Revision 1
November 1987

U.S. NUCLEAR REGULATORY COMMISSION

# REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 5.62
(Task SG 901-4)

## REPORTING OF SAFEGUARDS EVENTS

### A. INTRODUCTION

In 10 CFR Part 73, "Physical Protection of Plants and Materials," paragraphs 73.71(a) through (c) have recently been amended. Section 73.71 requires licensees to report to the Operations Center of the NRC or to record for quarterly transmittal to the NRC certain safeguards events. These events are those that threaten nuclear activities or lessen the effectiveness of a security system as established by safeguards regulations or an approved security or contingency plan.

This regulatory guide provides an approach acceptable to the NRC staff for use by the licensee for determining when and how an event should be reported. The examples provided represent the types of events that should be reported and are not intended to be all-inclusive. The applicability of events may vary from site to site.

Any information collection activities mentioned in this regulatory guide are contained as requirements in 10 CFR Part 73, which provides the regulatory basis for this guide. The information collection requirements in 10 CFR Part 73 have been cleared under OMB Clearance No. 3150-0002.

### B. DISCUSSION

The information reportable under § 73.71 is required so the NRC will be informed of safeguards-related events that have the potential to endanger public health and safety or national security. The required information is also used to monitor trends in safeguards system effectiveness.

Because certain significant safeguards events warrant immediate involvement by the NRC and possibly other government agencies such as the FBI, these events must be reported by telephone to the NRC within 1 hour of discovery of the event, and a detailed written report must follow within 30 days.

Certain other less significant safeguards events are required to be recorded in a log and copies of the recorded log submitted to the NRC every 3 months. While these events are less significant than those reportable within 1 hour, they are required to be reported to the NRC on a quarterly basis for review and long-term trend analysis. If an event occurs repeatedly at one facility or throughout the industry, it may represent a defect in the security program or a generic trend. Not all generic defects or trends require action on the part of the NRC; however, this decision cannot be made unless the events are reported to the NRC. Licensees have been required to maintain a separate log to record events reportable under § 73.71 in the past, but are now required to submit a copy of that log to the NRC on a quarterly basis.

For the purposes of this guide and for understanding the regulations, a glossary is given in Appendix A of this guide. Table 1 presents a summary of reportable events and reporting times.

### C. REGULATORY POSITION

#### 1. LICENSEES SUBJECT TO § 73.71

Licensees who are subject to the provisions of §§ 73.25, 73.26, 73.27(c), 73.37, 73.67(e), or 73.67(g) of 10 CFR Part 73 are subject to the provisions of paragraph 73.71(a).

Licensees who are subject to the provisions of §§ 73.20, 73.37, 73.50, 73.55, 73.60, or 73.67 are subject to the provisions of paragraph 73.71(b) for events described in paragraph (I)(a)(1) of the new Appendix G to Part 73. Licensees subject to the provisions of §§ 73.20, 73.37, 73.50, 73.55, 73.60, or each licensee possessing

## Table 1

## Summary of Reporting Requirements

| Required Reports | Description of Safeguards Event |
|---|---|
| Telephone report within 1 hour followed by a written report within 30 days | 1. Loss of shipment of SNM or spent fuel.<br>2. Recovery or accounting of lost shipment of SNM or spent fuel.<br>3. Threatened, attempted, or actual:<br>a. Theft or unlawful diversion of SNM,<br>b. Significant physical damage to a reactor or facility or carrier possessing SSNM,<br>c. Unauthorized interruption of normal operations at a power reactor.<br>4. Actual entry of unauthorized person into a PA, MAA, CAA, VA, or transport.<br>5. Uncompensated failure, degradation, or discovered vulnerability in a safeguards system that could allow unauthorized or undetected access to a PA, MAA, CAA, VA, or transport.<br>6. Actual or attempted introduction of contraband into a PA, MAA, VA, or transport. |
| Safeguards event log submitted every 3 months | 1. Compensated failure, degradation, or discovered vulnerability in a safeguards system that if uncompensated could have allowed unauthorized or undetected access to a PA, MAA, CAA, VA, or transport.<br>2. Any other threatened, attempted, or committed act not previously defined in Appendix G of 10 CFR Part 73 that has the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness. |

PA = protected area
MAA = material access area
CAA = controlled access area
VA = vital area
SNM = special nuclear material
SSNM = strategic special nuclear material

strategic special nuclear material (SSNM) and subject to paragraph 73.67(d) are subject to the provisions of paragraph 73.71(b) for events described in paragraphs I(a)(2), I(a)(3), I(b), and I(c) of Appendix G to Part 73. Licensees subject to the provisions of §§ 73.20, 73.37, 73.50, 73.55, or 73.60 are subject to the provisions of paragraph 73.71(b) for events described in paragraph I(d) of Appendix G to Part 73.

