U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

December 1997
Division 5
Draft DG-5008

DRAFT REGULATORY GUIDE

Contact: R.P. Rosano (301)415-3282

DRAFT REGULATORY GUIDE DG-5008

(Proposed Revision 2 of Regulatory Guide 5.62)

REPORTING OF SAFEGUARDS EVENTS

A. INTRODUCTION

In 10 CFR Part 73, "Physical Protection of Plants and Materials," Section 73.71 requires licensees to report to the Operations Center of the NRC or to record in a log certain safeguards events. The events to be reported are those that threaten nuclear activities or lessen the effectiveness of the physical protection system established by safeguards regulations and the licensees' approved physical protection and contingency plans.

This regulatory guide provides guidance acceptable to the NRC staff for use by licensees in determining when and how events should be reported. This guide is being revised to (1) incorporate pertinent points of Generic Letter 91-03[1] ("Reporting of Safeguards Events," March 6, 1991), (2) incorporate changes to the regulations, such as the rescission of the requirement to submit quarterly event logs to the NRC, and (3) clarify reporting requirements that might have been misunderstood by the industry in the past. The examples provided represent the types of events that should be reported and are not intended to be all-inclusive.

[1]Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343. GL 91-03 is also available on NRC's home page at http://www.nrc.gov/NRC/FEDWORLD/index.html under Generic Communications.

Regulatory guides are issued to describe to the public methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, to explain techniques used by the staff in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. Regulatory guides are issued in draft form for public comment to involve the public in developing the regulatory positions. Draft regulatory guides have not received complete staff review; they therefore do not represent official NRC staff positions.

The information collections contained in this draft regulatory guide are covered by the requirements of 10 CFR Part 73, which were approved by the Office of Management and Budget, approval number 3150-0002. The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

B. DISCUSSION

The information reportable under 10 CFR 73.71 is required so that the NRC may stay informed of safeguards-related events that could endanger public health and safety or national security and which could generate public inquiries. The required information permits analysis of safeguards system reliability and availability.

Certain significant safeguards events warrant immediate involvement by the NRC and other government agencies such as the FBI; therefore, these events must be reported by telephone to the NRC within one hour of discovery of the event, followed by a detailed written report within 30 days.

Certain less significant safeguards events must be recorded in a log and copies of the log must be maintained by the licensee for three years. The log entries allow the NRC to analyze repeated events at a particular site and similar events among licensees. If an event occurs repeatedly at one facility or throughout the industry, it may represent a generic issue or a defect in a physical protection program.

For the purposes of this guide and for understanding the regulations, a glossary is provided as Appendix A of this guide.

C. REGULATORY POSITION

1. LICENSEES SUBJECT TO 10 CFR 73.71

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

Licensees who are subject to the provisions of 10 CFR 73.20, 73.37, 73.50, 73.55, 73.60, or 73.67 are subject to the provisions of 10 CFR 73.71(b) for events described in Paragraph (I)(a)(1) of Appendix G, "Reportable Safeguards Events," to Part 73. Licensees subject to the provisions of 10 CFR 73.20, 73.37, 73.50, 73.55, 73.60, or each licensee possessing strategic special nuclear material (SSNM) and subject to 10 CFR 73.67(d), are subject to the provisions of 10 CFR 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 10 CFR 73.20, 73.37, 73.50, or 73.60 are subject to the provisions of 10 CFR 73.71(b) for events described in paragraph I(d) of Appendix G to Part 73.

Licensees subject to the provisions of 10 CFR 73.20, 73.37, 73.50, 73.55, 73.60, or each licensee possessing SSNM and subject to 10 CFR 73.67(d) are subject to the provisions of 10 CFR 73.71(c).

2. REPORTABLE EVENTS

2.1 Safeguards Events To Be Reported Within One Hour

According to 10 CFR 73.71(a) and (b), certain events must be reported within one hour of discovery. Events under 10 CFR 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 must be submitted to the NRC within 30 days on each event that is reported within one hour. Safeguards events reportable under 10 CFR 73.71(b) are described in Section I of Appendix G to 10 CFR Part 73:

(a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause:

(1) A theft or unlawful diversion of special nuclear material; or

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

(3) 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.

