NUREG-1304

Reporting of Safeguards Events

U.S. Nuclear Regulatory Commission

Office of Nuclear Reactor Regulation

P.A. Dwyer, N.E. Ervin

NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082, Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations,* and *Nuclear Regulatory Commission Issuances.*

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Information Support Services, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG-1304

Reporting of Safeguards Events

Manuscript Completed: February 1988
Date Published: February 1988

P.A. Dwyer, N.E. Ervin

Division of Reactor Inspection and Safeguards
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

ABSTRACT

On June 9, 1987, the Commission published in the Federal Register a final rule revising the reporting requirements for safeguards events. Safeguards events include actual or attempted theft of special nuclear material (SNM); actual or attempted acts or events which interrupt normal operations at power reactors due to unauthorized use of or tampering with machinery, components, or controls; certain threats made against facilities possessing SNM; and safeguards system failures impacting the effectiveness of the system. The revised rule was effective October 8, 1987. On September 14, 1987, the NRC held a workshop in Bethesda, MD to answer affected licensees' questions on the final rule. This report documents questions discussed at the September 14 meeting, reflects a completed staff review of the answers, and supersedes previous oral comment on the topics covered. Answers that have been revised are identified by an asterisk next to the question number. After additional experience is gained under the new reporting regulations in 10 CFR 73.71, the NRC staff also intends to revise its formal guidance in Regulatory Guide 5.62, as appropriate.

CONTENTS

1.0 INTRODUCTION

On September 14, 1987, the NRC staff conducted a workshop to respond to affected licensees' questions on revisions to 10 CFR 73.71, "Reporting Requirements for Safeguards Events", published on June 9, 1987 (52 FR 21651), effective on October 8, 1987. Many questions were also directed at the rule's supporting regulatory guide, Regulatory Guide 5.62, "Reporting of Safeguards Events", Rev. 1.

This report documents questions discussed at the September 14 meeting, reflects a completed staff review of the answers, and supersedes previous oral comment on the topics covered. Answers that have been revised are identified by an asterisk next the the question number. After additional experience is gained under the new reporting regulations in 10 CFR 73.71, the NRC staff also intends to revise its formal guidance in Regulatory Guide 5.62, as appropriate. The organization of this report is based on Sections 2.2 and 2.4 of Regulatory Guide 5.62; questions and responses are grouped under either "General" categories or appropriate regulatory guide examples of items to be reported or logged.

2.0 Reportable Events (General)

Q. 2.0.1. If a report is made under 10 CFR 50.72 or 10 CFR 50.73 for an event that is also reportable under 10 CFR 73.71, is a duplicate report required under 10 CFR 73.71?

A. No.

*Q. 2.0.2. If a report is made under 10 CFR 73.71 for an event that is also reportable under 10 CFR 50.72 or 50.73, is a duplicate report under 10 CFR 50.72 or 50.73 required to be made?

A. No. Duplicate reports are not required.

*Q. 2.0.3. Does guidance found in a regulatory guide supersede approved security plan commitments?

A. No.

Q. 2.0.4. Must plan amendments be submitted which commit to implement the revised 10 CFR 73.71?

A. No. However, if certain provisions in licensees' plans are no longer authorized under the new 73.71 rule, licensees should make conforming revisions to their plans through 10 CFR 50.54(p) or 10 CFR 70.32(e) changes, as appropriate.

Q. 2.0.5. Is there a relationship between the safeguards severity levels in Appendix C to 10 CFR Part 2 and the revised 10 CFR 73.71?

A. No. However, the staff did attempt to ensure consistency in philosophy.

2.1 Safeguards Events To Be Reported Within One Hour (General)

Q. 2.1.1. Can a one hour report be converted to a log item if a licensee erroneously reports an item that should be logged as a one hour report?

A. Yes.

Q. 2.1.2. If pertinent information is uncovered after an initial telephonic notification, should the pertinent information be telephoned to the NRC Operations Center?

A. Yes, but only if the information is significant. Significant information is that which would affect licensee or NRC response to the event.

*Q. 2.1.3. What procedures should licensees follow if compensatory measures in approved security plans are different than compensatory measures described in the guide?

A. The guidance in Regulatory Guide 5.62 is not intended to supplant any regulation or NRC-approved licensee safeguards plan. Accordingly, compensatory actions taken by licensees in accordance with approved security plans will permit the logging of certain events in lieu of reporting them within one hour.

The regulatory guide contains examples of acceptable compensatory measures to guide licensee reporting in situations not covered by approved safeguards plans.

Q. 2.1.4. When does the one hour notification clock for a safeguards event involving interruption of normal operation begin?

A. The clock begins when there is reasonable suspicion that the incident is the result of unauthorized use of or tampering with equipment, controls, etc.

*Q. 2.1.5. The LER form has a "block" where you provide a sequential number for events. Should we use the same numbering system for security events as for safety events?

A. No. The sequential numbering system for security events should start with the letter "S", followed by a two digit sequential number. (See the following example.)

EXAMPLE:

LER NUMBER (6)					REPORT DATE (7)		
YEAR		SEQ. NUMBER		REV. NUMBER	MONTH	DAY	YEAR
8 7	-	S 0 1	-	0 0	1 0	0 9	8 7

If you exceed 99 events in one year, replace the "S" with a "T".