Licensees subject to the provisions of §§ 73.20, 73.37, 73.50, 73.55, 73.60, or each licensee possessing SSNM and subject to paragraph 73.67(d) are subject to the provisions of paragraph 73.71(c).

## 2. REPORTABLE EVENTS

### 2.1 Safeguards Events To Be Reported Within 1 Hour

Paragraphs 73.71(a) and (b) require certain events to be reported within 1 hour of discovery. Events under paragraph 73.71(a) involve incidents in which theft, loss, or diversion of a shipment of special nuclear material (SNM) or spent fuel has occurred or is believed to have occurred. A written report should be submitted to the NRC within 30 days on each event that is reported within 1 hour. Safeguards events reportable under paragraph 73.71(b) and described in Appendix G to 10 CFR Part 73 include:

1. Acts, attempts, or threats to commit:

   (a) Theft or unlawful diversion of SNM or spent fuel;

   (b) Significant physical damage to a power reactor, to any facility possessing SSNM or such facility's equipment, to the carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel a facility or carrier possesses;

   (c) Interruption of normal operation of a licensed nuclear power reactor through the unauthorized use of or tampering with its machinery, components, or controls, including the security system.

2. Any actual entry of an unauthorized person into a protected area, material access area, controlled access area, vital area, or transport equipment.

3. Any uncompensated failure, degradation, or discovered vulnerability in a safeguards system that could allow unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or carrier transporting nuclear fuel, spent fuel, or formula quantities of SSNM.

4. Any actual or attempted introduction of contraband into a protected area, material access area, vital area, or transport equipment.

To clarify, safeguards system failures include not only mechanical or electrical system failures but also improper security procedures or personnel practices. Discovered vulnerabilities include incidents in which the security system has not failed, but some flaw in the security system that had existed without being noticed has been discovered.

### 2.2 Examples of Safeguards Events To Be Reported Within 1 Hour

The following are examples of events that should be reported to the NRC within 1 hour because of their potential to endanger public health and safety or national security. This list should not be considered all-inclusive. The applicable regulation is cited for each event, and compensatory measures are discussed if appropriate.

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 1 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 1 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 1 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 of this guide.)

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 1 hour even if the individual's unescorted access authorization is cancelled. (Also see number 3 in this section.)

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 the individual's unescorted access is suspended, then the event need only be logged.

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. No measure can adequately compensate for such an event, and events of this type should always be reported within 1 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.

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), (3), or I(d) of Appendix G) If the origin of a fire or explosion can be determined within 1 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. (Also see number 4 in Section 2.5.)

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 1 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.

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 1 hour of discovery.

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 1 hour or immediately after restoration of communications. If communications from the site are lost and cannot be restored within 1 hour, the licensee should use communications located offsite to notify the NRC.

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

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

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

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)

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 1 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.)

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.

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 1 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.

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 1 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.)

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 1 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 this section.)

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 equipment 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 1 hour. (Also see number 10 in Section 2.4.)

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 1 hour of discovery.

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 1 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.)

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 back-up intrusion detection equipment or posting a dedicated observer with a view of the entire area and capability to communicate with alarm stations.[1] Licensees are expected to discover this type of event upon occurrence. (Also see number 3 in Section 2.4.)

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.)

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 1 hour. If an actual introduction of contraband is made, steps should be taken to correct the vulnerability that allowed the introduction. The discovery of vehicular emergency equipment such as safety flares during entrance searches need not be reported or logged. (Also see number 5 in this section.)

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

## 2.3 Safeguards Events To Be Reported and Submitted Quarterly in a Log

The following safeguards events reportable under paragraph 73.71(c) need only be logged within 24 hours of their discovery and submitted quarterly to the NRC:

1. Any failure or degradation of a safeguards system or discovered vulnerability in a system that could have allowed unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport equipment if compensatory measures had not been established. (Logging is not required for preplanned situations that require compensatory measures, such as special outage work, equipment relocation, exercises and drills, and other situations that are not the result of a safeguards system failure.)

2. Any other threatened, attempted, or committed act not previously defined in Appendix G that has the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness.