(b) An actual entry of an unauthorized person into a protected area, material access area, controlled access area, vital area, or transport. [See the Glossary in Appendix A to this guide for a definition of "unauthorized person."]

(c) Any failure, degradation, or the discovered vulnerability in a safeguard system that could allow unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport for which compensatory measures have not been employed.

(d) The actual or attempted introduction of contraband into a protected area, material access area, vital area, or transport.

Safeguards systems include equipment, procedures, and personnel practices; therefore, failures include not only mechanical and electrical system failures but also improper security procedures and inadequate or inadequately implemented personnel practices. Discovered vulnerabilities include significant flaws in the physical protection system that could result in a reduction in overall protection at the site.

2.2 Examples of Safeguards Events To Be Reported Within One Hour

The following are examples of events that should be reported to the NRC within one hour because of their potential to endanger public health and safety or national security. This list should not be considered all-inclusive. The applicable portion of Appendix G to Part 73 is cited for each example, and compensatory measures that are acceptable to the NRC staff are discussed in Appendix C to this guide.

1. Events involving actual or attempted theft or diversion of SNM, attempts to steal or divert a shipment of spent fuel, significant physical damage to a power reactor, or tampering that causes or has the potential to cause an interruption of the normal operation of a licensed nuclear power reactor. (Paragraphs I(a)(1), I(a)(2), and I(a)(3) of Appendix G) There are no compensatory measures that would preclude reporting this event within one hour.

2. Bomb threat or extortion threats. (Paragraphs I(a)(2) and I(a)(3) of Appendix G) There are no compensatory measures that would preclude reporting this event within one hour.

3. Discovery of criminal acts that have a connection to plant operations or discovery of a conspiracy to bomb the facility or sabotage its vital components. (Paragraphs I(a)(2), I(a)(3), I(c), and I(d) of Appendix G) There are no compensatory measures that would preclude reporting this event within one hour.

4. Discovery of theft or loss of classified documents or significant unclassified safeguards information outside the protected area pertaining to facility or transport safeguards for which compensatory measures have not been implemented. (Paragraph I(c) of Appendix G) (Note: This is also reportable under 10 CFR 95.57 for classified information.) The licensee should also report results of a search for the classified documents or safeguards information. See Example 12 of Regulatory Position 2.4 for similar examples involving loss, not theft, of such information. There are no compensatory measures that would preclude reporting this event within one hour.

5. Fire or explosion of suspicious or unknown origin within the isolation zone, protected area, controlled access area, material access area, or vital area. (Note: Events reportable under 10 CFR 50.72 or 50.73 do not require duplicate reports under 10 CFR 73.71.) (Paragraphs I(a)(2), I(a)(3), and I(c) of Appendix G) See Example 4 of Regulatory Position 2.5 for similar examples that need not be reported or logged. There are no compensatory measures that would preclude reporting this event within one hour.

6. Discovery of a suspicious vehicle following a licensed carrier transporting formula quantities of SSNM. (Paragraph I(a)(1) of Appendix G) See Example 5 of Regulatory Position 2.5 for similar examples that need not be reported or logged. There are no compensatory measures that would preclude reporting this event within one hour.

7. Complete loss of offsite communications. (Paragraph I(a)(2) or (3) of Appendix G) If offsite communications are restored within one hour of the loss, the licensee should

report this event immediately after restoration of communications. If communications cannot be restored within one hour of the loss, the licensee should use alternative means to notify the NRC. There are no compensatory measures that would preclude reporting this event within one hour.

8. Mass demonstration or other civil disturbance at or near the plant site that could pose a threat to the facility. (Paragraphs I(a)(2), I(a)(3), I(b), or I(d) of Appendix G) There are no compensatory measures that would preclude reporting this event within one hour.

9. Tampering with safety or physical protection equipment that is confirmed to be of malevolent or suspicious origin. (Paragraphs I(a)(1), I(a)(2), I(a)(3), I(b), I(c), or I(d) of Appendix G) See Example 6 of Regulatory Position 2.5 for similar examples that need not be reported or logged. There are no compensatory measures that would preclude reporting this event within one hour.