2.2 Examples of Safeguards Events That Should Be Reported Within One Hour

2.2.1 Credible bomb or extortion threats. In addition to the initial telephone report, a telephone report of the results of a bomb search should be made within one hour of completion of the search. Unsubstantiated threats need not be reported immediately unless a specific organization or group claims responsibility or the threat is one of a pattern of harassing threats; in these cases, the threat must be reported within one hour. (Paragraph I(a)(1), (2), or (3) of Appendix G.) There are no compensatory measures that would preclude the reporting of a substantiated threat within one hour. If a threat cannot be substantiated (no organization or group identified, negative search results, and no additional evidence other than the threat message), the event need only be logged. (Also see number 13 in Section 2.4.)

Q. 2.2.1.a. Does this example include credible threats to commit certain actions?

A. Yes, if the threatened actions are as described in Appendix G Paragraph I, of 10 CFR 73.71, as events to be reported within one hour.

*Q 2.2.1.b. If a bomb threat is apparently unsubstantiated but search results cannot be obtained within an hour, should the threat be reported within one hour? If so, can the event status be changed if the result of subsequent search is negative?

A. If a specific organization or group has not claimed responsibility and the threat is not one of a pattern of harassing threats, the decision to report or log can await the results of the search if the search can be completed within a reasonable time. If the threat cannot be substantiated (no organization or group identified, negative search results, and no additional evidence other than the threat message), the event need only be logged. It should always be reported within one hour if substantiated.

> 2.2.2 Discovery of a criminal act involving individuals granted unescorted protected area or vital area access that, in the judgment of the licensee, adversely affects radiological safety in licensed activities or facility operations (e.g., felonious acts, discovery of a conspiracy to bomb the facility or disturb its vital components, vandalism of vital equipment, reasonable suspicion of illegal sale, use, possession, or introduction of a controlled substance onsite). (Paragraph I(a)(2) or (3) of Appendix G.) Because of the serious nature of such an event, discovery of the event should be reported within one hour even if the individual's unescorted access authorization is cancelled. (Also see number 3 in this section.)

Q. 2.2.2.a. Is this example intended to cover only criminal acts onsite? If so, how is onsite defined with respect to the facility's protected area and the introduction of a controlled substance?

A. Yes, this example is intended to cover only criminal acts onsite. Onsite is defined as inside the protected area. Detection of a controlled substance at an entry point to a protected area or within the owner controlled area outside of the protected areas should be logged.

Q. 2.2.2.b. Does the term "criminal act" imply conviction of the individual?

A. No. Acts of concern are those judged by licensees to adversely affect radiological safety in licensed activities or facility operations.

Q. 2.2.2.c. If management decides to perform drug screening on an individual based on reasonable suspicion for cause, does the time clock for reportability begin when initial tests give positive results or when the results are confirmed? If the individual's unescorted access is suspended, does the event need only be logged? Assume this person has safety-related responsibilities.

A. The time clock begins when the licensee has reasonable suspicion that an individual is abusing drugs onsite or is under the influence while onsite. Any illegal sale, possession, or use of a controlled substance onsite is reportable within one hour regardless of the responsibilities of the individual involved. For further discussion of the offsite aspects of this question see paragraph 2.2.3 below.

Q. 2.2.2.d. If a suspected controlled substance is found onsite, does the one hour time clock start when the discovery is made, or, after laboratory tests have confirmed that the material is a controlled substance?

A. The time clock begins when there is reasonable suspicion that the material is a controlled substance.

Q. 2.2.2.e. Do allegations of illegal sale, use, possession, or introduction of a controlled substance onsite constitute reasonable suspicion, thus making the allegation itself reportable within one hour?

A. No. Such an allegation should be reported within one hour only if, in the licensee's judgment, the allegation is valid.

Q. 2.2.2.f. Can the apparent validity of the allegation be used to determine reasonable suspicion, for example, whether the allegation was made anonymously, by a known individual, or by a private citizen versus a law enforcement officer?

A. Yes. The credibility of the source can be used to evaluate the reasonable suspicion factor.

Q. 2.2.2.g. Could not the reporting of suspicion of illegal use of a controlled substance undermine or compromise police undercover activities?

A. Licensees are expected to maintain liaison with local law enforcement agencies to minimize such conflicts and to internally protect such information. Submission of written reports can be delayed, with approval by the appropriate NRC Regional office, to minimize the possibility of compromise.

Q. 2.2.2.h. Define the term "reasonable suspicion."

A. Reasonable suspicion implies that there is some logical, or factual basis for believing that something is true.

> 2.2.3 Discovery of a criminal act involving a person granted unescorted protected area or vital area access if the act has the potential for adversely affecting the public health and safety, e.g., illegal use of a controlled substance offsite by a reactor control room operator. (Paragraph I(a)(2) or (3) of Appendix G.) Licensees should exercise judgment in determining the reportability of criminal acts conducted offsite. Only those acts with the potential for affecting the radiological safety of licensed activities need be reported. Criteria that can be used to judge reportability of these types of events include (1) the event indicates a failure in program design or implementation, (2) the person involved has safety-related responsibilities, or (3) the event is receiving media attention. Positive drug screens should be validated prior to determining reportability to the NRC. If the event is properly compensated, e.g., the program failure is corrected or, for individuals with no safety-related responsibilities, the individual's unescorted access is suspended, then the event need only be logged.

Q. 2.2.3.a. Is this example intended to cover only criminal acts committed offsite?

A. Yes.

Q. 2.2.3.b. Why is "media interest" required to be reported within one hour?

A. Media interest by itself is not required to be reported within one hour to the NRC. Licensees are encouraged to use media interest in a safeguards event

as one criterion for determining reportability of an event where licensee judgment must be exercised.

*Q. 2.2.3.c. If an employee turns himself or herself in to an employee assistance program because of drug or alcohol abuse, should this be reported or logged? Wouldn't this impact confidentiality of the program?