With respect to the proper compensation of an event, compensatory measures need to be implemented promptly to be effective. For example, measures used to compensate

[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.

for a design flaw or vulnerability in a safeguards barrier that has existed for some period of time and that could allow unauthorized or undetected access are not considered effective if implemented more than 10 minutes after the flaw or vulnerability occurs; such events require immediate reporting. Prompt implementation will minimize any period of degradation that may exist between the occurrence and proper compensation after discovery of certain events. Proper compensation after discovery of an event does not relieve the licensee from the responsibility for taking long-term corrective action, nor does it relieve the licensee from possible enforcement action by the NRC for non-compliance during the periods of safeguards system degradation. However, licensees are not ordinarily cited for violations resulting from matters not within their control, such as equipment failures that occurred despite reasonable licensee quality assurance measures, testing and maintenance programs, or management controls. (See 10 CFR Part 2, Appendix C, paragraph V.A.)

False alarms (those generated without any apparent cause) and nuisance alarms (those generated by an identified input that does not represent a safeguards threat) generally need not be reported or logged. However, if false or nuisance alarms are so frequent that the effectiveness of the alarm system is degraded or a pattern of false or nuisance alarms emerges, the licensee should take corrective action and note the degraded status and compensatory measures taken in the safeguards event log.

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

The following are examples of events that are less significant than those reportable within 1 hour, and according to the rule are required to be logged within 24 hours and submitted quarterly to the NRC. This list should not be considered all-inclusive. The applicable regulation is cited for each event, and compensatory measures are discussed where appropriate.

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.

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.

3. Properly compensated alarm failures. (Paragraph II(a) of Appendix G) For this event, proper compensation means deployment of back-up alarm equipment (a bolt-position alarm capability is not considered back-up 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. Licensees are expected to discover this type of event upon occurrence. (Also see number 21 in Section 2.2.)

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.

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.

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 onsite personnel discovering 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.)

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 back-up 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 1 hour. Licensees are expected to discover this type of event upon occurrence. (Also see number 20 in Section 2.2.)

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 number 23 in Section 2.2.)

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

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.)

11. Tailgating by a licensee or contractor employee 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.)

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)

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 1 hour.

### 2.5 Events Not Required To Be Logged or Reported

Certain failures of the safeguards system that do not and could not reduce the effectiveness of the system have little or no safeguards significance; events having little or no safeguards significance need not be reported or logged. The following are examples of events that are not required to be logged or reported. This list should not be considered all-inclusive.

1. Cuts made by authorized maintenance personnel through a vital area barrier for a legitimate reason (e.g., to install pipe) if prior approval, coordination with security, and proper compensatory measures have been established.

2. A person attempting to climb a protected area fence if the person is obviously a child.

3. Infrequent nuisance alarms caused by mechanical or environmental problems and false alarms that do not exceed the rates committed to in the licensee's approved security plan or do not degrade alarm system effectiveness.

4. When the origin of a fire or explosion can be determined within 1 hour to be nonsuspicious and the facility sustains no significant damage.

## 3. PROCEDURES

The determination for reporting an event under paragraphs 73.71(a), (b), and (c) should be made by onsite security management or their equivalent. However, discovery of such an event is not limited to members of the security organization. It is recommended that all regular site employees receive security orientation by the security organization to foster an awareness of site security and to be briefed on their responsibility to immediately notify site security of safeguards anomalies.

Events of a dual nature (i.e., having both safety and safeguards implications and subject to the requirements of §§ 50.72, 50.73, and 73.71) do not require duplicate reports under the requirements of § 73.71. If a power reactor licensee reports an event that is reportable in accordance with both §§ 50.73 and 73.71, the procedures described in § 50.73 (i.e., submittal of a licensee event report (LER)) must be followed. The procedures contained in NUREG-1022, "Licensee Event Report System,"[2] describe how to indicate that an LER meets multiple reporting requirements. When submitting reports of events reportable solely under the provisions of § 73.71, power reactor licensees should use LER Form 366; all other licensees should write a letter. If the written report contains restricted data, e.g., unclassified safeguards information, the report must be appropriately marked. If NRC Form 366 or 366A is used, restricted data may be included only in the text section (Item 17 of the form). Restricted data should not be included in the abstract section (Item 16) or any other section of the form other than the text section. In addition, the text should clearly indicate the information that is restricted. Finally, the requirements of paragraph 73.21(g) must be met when transmitting written proprietary information.