10. An assault on a power reactor, facility, or transport possessing or transporting SSNM regardless of whether perimeter penetration is achieved. (Paragraphs I(a)(2), I(a)(3), I(b), or I(d) of Appendix G) There are no compensatory measures that would preclude reporting this event within one hour.

11. Discovery of falsified identification badges or key cards. (Paragraph I(a) of Appendix G) There are no compensatory measures that would preclude reporting this event within one hour; however, steps 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.

12. Discovery of uncompensated and unaccounted for, lost, or stolen key cards, identification card blanks, keys, or any access device that could allow unauthorized or undetected access to protected areas, controlled access areas, or vital areas. (Paragraph I(c) of Appendix G) See Example 6 of Regulatory Position 2.4 for similar examples that need only be logged. See Appendix C for a discussion of acceptable compensatory measures.

13. 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)

14. Uncompensated loss of the ability to detect intrusion (a) at the protected area perimeter when the loss involves several intrusion detection system zones or (b) within a single intrusion detection system zone when the condition could become known to a person not authorized unescorted access, either because it lasts for a considerable time or is visually conspicuous to the casual observer. (Paragraph I(c) of Appendix G) See Examples 3 and 4 of Regulatory Position 2.4 for similar examples that need only to be logged.

15. Uncompensated loss of alarm capability or locking mechanism on a vital area portal. (Paragraph I(c) of Appendix G) See Example 9 in Regulatory Position 2.4 for similar examples that need only to be logged.

16. Improper control (to include loss or offsite removal) of access control media, including picture badges, keys, key cards, or access control computer codes, that results in someone using the medium during the time that it is not controlled. ("Improper control," as used here, does not include approved systems allowing employees to take badges offsite.) See Example 18.7 of Regulatory Position 2.4 for similar examples that need only to be logged. See Example 9 of Regulatory Position 2.5 for similar examples that need not be reported or logged.

17. Incomplete or inaccurate preemployment screening records (to include falsification of background information or inadequate administration, control, or evaluation of psychological tests) if the licensee would have denied unescorted access based on knowledge of the complete or accurate information, had a complete preemployment screening been done. See Example 18.9 of Regulatory Position 2.4 for similar examples that need only to be logged.

18. Unavailability of a minimum number of security personnel or an actual or imminent strike by the guard force. (Paragraph I(c) of Appendix G)

19. Loss of a security weapon onsite that is not retrieved within one hour of the discovery of its loss. See Example 13 of Regulatory Position 2.4 for similar examples that need only to be logged.

20. Loss of alarm capability or locking mechanism on a material access area portal.

21. Discovery of unaccounted for, lost, or stolen keycards, identification card blanks, keys, or any access device that could allow unauthorized or undetected access to material access areas.

22. At a fuel facility, loss of the capability at a single alarm station to monitor or remotely assess alarms.

2.3 Safeguards Events To Be Logged

The following safeguards events are reportable under 10 CFR 73.71(c) and described in Section II of Appendix G to 10 CFR Part 73; they need only to be logged within 24 hours of their discovery.

1. Any failure, degradation, or discovered vulnerability in a physical protection system that could have allowed unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport had compensatory measures not been established. (If compensatory measures had not been established, this report would be required within one hour. See Paragraph I(c) of Appendix G.) 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 failure of the physical protection system. See Appendix C to this guide for a discussion of acceptable compensatory measures.

2. Any other threatened, attempted, or committed act not previously defined in Appendix G to Part 73 that could reduce the effectiveness of the physical protection system below that committed to in a licensed physical protection or contingency plan or the actual condition of such reduction in effectiveness.