A. If continued performance in the individual's state constitutes a hazard to the public health and safety, including fellow employees, then the EAP has the obligation to inform appropriate management who should withdraw unescorted access and log the event. Presumably, licensees will handle such cases with due regard for confidentiality and privacy. However, public health and safety considerations must outweigh all other considerations in such cases.

*Q. 2.2.3.d. What steps should a licensee take when an allegation of drug use offsite is received?

A. (1) Attempt to verify the allegation, (2) if reasonable suspicion exists, log the item and follow normal procedures for handling an allegation.

*Q. 2.2.3.e. What does the term "....person involved has safety-related responsibilities" mean?

A. Actions of the person have the potential for affecting the radiological safety of licensed activities.

*Q. 2.2.3.f. If results of an individual's annual drug screen are positive should the event be reported or logged?

A. The event may be logged if their unescorted access is suspended pending completion of any additional confirmatory tests and reviews.

2.2.4 Discovery of theft or loss of classified documents pertaining to facility or transport safeguards. (Paragraph I(a) of Appendix G.) (Note: This is also reportable under § 95.57 of 10 CFR Part 95.) This type of event is considered a credible threat to the proper safeguarding of a facility or transport. By the nature of this event, its discovery can occur only after a significant degradation of the safeguards system designed to protect the classified documents has occurred. No measure can adequately compensate for such an event, and events of this type should always be reported within one hour of discovery. After the discovery, the licensee should endeavor to locate the missing or stolen document, take measures to help ensure the event is not repeated, and take whatever steps are possible to minimize the consequences of the event.

No questions were received on this item.

2.2.5 Fire or explosion of suspicious or unknown origin within the isolation zone, protected area, material access area, or vital area. (Note: Events reportable under §§ 50.72 or 50.73 do not require duplicate reports under § 73.71.) (Paragraphs I(a)(1), (2), or (3), or I(d) of Appendix G.) If the origin of a fire or explosion can be determined within one hour to be nonsuspicious and the facility sustains no

significant damage, the event is not considered a security threat to the facility and need not be reported or logged.

No questions were received on this item.

2.2.6 Discovery of a suspicious vehicle following a licensed carrier transporting formula quantities of SSNM. (Paragraph I(a)(1) of Appendix G.) In this situation, armed escorts or other responsible personnel should determine whether or not a threat exists and assess the extent of the threat, if any. If a threat exists, it should be reported to the NRC within one hour of confirmation and the provisions of paragraph 73.26(e) should be followed. If no threat exists, the event need not be reported or logged.

No questions were received on this item.

2.2.7 Mechanical breakdown of transport vehicle carrying formula quantities of SSNM. (Paragraphs I(a)(1), (2) of Appendix G.) Since it is difficult to readily determine if a mechanical breakdown is random or intentional, and because of the strategic significance of the material, mechanical breakdowns of transports carrying formula quantities of SSNM should always be reported to the NRC within one hour of discovery.

No questions were received on this item.

2.2.8 Complete loss of offsite communications. (Paragraph I(a)(2) or (3) of Appendix G.) If possible, the licensee should report the complete loss of communications from the site within one hour or immediately after restoration of communications. If communications from the site are lost and cannot be restored within one hour, the licensee should use communications located offsite to notify the NRC.

Q. 2.2.8.a. Explain which offsite communications this example refers to.

A. Complete loss of offsite communications means loss of telephone and radio capabilities.

2.2.9 Mass demonstration at plant site that may pose a threat to the facility. (Paragraph I(a)(2) or (3) of Appendix G.)

Q. 2.2.9.a. Does a demonstration directed at other than nuclear-related activities at a facility need to be reported to the NRC?

A. No, not if it has no impact on nuclear activities.

2.2.10 Civil disturbance near the plant site that may pose a threat to the facility. (Paragraph I(a)(2) or (3) of Appendix G.)

No questions were received on this item.

2.2.11 Confirmed tampering of suspicious origin with safety or security equipment. (Paragraph I(a)(1), (2), or (3) of Appendix G.)

No questions were received on this item.

2.2.12 An assault on a power reactor, facility, or transport possessing or transporting SSNM regardless of whether perimeter penetration is achieved. (Paragraph I(a)(1), (2), or (3) of Appendix G.)

No questions were received on this item.

2.2.13 Confirmed intrusions by unauthorized individuals into the protected area, material access area, controlled access area, vital area, or carrier transporting formula quantities of SSNM. (Paragraph I(b) of Appendix G.) Measures should be taken to preclude the recurrence of such events. Since any compensatory measures for such an event would be after the fact of a serious safeguards degradation, there are no compensatory measures that would preclude reporting such an event within one hour of discovery. The violation of licensee-established work rules (e.g., area zoning) within an area by an authorized individual need not be reported or logged as a safeguards event. (Also see number 11 in Section 2.4.)

*Q. 2.2.13.a. If a visitor, e.g., an individual requiring an escort while onsite, temporarily is left behind by an escort in an area that he or she entered in an authorized manner, should the event be reported?

A. If the escort or other employees authorized unescorted access promptly recognize and rectify the situation (e.g., within several minutes of occurrence), the event need only be logged. Escorts need not be maintained within restrooms from which there are limited means of egress. Otherwise, the incident should be reported within one hour because the visitor has not been authorized unescorted access.

Q. 2.2.13.b. What does the term "...licensee established work rules (e.g., area zoning)..." mean?

A. This term refers to areas to which access is restricted for reasons other than security (e.g., radiation areas). It is primarily used at fuel facilities and does not apply to vital area access at power reactors except with respect to zoning for safety-related purposes.

