compensated loss of all electrical power supply to security systems that if uncompensated would allow unauthorized or undetected access.

Add:

- (12) Unsubstantiated bomb or extortion threats received from individuals.

Add:

- (13) Confirmed security equipment tampering of non-suspicious origin.

Add:

- (14) Theft of security weapon at the site.

Summary of Regional Comment Re: Lost/Stolen Access Badges

The vast majority of access badges do not leave the facility. In all the Regions, only one facility was noted as allowing access badges to be taken off site.

The number of badges granting access to the PA or VA lost or stolen annually without proper compensation is extremely low.

The consensus of Regional comment indicates that if an access badge is lost or stolen and not properly compensated then it should be reported to the NRC within one hour.

Other than the regulation, few regional guidelines exist on the reporting of an uncompensated lost or stolen badge because of the infrequency of the event. Lost or stolen access badges that are properly compensated are logged.

AB46-1

REGION SURVEY RE: LOST/STOLEN ACCESS BADGES

CONTACT: Region I

DATE: April 19, 1985

1. Do any utilities that use picture ID badges for access to the PA or VA allow the badges to leave the site?

Badges for PA or VA access do not leave the site. In some cases an owner controlled access card is allowed to leave the site. This card is surrendered prior to entering the PA and replaced with PA or PA/VA access cards and/or key cards.

2. On average, how many badges granting access to the PA are lost or stolen annually without being properly compensated?

Uncompensated loss extremely infrequent, cannot recall an instance of this.

3. On average, how many badges granting access to a VA are lost or stolen annually without being properly compensated?

See #2.

4. What is your view on the present requirement for a licensee to report an uncompensated lost or stolen badge that could allow unauthorized or undetected access to the PA or VA?

Situation where employee with PA access only picks up lost VA badge within a facility is troublesome. Some utilities use cipher codes in addition to access cards; this would counter unauthorized use of VA access card. Missing badge would be reported at end of shift when individual who lost card attempted to leave facility. At this time the badge could be properly compensated.

5. What guidelines are used by the Regions to counsel licensees on whether or not to report an uncompensated for lost or stolen badge?

Situation does not occur where a lost or stolen badge is not properly compensated. Noted one event at Beaver Valley where a badge was found (no details whether it had been stolen or lost.) The licensee implemented compensatory measures, logged the event and reported event to Regional Office.

REGION SURVEY RE: LOST/STOLEN ACCESS BADGES

CONTACT: Region II

DATE: April 19, 1985

1. Do any utilities that use picture ID badges for access to the PA or VA allow the badges to leave the site?

Yes, one - B&W Navy allows access badges to go home with employees.

2. On average, how many badges granting access to the PA are lost or stolen annually without being properly compensated?

Some utilities do not lose any because people are posted at exit points with the purpose of collecting badges. Some, like TVA, have problems. Estimate <12 per day "misplaced" in RII. Amount lost or stolen infinitesimal. For site with worst access controls, May-six badges taken offsite, June-one, July-3.

3. On average, how many badges granting access to a VA are lost or stolen annually without being properly compensated?

See #2, one badge is used for PA/VA entrance.

4. What is your view on the present requirement for a licensee to report an uncompensated lost or stolen badge that could allow unauthorized or undetected access to the PA or VA?

Cannot think of any example where this would occur and not be properly compensated. If it did occur would worry more about why the licensee could not properly compensate than the lost badge. Thinks this should be reported within one hour.

5. What guidelines are used by the Regions to counsel licensees on whether or not to report an uncompensated for lost or stolen badge?

Log in daily journal if properly compensated.

REGION SURVEY RE: LOST/STOLEN ACCESS BADGES

CONTACT: Region III

DATE: April 19, 1985

1. Do any utilities that use picture ID badges for access to the PA or VA allow the badges to leave the site?

No

2. On average, how many badges granting access to the PA are lost or stolen annually without being properly compensated?

Maybe 10's, not 100's.

3. On average, how many badges granting access to a VA are lost or stolen annually without being properly compensated?

See #2, number above includes PA's/VA's.

4. What is your view on the present requirement for a licensee to report an uncompensated lost or stolen badge that could allow unauthorized or undetected access to the PA or VA?

Would be concerned if individual w/PA access only picked up a lost VA badge and attempted to enter VA, this should be immediately reported. Also, agrees w/Region II, that if lost/stolen badge cannot be properly compensated, this is an indication of a problem that should be reported immediately.