False alarms generally need not be reported or logged. However, if false or nuisance alarm rates significantly reduce the effectiveness of the system, 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 Logged

The following are examples of events that are less significant than those reportable within one hour, and they must be logged. 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)

2. Properly compensated vital area card reader failures. (Paragraph II(a) of Appendix G)

3. Loss of ability to detect within a single intrusion detection system zone for a short period of time. See Example 14 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

4. Properly compensated loss of the ability to detect intrusion (a) at the protected area perimeter when the loss involves several intrusion detection system zones or (b) within a single intrusion detection system zone when the condition could become known to a person not authorized unescorted access, either because it lasts for a considerable time or is visually conspicuous to the casual observer. (Paragraph I(c) of Appendix G) See Example 14 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

5. Properly compensated failure or degradation of a single perimeter lighting zone below the acceptable standard described in the physical security plan, if the intrusion detection system remains operational. (Paragraph II(a) of Appendix G)

6. Accidental removal offsite or loss of access badge or other access medium, if measures have been taken within 10 minutes of the discovery of the loss to preclude

the use of the badge to gain access to a controlled area and to ensure that the badge has not been used in an unauthorized manner. If an access control system also uses biometrics, the loss of an access badge or keycard does not need to be logged. (Paragraph II(a) of Appendix G) See Example 12 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

7. Properly compensated loss of either alarm or locking mechanism on a vital area portal. (Paragraph II(a) of Appendix G) See Example 15 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

8. Security computer failures that have the potential to reduce the effectiveness of the physical protection system. (Paragraph II(b) of Appendix G)

9. Properly compensated loss of alarms, closed circuit television, or security computers.[2] The loss of backup capability may also be only logged if immediate restoration of system capability is provided by activating secondary computers. See Examples 15 and 16 in Regulatory Position 2.2 for similar examples that must be reported within one hour.

10. At a power reactor, 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)

11. 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)

12. Loss of unclassified safeguards information when there does not appear to be evidence of theft and, within the first hour after the discovery, the information is retrieved and determined not to have been in the possession of an unauthorized

[2] 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.

person, or theft of such information when (i) the information would not have allowed unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport, or (ii) the vulnerability caused by the loss of the information is fully compensated upon discovery. See Example 4 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

13. Loss of a security weapon onsite that is retrieved within one hour of the discovery of its loss. See Example 19 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

14. Properly compensated closed circuit television failure in a single zone while the intrusion detection system remains operational. (Paragraph II(a) of Appendix G)[2]

15. A design flaw or vulnerability in the physical barrier of a protected area, controlled access area, or vital area that could have allowed unauthorized access. (Paragraph II(a) of Appendix G)

16. Discovery of contraband inside the protected area that is not a significant threat. (Paragraph II(b) of Appendix G)

17. Compromise of safeguards information that would not significantly assist an individual in gaining unauthorized or undetected access to a facility or would not significantly assist an individual in an act of radiological sabotage or theft of SNM. (Paragraph II(a) of Appendix G)

18. Partial failure of an otherwise satisfactory access authorization or access control program. The following are examples of partial failure.

    18.1 An employee or vendor who has been cleared and authorized to receive a badge permitting unescorted access to protected and vital areas inadvertently enters the protected area improperly, e.g., through a vehicle gate, without being searched and issued a badge. The licensee discovers the event, searches the individual, issues a badge, and takes corrective action to prevent recurrence.

18.2 Search equipment does not perform properly, which could allow unsearched individuals to enter the protected area, and the licensee does not detect the failure for a short period. See Example 8 in Regulatory Position 2.5 for similar examples that do not need to be reported or logged.

18.3 An individual who is required to have an escort for a particular area inadvertently becomes separated from his or her escort but the escort or another person authorized for unescorted access recognizes the situation within several minutes and corrects it.

18.4 An employee of a licensee or contractor who is authorized entry to a vital area enters that vital area improperly without realizing that the card reader is processing a preceding employee's card, or the employee walks in behind another employee without using a key card.

18.5 An individual enters a vital area to which he or she is authorized unescorted access by mistakenly using an access control medium (key card or badge) intended for another individual who is also authorized unescorted access to the area.

18.6 An individual is incorrectly issued a badge granting access to vital areas to which he or she is not authorized, but does not enter any vital areas or does not enter any vital areas with malevolent intent. Another example is an individual who is incorrectly issued a badge but cannot reasonably use it because he or she does not know the personal identification number needed to enter the area, and the event is promptly discovered and corrected by the licensee.