*Q. 2.2.13.c. If an individual enters a vital area to which he or she is authorized unescorted access by inadvertently using an access device intended for another individual who also has unescorted access to the area, should the event be reported or logged?

A. The event should be logged. For individuals with unescorted vital area access, only those entries which cannot be satisfactorily explained need be reported within one hour of discovery.

*Q. 2.2.13.d. If an individual with access only to the protected area inadvertently receives a badge granting vital area access but is stopped before any vital area entry is made, should the event be reported or logged?

A. Logged.

2.2.14 Uncompensated suspension of safeguards controls during either radiological or nonradiological emergencies that could allow undetected or unauthorized access. (Note: Events reportable under §§ 50.72 or 50.73 do not require duplicate reports under § 73.71.) (Paragraph I(c) of Appendix G.) Section 5.3, "Controls that Can Be Suspended During an Emergency," of Regulatory Guide 5.65, "Vital Area Access Controls, Protection of Physical Security Equipment, and Key and Lock Controls," describes safeguards measures that may be suspended during nonradiological emergencies.

No questions were received on this item.

2.2.15 Discovery of intentionally falsified identification badges or key cards. (Paragraph I(a) of Appendix G.) This event is considered a safeguards threat to the facility and should always be reported within one hour of discovery. Measures should be taken immediately to cancel the badges or key cards from the access system and to determine to what extent the badges or key cards have been used.

No questions were received on this item.

2.2.16 Discovery of uncompensated and unaccounted for, lost, or stolen key cards, I.D. 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 areas. (Paragraph I(c) of Appendix G.) Such events need not be reported within one hour if measures are taken within 10 minutes of the discovery of the loss to preclude the use of the lost or stolen device for gaining access to a controlled area and to ensure that the lost or stolen device has not been used in an unauthorized manner prior to completion of actions to prevent unauthorized use of the device. (Also see number 6 in Section 2.4.)

*Q. 2.2.16.a. If an access device is lost or stolen, must two actions be taken, e.g., action to preclude the use of the lost or stolen device and action to ensure that the lost or stolen device has not been used in an unauthorized manner, in order to log the event?

A. If action to preclude the use of the lost or stolen device is completed within 10 minutes of discovery, and action is initiated to ensure that the device has not been used in an unauthorized manner, the event should be logged.

2.2.17 Compromise of safeguards information (including loss or theft) that would significantly assist a person in an act of radiological sabotage or theft of SNM. (Paragraph I(a) of Appendix G.) There is no measure that would adequately compensate a compromise of safeguards information once the event has occurred. A licensee should always report this type of event within one hour of discovery, and follow-up measures similar to those for theft or loss of a classified document should be taken. (Also see number 4 in Section 2.2 above.)

Q. 2.2.17.a. What does the term "... significantly assist in an act of radiological sabotage..." mean with respect to loss of safeguards information?

A. This term means information that could be used to gain unauthorized or undetected access to a facility or information which would significantly assist an individual in damaging the facility or in theft of SNM.

Q. 2.2.17.b. Beyond verbal compromise, is there a difference between compromise of safeguards information and theft or loss of a classified document?

A. Yes. Classified documents are national security information. Theft or loss of these documents is always required to be reported within one hour of discovery. If lost safeguards information could significantly assist an individual in an act of radiological sabotage or theft of SNM, it is also required to be reported within one hour. However, if the lost safeguards information could not significantly assist in these acts, the event should be logged and the system failure corrected.

Q. 2.2.17.c. How long can safeguards information be missing before it is considered lost?

A. The NRC staff expects a report to be made within one hour of discovery that the document is missing.

Q. 2.2.17.d. In view of the regulatory reference in Appendix G to Part 73, which allows for reduced reporting if the event is compensated, why can't a significant loss or theft of safeguards information be compensated and logged?

A. There is no adequate compensatory measure. The reference to Appendix G contained a typographical error which has since been corrected. The reference has been changed to Appendix G.I.(a).

> 2.2.18 Uncompensated loss of the ability to monitor or remotely assess protected area alarms through loss of both central and secondary alarm stations. (Paragraph I(c) of Appendix G.) If the event involves an outage of the alarms, closed circuit television, or security computers, the event is considered properly compensated if the original capability is restored within 10 minutes of discovery of the event or if dedicated observers with appropriate communications are in place within 10 minutes of the discovery to provide total observation of each area.[1] Licensees are expected to discover this type of event upon occurrence. If immediate restoration of system capability is provided by activating secondary computers, the loss of backup capability need not be reported within one hour. (Also see number 10 in Section 2.4.)

Q. 2.2.18.a. Does immediate restoration of system capability mean restoration within 10 minutes?

A. Yes.

[1]Posting personnel as a compensatory measure implies that the personnel are capable of performing the lost or degraded function. When they cannot perform that function, such as when they are asleep, there is an uncompensated loss that must be reported within 1 hour of discovery. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

Q. 2.2.18.b. If the loss of both the central alarm station and the secondary alarm station is properly compensated as described in item 18, should the event be logged? If the secondary computer is lost also, should the event be reported within one hour?

A. Yes in both cases.

Q. 2.2.18.c. What is meant by the term "back-up capability" in item 18?

A. As used in item 18, this term means secondary computers.

Q. 2.2.18.d. Must a "dedicated observer" receive security training?

A. A dedicated observer must be trained in and capable of performing any assigned security function. However, dedicated observers are not required to be members of the security force.

Q. 2.2.18.e. Many security systems are designed with built-in redundancies such that if one element of the system fails, such as a central processing unit in a security computer, another one instantaneously functions in its place. Is the failure of one such redundant element reportable under 10 CFR 73.71?