It is recognized that not all items of NRC Form 366 may apply when safeguards events are reported. Power reactor licensees should be sure that all the information needed by the NRC for analysis and evaluation, as described in section 3.2 of this guide, is included on the form, whether under a specific item or in the text section.

Procedures for the 1-hour report, the 30-day followup report, and the quarterly log are discussed in the following sections.

[2] F. J. Hebdon, "Licensee Event Report System," U.S. Nuclear Regulatory Commission, NUREG-1022, September 1983.

### 3.1 1-Hour Reports

When a licensee, licensee employee, or contract employee discovers an event reportable under paragraph 73.71(a) or (b), telephone notification to the NRC Operations Center listed in Appendix A to 10 CFR Part 73 should be made within 1 hour of the discovery. Telephone notification should be made via the Emergency Notification System (ENS) if the licensee is party to that system. If the ENS is inoperative or unavailable, a commercial telephone should be used to ensure that the required notification is received by the NRC Operations Center within 1 hour of discovery of the event. The commercial telephone number that may be used to contact the NRC Operations Center is (301) 951-0550. Other methods that may be used to ensure notification within 1 hour include telegram, mailgram, or facsimile. Telegrams and mailgrams should be hand delivered to the Operations Officer at the NRC Operations Center, Maryland National Bank Building, 7735 Old Georgetown Road, Bethesda, Maryland 20814. For information concerning facsimiles, telephone the NRC Operations Center at (301) 492-8893. If pertinent information or errors are uncovered after the initial telephone report but prior to submittal of the written report, the licensee should notify the NRC Operations Center of the information or error by telephone.

Under the provisions of paragraph 73.71(a), the licensee (or agent) should also notify the NRC Operations Center by telephone within 1 hour of the recovery of or accounting for a shipment with information on the material located, known reason for loss, etc.

Telephone reports made pursuant to § 73.71 may be transmitted over unprotected lines as permitted by the exemption in paragraph 73.21(g)(3).

### 3.2 30-Day Followup Written Reports

A followup written report must be submitted within 30 days of a 1-hour report. Power reactor licensees should use the Licensee Event Report form, NRC Form 366, in submitting their reports; all other licensees should use a letter format. For all licensees, the information described below is sufficient for NRC analysis and evaluation and should be included in the report as a minimum. Reports of events must be legible and reproducible and should include the following:

1. Date and time of event (start and end time).
2. Location of actual or threatened event in a protected area, material access area, controlled access area, vital area, or other (specify area).
3. For power reactors, the operating phase, e.g., shut-down, operating.
4. Safety systems affected or threatened, directly or indirectly.
5. Type of security force onsite (proprietary or contract).
6. Number and type of personnel involved, e.g., contractors, security, visitors, NRC personnel, other (specify).
7. Method of discovery of incident, e.g., routine inspection, test, maintenance, alarm, chance, informant, communicated threat, unusual circumstances (give details).
8. Procedural errors involved, if applicable.
9. Immediate actions taken in response to event.
10. Corrective actions taken or planned.
11. Local, State, or Federal law enforcement agencies contacted.
12. Description of media interest and press release.
13. Indication of previous similar events.
14. Knowledgeable contact.

For security system failures, provide the following in addition to Items 1 through 14:

15. Description of failed or malfunctioned equipment (including manufacturer and model number).
16. Apparent cause of each component or system failure. (For uncompensated security computer failures, state the reason the event could not be compensated and list specific components affected, e.g., central processor, peripheral/terminal equipment, software.)
17. Status of the equipment prior to the event (e.g., operating, being maintained, made secure) and compensatory measures in place.
18. Secondary functions affected (for multiple-function components).
19. Effect on plant safety.
20. Unusual conditions that may have contributed to failure, e.g., environmental extremes.

For threat-related incidents, provide the following in addition to Items 1 through 14:

21. Number of perpetrators.
22. Type of threat, e.g., bomb, extortion.
23. Means of communication, e.g., letter, telephone.

24. Text of threat.

25. Mode of operation.

26. Clear photocopy of threat letter and accompanying envelope if applicable.

Licensees should submit one copy of each written report to the U.S. Nuclear Regulatory Commission, Document Control Desk, Washington, DC 20555, and one copy to the appropriate Regional Office listed in Appendix A to 10 CFR Part 73. If pertinent information or errors are uncovered after the initial telephone report or the written report is submitted, the licensee should notify the NRC Operations Center by telephone of the information or errors. If the information is uncovered after the written report has been submitted, the licensee should submit a complete revised written report with revisions indicated to the Document Control Desk and the Regional Office. The revised report should be complete and should not contain only the supplementary or revised information.