18.7 Improper control (to include loss or offsite removal) of access control media, including picture badges, keys, key cards, or access control computer codes, that could be used to gain unauthorized or undetected access, when the event is discovered and corrected by the licensee. See Example 16 in Regulatory Position 2.2 for similar examples that must be reported within one hour. See

Example 9 in Regulatory Position 2.5 for similar examples that need not be reported or logged.

18.8 Card reader failure that causes vital area doors to unlock in the open position or to lock in the closed position but with no functional door alarm. See Example 10 of Regulatory Position 2.5 for similar examples that need not be reported or logged.

18.9 Incomplete or inaccurate preemployment screening records or inadequate administration, control, or evaluation of psychological tests that would not necessarily have resulted in a denial of access. See Example 17 of Regulatory Position 2.2 for similar examples that must be reported within one 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 that have 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 material access area or vital area barrier for a legitimate reason (e.g., to install a pipe) with prior approval, coordination with security, and proper compensatory measures.

2. A child attempting to climb a protected area fence.

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 physical protection plan or do not degrade system effectiveness.

4. A fire or explosion if the origin can be determined, within one hour, to be nonsuspicious and the facility sustains no significant damage. See Example 5 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

5. A suspicious vehicle following a transport that is determined, within one hour, not to be a threat. See Example 6 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

6. Suspected tampering with safety equipment that is determined, within one hour, not to be tampering. See Example 9 of Regulatory Position 2.2 for similar examples that must be reported within one hour.

7. Discovery of vehicular emergency equipment such as safety flares during entrance searches, unless the introduction was done for malevolent purposes.

8. Failure of search equipment if the failure is discovered by the licensee before anyone goes through unsearched and the licensee uses other equipment with the same capabilities (such as hand-held or walk-through search devices). See Example 18.2 of Regulatory Position 2.4 for similar examples that need to be logged.

9. Improper control (to include loss or offsite removal) of access control media, including picture badges, keys, key cards, or access control computer codes, that the licensee determines could not be used to gain unauthorized or undetected access. See Example 16 of Regulatory Position 2.2 for similar examples that must be reported within one hour. See Example 18.7 of Regulatory Position 2.4 for similar examples that need only to be logged.

10. Card reader failure that causes vital area doors to lock in the closed position but the door alarm functions properly, provided that access control measures are implemented before allowing individuals into the vital areas. See Example 18.8 of Regulatory Position 2.4 for similar examples that need only to be logged.

3. PROCEDURES

3.1 Training of Non-Security Staff

Discovery of reportable events is not limited to members of the security organization. It is recommended that all regular site employees receive security training to foster an

awareness of site security and be briefed on their responsibility to immediately notify site security of security anomalies.

3.2 Dual Reporting

Events of a dual nature (i.e., both having safety and safeguards implications and being subject to the requirements of 10 CFR 50.72, 50.73, and 73.71) do not require duplicate reports under the requirements of 10 CFR 73.71. If a power reactor licensee reports an event that is reportable in accordance with both 10 CFR 50.73 and 73.71, the procedures described in 10 CFR 50.73 (i.e., submittal of a licensee event report (LER)) must be followed. The procedures contained in NUREG-1022, "Licensee Event Report System,"[3] describe how to indicate that an LER meets multiple reporting requirements. Similarly, SNM licensees need not report more than once for events covered under both 10 CFR 70.52 and 73.71, or under both 10 CFR 74.11 and 73.71.

3.3 NRC Form 366

When submitting reports of events that are reportable solely under the provisions of 10 CFR 73.71, power reactor licensees should use LER Form 366; all other licensees should write a letter. The requirements of 10 CFR 73.21(g) must be met when transmitting safeguards information. In addition, when transmitting classified information, the requirements of 10 CFR 95.39 must be followed.

It is recognized that not all items of NRC Form 366 may apply when safeguards events are reported. Licensees should be sure that all the information needed by the NRC, as described in Regulatory Position 3.5 of this guide, is included on the form, whether under a specific item or in the text section.