A. No. If switchover is automatic such that there is no loss of system integrity or system degradation, the event is not required to be reported or logged.

*Q. 2.2.18.f. With use of the phrase "...licensees are expected to discover this type of event upon occurrence...", it is recognized that in most cases, component failures of security electronics systems will be discovered upon occurrence when the failure can be detected by line supervision design, etc. However, when failure is due to a loss in sensitivity, the event will not be discovered upon occurrence, but rather when a test is made of that component. Does "upon occurrence" mean "upon discovery" when the failure of the alarm is due to loss of sensitivity?

A. Licensees are required to monitor the functioning of their alarms and maintain their effectiveness through proper maintenance and testing programs, which may lead to periodic recalibrations. Regardless of when it may have occurred, if a system "fails" due to loss of sensitivity it should be immediately compensated (within 10 minutes of discovery) and the event should be logged. If it cannot be compensated within 10 minutes of discovery it should be reported within one hour.

> 2.2.19 Unavailability of a minimum number of security personnel or an actual or imminent strike by the security force. (Paragraph I(c) of Appendix G.) If an unexpected unavailability of a minimum number of security personnel occurs, procedures pre-approved by the NRC may be used; or "on call" guards or trained management, supervisory, or operations personnel available within 10 minutes may be used to supplement the on-duty security force. If minimum requirements cannot be met, the event should be reported within one hour of discovery.

Q. 2.2.19.a. What does the term "imminent" mean with respect to a security force strike?

A. In this case, the term means within three days.

Q. 2.2.19.b. Since it is highly unlikely that either an actual or imminent strike is something that would occur suddenly or would require immediate response by the NRC, what is the need for one hour reporting? This is particularly true if the utility has approved plans for dealing with a strike contingency.

A. The NRC staff believes that it can only discharge its responsibility for assuring that a licensee maintains protection of a facility during a strike by having current knowledge of the event. This cannot be accomplished through a log submitted quarterly.

Q. 2.2.19.c. As a compensatory measure for the unavailability of a minimum number of a security force onsite, does initiation of getting additional members onsite within 10 minutes suffice or do these guard force members have to be posted within 10 minutes?

A. In general, a minimum number must be posted within 10 minutes. NRC-approved site-specific plans may specify other measures and unique situations may require consultation with appropriate NRC staff to arrive at alternate solutions (e.g., contingency plans for replacing a sick security guard).

*Q. 2.2.19.d. If the NRC is already on notice that a strike is going to occur, is a one hour report necessary when the strike actually does occur?

A. Not for 10 CFR 73.71 requirements, however, such a report might be required in accordance with 10 CFR 50.72.

> 2.2.20 Uncompensated loss of all ac power supply to security systems that could allow unauthorized or undetected access to a protected area, material access area, controlled access area, or vital area. (Paragraph I(c) of Appendix G.) If the security system integrity can be maintained by standby power, the event is considered properly compensated and need only be logged. However, if standby power fails prior to restoration of ac power, the event should be reported within one hour of loss of standby power. Licensees are expected to discover this type of event upon occurrence. (Also see number 7 in Section 2.4.)

*Q. 2.2.20.a. If power loss is momentary, (e.g., less than 10 minutes) should the event be reported or logged?

A. If all AC power supply is lost and security system integrity is not maintained by standby power, the event should be reported within one hour, unless compensated in accordance with an NRC-approved security plan.

> 2.2.21 Uncompensated loss of ability to detect within a single intrusion detection system zone. (Paragraph I(c) of Appendix G.) Proper compensation for this event means immediate deployment (within 10 minutes of discovery) of backup intrusion detection equipment or posting a dedicated observer with a view of the entire area and capability to

communicate with alarm stations.[1] (Also see number 3 in Section 2.4.) Licensees are expected to discover this type of event upon occurrence.

No questions were received on this item.

2.2.22 Loss of alarm capability or locking mechanism on a material access area or vital area portal. (Paragraph I(c) of Appendix G.) A bolt-position alarm capability is not a proper compensatory measure for loss of a balanced-magnetic alarm because it is not tamper-resistant. Proper compensation for either of these events means immediate (within 10 minutes of discovery) posting of a dedicated observer for loss of an alarm or posting an armed member of the security force for loss of a lock. The posted observer or guard should have appropriate communications equipment.[1] In addition, a thorough search of the affected area should be initiated immediately and completed as soon as practicable. Licensees are expected to discover this type of event upon occurrence. (Also see number 8 in Section 2.4.)

*Q. 2.2.22.a. Does "upon occurrence" mean "upon discovery" when the failure of a locking device is due to mechanical breakdown?

A. Regardless of cause, actions to compensate for loss of locking mechanism should be initiated upon discovery.

*Q. 2.2.22.b. If a lock fails on a vital area door but the alarm remains operational should this event be reported or logged?

A. Logged, if properly compensated. Proper compensation means immediate (within 10 minutes of discovery) posting of an armed member of the security force or other measures as described in the licensee's NRC-approved security plans, as applicable.

*Q. 2.2.22.c. The requirement to post an armed member of the security force for the loss of a lock is inconsistent with 10 CFR 73.55(d)(8) which allows an unarmed watchman to control access to a reactor containment building and NUREG-1045 which allows watchpersons to provide access control to protected and vital areas.

A. NUREG-1045 and RG 5.62 both call for an armed member of the security force as a compensatory measure whenever barrier integrity is reduced, including doors and appropriate hardware. NUREG-1045 does allow security personnel, including watch persons to be used where barrier integrity is maintained but the computer is not able to verify the identity and maintain the required log. The first example cited, 10 CFR 73.55(d)(8), refers to an outage situation when the reactor is not operating. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

Q: 2.2.22.d. What is proper compensation for an open vital area door during a planned maintenance evolution with the reactor operating?