### 3.3 Maintenance and Quarterly Submittal of Log

Events reportable under paragraph 73.71(c) only need to be logged. In maintaining the log, it is recommended that the licensee log the information as received and then summarize and update the log entry when the event terminates. However, licensees are required by paragraph 73.71(c) to log entries within 24 hours of the discovery of the event. Since the licensee would immediately investigate all events that threatened nuclear activities or lessened the effectiveness of the security system, the details would generally be available when the entry was made in the log. Log entries should include as a minimum:

1. Date and time of the event;

2. Brief (one-line) description of the event;

3. Brief (one-line) description of compensatory or corrective actions taken;

4. Area affected, e.g., vital area, protected area, owner controlled, transport; and

5. How detected, e.g., alarm, routine inspections, patrol, informants.

Every 3 months, the licensee is required to submit one copy of all log entries not previously submitted to the NRC Document Control Desk. The log entries need not be typed as long as they are legible; a photocopy is acceptable. Licensees are permitted a 30-day grace period for all log submittals.

Events of a similar nature that are logged and submitted to the NRC under paragraph 73.71(c) may be consolidated into a single log entry if they occur repeatedly within the quarterly submittal period. The date and time should be specified for each occurrence of the event. For example, if there is a repeated occurrence of a compensated computer failure and each failure is the result of the same problem, only one log entry providing the details of 1 through 5 above need be made. However, the date, time, and duration of the event should be recorded in the log for each occurrence.

Each log must be retained for 3 years after the last entry to that log.

## APPENDIX A

## GLOSSARY

**NOTE:** This glossary only applies to the requirements of §73.71 of 10 CFR Part 73.

***Any failure, degradation, or discovered vulnerability***: The cessation of proper functioning or performance of equipment, personnel, or procedures that compose the physical protection program necessary to meet Part 73 requirements, or a discovered defect in such equipment, personnel, or procedures that degrades function or performance.

***Credible threat***: A threat should be considered credible when (1) physical evidence supporting the threat exists, (2) information independent from the actual threat message exists that supports the threat, or (3) a specific group or organization claims responsibility for the threat.

***Dedicated observer***: A person, not necessarily a member of the security force, posted as a temporary compensatory measure for a degraded assessment or detection capability or both. While performing this function, duties must be limited to detection and assessment. As a minimum, the person must be able to view the entire area affected by the degradation and must be able to communicate with the central alarm station.

***Diversion of SNM***: Unauthorized movement of SNM by individuals authorized access to or control over the material.

***False alarm***: An alarm generated without an apparent cause. Investigation discloses no evidence of a valid alarm condition, including tampering, no nuisance alarm conditions, and no equipment malfunction.

***Interruption of normal operation***: The cessation of normal operation that, if accomplished, would result in substantial economic harm or cost to the licensee.

***Loss of SNM***: (1) A failure to measure or account for material by the material control and accounting system approved for the facility when the material is authorized to be possessed by the licensee and is not confirmed stolen or diverted or (2) an accidental (i.e., unplanned) offsite release or dispersal of SNM known or suspected to be 10 times greater than normal operating losses for the time in question, whether or not the release is measured. The term loss implies that a search has been conducted to confirm the material is missing. For fixed sites, this search should be conducted within the 1-hour time for reporting.

***"Lost" versus "unaccounted for" in regard to transportation of material***: The term "lost" covers material that is no longer in the possession of the party authorized to possess it during a specific time period, and a search for the material has verified the loss. "Unaccounted for" refers to material in transit that has not arrived at its delivery point 4 hours or more after the estimated arrival time; however, a search has not confirmed the material to be lost.

***Nuisance alarm***: An alarm generated by an identified input that does not represent a safeguards threat. Nuisance alarms may be caused by environmental (rain, sleet, snow, lightning) or mechanical (natural objects such as animals or tall grass) factors.

***Properly compensated***: Measures, including backup equipment, additional security personnel, and specific procedures, taken to ensure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security-related equipment or structures. Preplanned compensatory measures are normally described in NRC-approved safeguards plans.

***Safeguards event***: Any incident representing an attempted, threatened, or actual breach of the safeguards system or reduction of the operational effectiveness of that system.