5. What guidelines are used by the Regions to counsel licensees on whether or not to report an uncompensated for lost or stolen badge?

Most cases involve a dropped or misplaced badge within the PA which is returned to security immediately when found. Badges lost/stolen that are not found are properly compensated for through computerized access controls. If a lost/stolen badge cannot be properly compensated it should be reported immediately. Knows of no examples of this situation, but feels example should be in guidance if situation does occur.

AB46-1

REGION SURVEY RE: LOST/STOLEN ACCESS BADGES

CONTACT: Region IV

DATE: April 19, 1985

1. Do any utilities that use picture ID badges for access to the PA or VA allow the badges to leave the site?

No, all have recall system where badge is recalled at end of shift. If card is not surrendered at end of shift, individual is paged. If no response is received, individual is called at home. If individual refuses to cooperate, he or she is visited by member of security.

2. On average, how many badges granting access to the PA are lost or stolen annually without being properly compensated?

Minimal number

3. On average, how many badges granting access to a VA are lost or stolen annually without being properly compensated?

See #2 above

4. What is your view on the present requirement for a licensee to report an uncompensated lost or stolen badge that could allow unauthorized or undetected access to the PA or VA?

Lost or stolen badges are not a problem because of infrequency of event. If a badge is accidentally removed from site it has not been logged out on the computer system. Attempted use of the badge to gain PA entrance will cause an alarm. If a badge is lost or stolen and proper compensatory measures are not affected, then the event should be immediately reported to NRC.

5. What guidelines are used by the Regions to counsel licensees on whether or not to report an uncompensated for lost or stolen badge?

Cannot remember situation ever occurring where lost/stolen access badge was not properly compensated for. Feels bigger problem is lost NRC badges that could be used to gain licensee facility access.

AB46-1

REGION SURVEY RE: LOST/STOLEN ACCESS BADGES

CONTACT: Region V

DATE: April 19, 1985

1. Do any utilities that use picture I.D. badges for access to the PA or VA allow the badges to leave the site?

No

2. On average, how many badges granting access to the PA are lost or stolen annually without being properly compensated?

Could not provide a number because it is not a problem.

3. On average, how many badges granting access to a VA are lost or stolen annually without being properly compensated?

See above.

4. What is your view on the present requirement for a licensee to report an uncompensated lost or stolen badge that could allow unauthorized or undetected access to the PA or VA?

Cannot think of example of situation over past eight years. Facilities have computerized access controls that allow for immediate compensation of lost or stolen badge.

5. What guidelines are used by the Regions to counsel licensees on whether or not to report an uncompensated for lost or stolen badge?

Knows of no guidelines because situation does not exist. Lost/stolen badges are immediately compensated for, then noted in log.

7/5/85

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

JUL 3 1985



AB46-1  
1. Davis  
2. Hauschild  
CC: SG

MEMORANDUM FOR: John G. Davis, Director  
Office of Nuclear Material Safety and Safeguards

FROM: Victor Stello, Jr., Chairman  
Committee to Review Generic Requirements

SUBJECT: CRGR REVIEW OF NMSS PROPOSAL TO REVISE SAFEGUARDS  
EVENT REPORTING

*mine*  
*Dwyer*

At CRGR Meeting No. 74, R. Burnett (NMSS) presented for CRGR review, a proposal to revise NRC reporting and recordkeeping requirements and guidance concerning safeguards events. In summary, the CRGR recommended that the proposal be modified to incorporate clarifications and reviewed by the staff to assure that both immediate and other reporting of safeguards events are necessary and timely. Furthermore, Mr. Burnett stated that he would promptly examine the matter concerning badge loss and report his findings to the CRGR. After consideration of the findings of such a review and examination, the Committee was to decide whether further CRGR consideration of the proposal is necessary.

In a May 8, 1985 memorandum to me, Mr. Burnett enclosed his review and examination findings along with proposed modifications to the Regulatory Guide Revision which was reviewed at CRGR Meeting No. 74. The CRGR has considered Mr. Burnett's findings and proposed modifications and decided that further CRGR consideration of this matter at this time is not necessary.

*Victor Stello, Jr.*  
Victor Stello, Jr., Chairman  
Committee to Review Generic  
Requirements

cc: SECY  
Commission (5)  
W. J. Dircks  
Office Directors  
Regional Administrators  
CRGR Members  
G. Cunningham  
R. Burnett

~~8507120079~~ 18