[1]Posting personnel as a compensatory measure implies that the personnel are capable of performing the lost or degraded function. When they cannot perform that function, such as when they are asleep, there is an uncompensated loss that must be reported within 1 hour of discovery. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

A. Armed guards should be posted with appropriate communication devices.

2.2.23 Discovery of the actual or attempted introduction into or possession within the protected area, material access area, or vital area of unauthorized weapons, explosives, or incendiary devices. (Paragraph I(d) of Appendix G.) There are no compensatory measures that would preclude reporting this event within one hour. If an actual introduction of contraband is made, steps should be taken to correct the vulnerability that allowed the introduction. (Also see number 5 in this section.) The discovery of vehicular emergency equipment such as safety flares during entrance searches need not be reported or logged.

Q. 2.2.23.a. "Cad-weld" material is frequently used for installation and repair at most nuclear sites. If authorized for onsite use, should discovery of this material be reported? If not authorized, should discovery be reported or logged?

A. Discovery of material such as "cad-weld" that is authorized for onsite use and properly controlled should not be reported or logged. If the event can be satisfactorily explained, discovery of weapons, explosives, or incendiary devices during routine entrance search should be logged. Weapons, explosives, or incendiary devices (including materials such as "cad-weld") <u>not authorized</u> onsite and discovered within the PA should be reported within one hour.

Q. 2.2.23.b. Define the term "contraband."

A. Contraband includes any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property. Safety flares carried on vehicles as emergency road equipment need not be considered incendiary devices for the purpose of reportability.

Q. 2.2.23.c. If a vehicle operator fails to turn in a weapon stored in the vehicle prior to search and the weapon is not found during the search, but is found later, should the event be reported within one hour?

A. Yes. Contraband has entered the protected area.

Q. 2.2.23.d. If a weapon is found in a vehicle located in a parking lot outside the protected area, should it be reported within one hour?

A. Generally, the discovery of a weapon in a vehicle parked in a lot outside of the PA need not be reported or logged.

Q. 2.2.23.e. If a weapon is found on a vehicle during an entrance search should it be reported or logged?

A. Logged, unless malevolent intent is established.

Q. 2.2.23.f. If a weapons contractor ships a licensee one more weapon than ordered, is the extra weapon considered unauthorized and should it be reported?

A. If there is reasonable suspicion that this constituted a deliberate attempt to introduce an unauthorized weapon onsite, a one hour report should be made.

Q. 2.2.23.g. If a driver turns in a weapon upon request prior to search, should it be reported?

A. No.

Q. 2.2.23.h. Does the term "weapon" refer strictly to firearms.

A. No.

2.24 Loss of security weapon at the site. (Paragraph I(a)(3) of Appendix G.)

No questions were received on this item.

2.3 Safeguards Events To Be Reported and Submitted Quarterly in a Log (General)

*Q. 2.3.1. Must a licensee maintain backup documentation for follow-up inspections resulting from NRC review of log entries? How long must this backup documentation be maintained?

A. A licensee should maintain information which resolves log entries for three years.

*Q. 2.3.2. Paragraph II.b. of Appendix G requires logging of events which reduce capabilities below that committed to in a licensed physical security or contingency plan. Certain compensatory measures may go beyond what has been approved in a licensee's security plan. What takes precedence?

A. The guidance in Regulatory Guide 5.62 is not intended to supplant any regulation or NRC-approved licensee safeguards plan. Accordingly, compensatory actions taken by licensees in accordance with approved security plans will permit the logging of certain events in lieu of reporting them within one hour. The regulatory guide contains examples of acceptable compensatory measures to guide licensee reporting in situations not covered by approved safeguards plans.

Q. 2.3.3. When must false or nuisance alarms be logged?

A. False or nuisance alarms should be logged if a pattern of such alarms emerges or when their frequency is such that system effectiveness is degraded below that committed to in an approved security plan.

Q. 2.3.4. The regulatory guide states that log entries should be updated when the event terminates. Define the term "... when the event terminates..."

A. This term means when compensatory measures are established or the original system capability is restored.

Q. 2.3.5. Define "end of the quarter" with respect to quarterly submittal of the safeguards events log.

A. The end of the quarter is defined as December 31, March 31, June 30, and September 30. Safeguards event logs should be postmarked within 30 days of the end of each quarter.

*Q. 2.3.6. If an audit conducted under provisions of 10 CFR 73.55(g)(4) or Appendix B to 10 CFR Part 50 uncovers events not previously reported or logged, should a licensee make a report?

A. No. It should not be reported or logged under 10 CFR 73.71. However, it would be a licensee-identified finding which should be brought to the attention of the appropriate NRC Regional Office.

2.4 Examples of Safeguards Events To Be Reported and Submitted Quarterly in a Log

2.4.1 Properly compensated security computer failures. (Paragraph II(a) of Appendix G.) Properly compensated means that within 10 minutes of the discovery of the failure the system is restored to operation, the backup system is operational, or other resources, e.g., security personnel with appropriate communications equipment, are posted to provide an equivalent level of protection. In all cases, a thorough search of all areas where alarms or access controls may have been compromised by the failure should be initiated immediately and completed as soon as practicable. Licensees are expected to discover this type of event upon occurrence.

Q. 2.4.1.a. For fuel cycle facilities, what constitutes a "thorough search"?

A. This term means a search for unauthorized individuals, tampering, or unauthorized packages. It does not usually mean equipment search for SNM.