***Safeguards Event Log***: A compilation of log entries for the events described in Section II of Appendix G to 10 CFR Part 73. Entries must include the date and time of the event, a description of the event, and any action taken. Repeated events may be consolidated into a single log entry with the date, time, and duration of each event recorded for each occurrence. The ongoing safeguards event log may be maintained in more than one location onsite. The log may be typed or handwritten as long as it is legible and reproducible. Entries in a safeguards event log submitted to the NRC need not be in time-sequential order.

***Safeguards system***: The equipment, personnel, and procedures that make up the physical protection program necessary to meet Part 73 requirements.

***Significant physical damage***: Physical damage to the extent that the facility, equipment, transport, or fuel cannot perform its normal function (applies to a power reactor, a facility possessing SSNM or its equipment, carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel a facility or carrier possesses).

***Tampering***: When used in connection with Appendix G to 10 CFR Part 73, altering for improper purposes or in an improper manner.

***Theft of SNM***: The unauthorized taking of SNM for unauthorized use.

***Unauthorized person***: Any unescorted person in an area to which the person is not authorized unescorted access.

## APPENDIX B

## SAMPLE LOG ENTRIES

Safeguards events reportable under paragraph 73.71(c) of 10 CFR Part 73 need only be logged within 24 hours of their discovery. The copy of the log (photocopy) submitted to the NRC every 3 months does not have to be typewritten, but it must be legible. The sample log items presented here should not be considered all-inclusive.

| | LOG ENTRY DATE/TIME | EVENT DATE/TIME | EVENT | RESPONSE |
|---|---|---|---|---|
| 1. | 1-8-87/0140 | 1-8-87/0130 | CAS operator received telephone bomb threat from unidentified male. Bomb reported near diesel generator. | Area search initiated at 0135 hrs, completed 0140 hrs, nothing found. |
| 2. | 1-8-87/1245 | 1-8-87/1043 | Delivery truck significantly damaged PA fence in zone No. 4. Discovered at 1047 by security patrol, no PA or VA alarms received. | Guard posted at 1050 hrs, relieving patrol (immediate comp), PA searched. |
| 3. | 1-9-87/1605 | 1-9-87/1433 | Card reader failure at VA portal No. 2. | At 1440 hrs, posted guard with current access list. System failure corrected and operational at 1600 hrs. |
| 4. | 1-9-87/1815 | 1-9-87/1730 | I.D. badge No. 342 lost onsite. | Badge cancelled 1732 hrs. Badge found on employee's jacket at 1745 hrs. |
| 5. | 1-9-87/2055 | 1-9-87/2025 | Security system failure, single CPU outage. | Determined caused by electrical storm/power surge. System back on line at 2028 hrs. All VA portals confirmed locked and alarmed by security. |
| 6. | 1-10-87/1410 | 1-10-87/1405 | Fence repaired. (See Entry No. 2.) | Compensatory post discontinued at 1405. |
| 7. | 1-12-87/1100 | 1-12-87/0812<br>1-12-87/0815<br>1-12-87/0817<br>1-12-87/0819<br>1-12-87/0823 | Perimeter fence alarms received zone No. 4. | Area searched by security patrol. No apparent cause for alarms. Security posted after third alarm and maintenance called to check system. System function verified through test each occurrence. All actions completed 1035. |
| 8. | 1-12-87/1610 | 1-12-87/1443 | CCTV failure, perimeter zone No. 2 (IDS operational). | Dedicated observer in place 1450 hrs. No alarms received. Camera replaced and operational at 1610. |
| 9. | 1-12-87/2015 | 1-12-87/2007 | See No. 5 above. | Same as No. 5 above. System on-line at 2011 hrs. |
| 10. | 1-12-87/2350 | 1-12-87/2230 | Latch alarm received on VA portal No. 6. Responder found door slightly ajar. | Guard posted at 2238. Area searched, no abnormalities found. Maintenance request initiated at 2315. |

*U. S. GOVERNMENT PRINTING OFFICE: 1987- 202-292:60277

## VALUE/IMPACT STATEMENT

A separate value/impact statement has not been prepared for this regulatory guide. The guide was revised to provide guidance on reporting physical security events in accordance with paragraphs 73.71(a) through (c) of 10 CFR Part 73. A regulatory analysis was prepared for the proposed revisions to § 73.71 and was made available in the NRC Public Document Room at the time of publication (August 27, 1985–50 FR 34708). This regulatory analysis is also appropriate for this regulatory guide.