*Q. 2.4.1.b. Must a guard be posted at every vital area portal when a security computer fails?

A. Unless compensated by some other means described in an NRC-approved safeguards plan, guards must be posted at all vital area portals that fail open or are used for access.

2.4.2 Properly compensated vital area card reader failures. (Paragraph II(a) of Appendix G.) For this event, proper compensation means posting appropriate personnel (i.e., armed guard if door is unlocked, dedicated observer if door remains locked but access is required) within 10 minutes of discovery.[1] The appropriate personnel must have a current access list and communications capability to alarm stations. A thorough search of the affected area must be initiated immediately and completed as soon as practicable. Licensees are expected to discover this type of event upon occurrence.

Q. 2.4.2.a. If a vital area card reader fails, is it a sufficient compensatory measure to post a guard with an access list and check I.D. cards as badged individuals enter the area?

[1]Posting personnel as a compensatory measure implies that the personnel are capable of performing the lost or degraded function. When they cannot perform that function, such as when they are asleep, there is an uncompensated loss that must be reported within 1 hour of discovery. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

A. The guard would also be required to maintain a log of individuals in the affected area. This is required under the Miscellaneous Amendments issued August 4, 1986, (51 FR 27817).

Q. 2.4.2.b. Can coded badges be used in lieu of an access list when seeking access to areas during card reader failures?

A. Coded badges may be used in lieu of an access list. However, a record must still be kept of entries to and exits from the vital area.

*Q. 2.4.2.c. The example states that licensees are expected to discover this type of event upon occurrence. Is it correct to assume that "upon occurrence" means at the time someone attempts to use the card reader?

A. It is possible that this event may not be discovered until someone attempts to use the card reader. Regardless of when the failure may have occurred, it should be compensated within 10 minutes of discovery and logged. If it cannot be compensated within 10 minutes of discovery it should be reported within one hour.

*Q. 2.4.2.d. If a CCTV system has a failure and the approved security plan does not require the posting of a dedicated observer, (it commits to an armed response to an alarm, only), must a one hour report be made if a dedicated observer is not posted?

A. No. Licensees are expected to take compensatory actions in accordance with NRC-approved safeguards plans and log such events as "compensated".

2.4.3 Properly compensated alarm failures. (Paragraph II(a) of Appendix G.) For this event, proper compensation means deployment of backup alarm equipment (a bolt-position alarm capability is not considered backup alarm equipment because it is not tamper-resistant) or posting a dedicated observer within 10 minutes of discovery.[1] The dedicated observer should have appropriate communications equipment and should be able to observe the entire affected area of the portal. In addition, a thorough search of the affected area should be initiated immediately and completed as soon as practicable. (Also see number 21 in Section 2.2.) Licensees are expected to discover this type of event upon occurrence.

No questions were received on this item.

2.4.4 Properly compensated closed circuit television failure in a single zone while the intrusion detection system remains operational. (Paragraph II(a) of Appendix G.) Properly compensated means providing other assessment capability, such as posting a dedicated observer with communications equipment to assess the entire zone within 10 minutes of discovery of the failure.[1] Licensees are expected to discover this type of event upon occurrence.

[1]Posting personnel as a compensatory measure implies that the personnel are capable of performing the lost or degraded function. When they cannot perform that function, such as when they are asleep, there is an uncompensated loss that must be reported within 1 hour of discovery. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

Q. 2.4.4.a. May multiple failed zones be compensated by one dedicated observer with observation of all zones?

A. Yes, if the individual can observe all affected zones.

*Q. 2.4.4.b. If a CCTV system assessing multiple zones has been approved for use at a site, must dedicated observers be posted at each zone if the CCTV fails?

A. Some site-specific unique situations may permit fewer than one dedicated observer per zone. Licensees should consult with appropriate NRC staff if it is believed their situation is unique. Licensees are expected to take compensatory actions in accordance with approved security plans if applicable to an event and log it accordingly.

2.4.5 Properly compensated failure or degradation of a single perimeter lighting zone if the intrusion detection system remains operational. (Paragraph II(a) of Appendix G.) Measures to properly compensate for failure or degradation of a lighting zone must be implemented within 10 minutes of discovery and may include (1) using standby power, (2) using low-light-level surveillance devices, (3) using portable lighting systems or (4) posting dedicated observers with appropriate communications equipment to provide an equivalent level of protection.

Q. 2.4.5.a. If some lighting is lost but not enough to go below the level committed to in the security plan (e.g., 0.2 foot-candles), is a report required or can the event be logged?

A. Neither a report within one hour nor a log entry need be made.

Q. 2.4.5.b. With respect to this example, what if failure is less than system-wide but more than a single zone? How should this be reported or logged?

A. Use the reporting criteria as if it was a single zone.

2.4.6 Properly compensated accidental removal offsite or loss of badge by employee. (Paragraph II(a) of Appendix G.) For this event, proper compensation is cancelling the badge from the access control system within 10 minutes of discovery by onsite personnel that the badge is missing. Measures must be taken to be sure the badge has not been used in an unauthorized manner while it has been missing. (Also see number 16 in Section 2.2.)

No questions were received on this item.

2.4.7 Properly compensated loss of the AC power supply for the entire intrusion detection system that, if uncompensated, would allow unauthorized or undetected access. (Paragraph II(a) of Appendix G.) Proper compensation for this event is immediately available emergency power through an uninterruptible power source such as a battery supported

by a generator. If backup power is not available, security personnel with communications equipment should be posted within 10 minutes of discovery; however, this action is not considered proper compensation for the event and does not excuse a licensee from reporting the event within one hour. Licensees are expected to discover this type of event upon occurrence. (Also see number 20 in Section 2.2.)

Q. 2.4.7.a. Why is timely posting of properly equipped security personnel not considered proper compensation for loss of AC power supply to the entire intrusion detection system?

A. A significant degradation that cannot be properly compensated has occurred. The level of effectiveness existing prior to the loss cannot be maintained only through posting.

2.4.8 Properly compensated loss of either alarm or locking mechanism on a material access area or a vital area portal. (Paragraph II(a) of Appendix G.) A bolt-position alarm capability is not considered a proper compensatory measure because it is not tamper-resistant. Proper compensation for this event is immediate (within 10 minutes of discovery) posting of a dedicated observer for a loss of alarm or an armed member of the security force for loss of a lock.[1] The posted personnel should have appropriate communications equipment. In addition, a thorough search of the affected area should be initiated immediately and completed as soon as practicable. Licensees are expected to discover this type of event upon occurrence. (Also see numvwe 22 in Section 2.2.)

No questions were received on this item.

2.4.9 Security computer failures that may not enable unauthorized or undetected access. (Paragraph II(b) of Appendix G.)

Q. 2.4.9.a. What type of events are security computer failures that may not enable unauthorized or undetected access?

A. Such things as loss of printing capability only, or when a computer fails to store entries on a disk, are security computer failures of this type.

*Q. 2.4.9.b. Should a security computer data base failure that does not impact effectiveness be reported?

A. No.

2.4.10 Loss of the capability of a single alarm station to monitor or remotely assess alarms but monitoring or assessment capability remains in other stations. (Paragraph II(b) of Appendix G.) (Also see number 18 in Section 2.2.)

[1]Posting personnel as a compensatory measure implies that the personnel are capable of performing the lost or degraded function. When they cannot perform that function, such as when they are asleep, there is an uncompensated loss that must be reported within 1 hour of discovery. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

Q. 2.4.10.a. Does this example imply that all vital area portal alarms should be logged, or only those alarms which are caused by actual problems?

A. This example implies neither. In some cases vital area alarms caused by actual problems may require one hour reporting. In most cases, if a reportable event is properly compensated, it need only be logged.

2.4.11 Tailgating by a licensee employee or contractor to gain access to an area to which he or she is authorized access. (Paragraph II(b) of Appendix G.) (Also see number 13 in Section 2.2.)

*Q. 2.4.11.a. Does specific intent affect reportability of tailgating?

A. Yes. For example, if tailgating is committed by an authorized employee or contractor, it is considered an administrative matter that should be corrected and the event should be logged. If tailgating is committed by unauthorized individuals, the event should be logged if it can be satisfactorily explained and their level of screening would qualify them for unescorted access. Otherwise, the event should be reported within one hour. Licensees are expected to investigate the matter and correct any deficiencies in programs and procedures.

2.4.12 For shipments of formula quantities of SSNM, intra-convoy communications ability is lost, but ability to communicate with movement control center remains. (Paragraph II(b) of Appendix G.)

No questions were received on this item.

2.4.13 Unsubstantiated bomb or extortion threat. (Paragraph II(b) of Appendix G.) An unsubstantiated bomb or extortion threat is a threat in which no specific organization or group claims responsibility, the search result is negative, and no evidence is available other than the threat message. If a threat is one of a pattern of harassing, even if unsubstantiated, it should be reported within one hour.

No questions were received on this item.

NRC FORM 336 (2 84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1 REPORT NUMBER (Assigned by TIDC and Vol No., if any)

NUREG-1304

2 TITLE AND SUBTITLE

REPORTING OF SAFEGUARDS EVENTS

3 LEAVE BLANK

4 DATE REPORT COMPLETED

MONTH: February YEAR: 1988

5 AUTHOR(S)

Priscilla A. Dwyer
Nancy E. Ervin

6 DATE REPORT ISSUED

MONTH: February YEAR: 1988

7 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Division of Reactor Inspection and Safeguards
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, DC 20555

8 PROJECT/TASK/WORK UNIT NUMBER

9 FIN OR GRANT NUMBER

10 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Division of Reactor Inspection and Safeguards
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20545

11a TYPE OF REPORT

b PERIOD COVERED (Inclusive dates)

12 SUPPLEMENTARY NOTES

Technical Report

13 ABSTRACT (200 words or less)

On June 9, 1987, the Commission published in the Federal Register a final rule revising the reporting requirements for safeguards events. Safeguards events include actual or attempted theft of special nuclear material (SNM); actual or attempted acts or events which interrupt normal operations at power reactors due to unauthorized use of or tampering with machinery, components, or controls; certain threats made against facilities possessing SNM; and safeguards system failures impacting the effectiveness of the system. The revised rule was effective October 8, 1987. On September 14, 1987, the NRC held a workshop in Bethesda, MD to answer affected licensees' questions on the final rule. This report documents questions discussed at the September 14 meeting, reflects a completed staff review of the answers, and supersedes previous oral comment on the topics covered.

14 DOCUMENT ANALYSIS - a KEYWORDS/DESCRIPTORS

Safeguards Events

Physical Protection

b IDENTIFIERS/OPEN ENDED TERMS

15 AVAILABILITY STATEMENT

Unlimited

16 SECURITY CLASSIFICATION

(This page) Unclassified

(This report) Unclassified

17 NUMBER OF PAGES

18 PRICE

*U.S. GOVERNMENT PRINTING OFFICE:1988-202-292:50342

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

SPECIAL FOURTH-CLASS RATE
POSTAGE & FEES PAID
USNRC
PERMIT No. G-67

NUREG-1304

REPORTING OF SAFEGUARDS EVENTS

FEBRUARY 1988