---

[3] Copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are also available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

3.4 One-Hour Reports

When a licensee, licensee employee, or contract employee discovers an event reportable under 10 CFR 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 one hour of the discovery. Telephone notification should be made via the Emergency Notification System (ENS) if the licensee is a 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 one hour of discovery of the event. The commercial telephone number that may be used to contact the NRC Operations Center is (301)816-5100. Other methods that may be used to ensure notification within one hour include telegram, mailgram, or facsimile. Telegrams and mailgrams should be hand-delivered to the Operations Officer at the NRC Operations Center, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852. For information concerning facsimiles, telephone the NRC Operations Center at (301) 816-5100. 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 10 CFR 73.71(a), the licensee (or agent) should also notify the NRC Operations Center by telephone within one 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 10 CFR 73.71 may be transmitted over unprotected lines as permitted by the exemption in 10 CFR 73.21(g)(3).

3.5 30-Day Follow-Up Written Reports

A follow-up written report must be submitted within 30 days of a one 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. 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 additional pertinent 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.

3.6 Maintenance of Log

Events reportable under 10 CFR 73.71(c) only need to be logged. Each log must be retained for three years after the last entry to that log. 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 10 CFR 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 measure or corrective actions taken.
4. Area affected, e.g., vital area, protected area, material access area, owner-controlled area, transport.
5. How detected, e.g., alarm, routine inspection, patrol, informants.

APPENDIX A
GLOSSARY

NOTE: This glossary applies only to the requirements of 10 CFR 73.71.

Any failure, degradation, or discovered vulnerability. The cessation of proper functioning or performance of equipment, personnel, or procedures that are part of 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.

Contraband. Unauthorized materials, including firearms, explosives, and other tools or weapons useful in radiological sabotage, or materials that could be used to perpetrate or conceal a theft of SNM (e.g., shielding materials used to defeat SNM exit detectors or radioactive sources that could be used to falsely trigger an evacuation alarm).

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

Dedicated observer. A person, not necessarily a member of the guard 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 alarm station.

Diversion of SNM. Unauthorized removal of SNM.

False alarm. An alarm generated without an apparent cause. Investigation discloses no evidence of a valid alarm condition, such as tampering, nuisance alarm conditions, or equipment malfunction.

Interruption of normal operation. A departure from normal operation that, if accomplished, would result in a challenge to the plant safety systems.

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

Properly compensated. Measures, which may include backup equipment, security personnel, or 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 physical protection plans. (See Appendix C of this guide for more detail.)

Safeguards event. Any incident representing an attempted, threatened, or actual breach of the physical protection 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 should 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 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.

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. Altering for improper purposes or in an improper manner.

Theft of SNM. The unauthorized taking of SNM.

Unauthorized person. Any unescorted person in an area to which the person is not authorized unescorted access. This includes authorized and unauthorized persons who gain access in an unauthorized manner.

APPENDIX B

SAMPLE LOG ENTRIES

Safeguards events reportable under 10 CFR 73.71(c) need only be logged within 24 hours of their discovery. The sample log items presented here should not be considered all-inclusive.

	LOG ENTRY DATE/TIME	EVENT DATE/TIME	EVENT	RESPONSE
1.	1-8-97/0140	1-8-97/0130	CAS operator received telephone bomb threat from unidentified male. Bomb reported near diesel generator.	Area search initiated at 0135 hours, completed 0140 hours, nothing found.
2.	1-8-97/1245	1-8-97/1043	Delivery truck significantly damaged PA fence in zone No. 4. Discovered at 1047 by guard patrol, no PA or VA alarms received.	Guard posted at 1050 hours, relieving patrol (immediate comp.), PA searched.
3.	1-9-97/1605	1-9-97/1433	Card reader failure at VA portal No. 2.	At 1440 hours, posted guard with current access list. System failure corrected and operational at 1600 hours.
4.	1-9-97/1815	1-9-97/1730	ID badge No. 342 lost onsite.	Badge cancelled 1732 hours. Badge found on employee's jacket at 1745 hours.
5.	1-9-97/2055	1-9-97/2025	Security system failure, single CPU outage.	Determined caused by electrical storm/power surge. System back on line at 2028 hours. All VA portals confirmed locked and alarmed by guard force.
6.	1-10-97/1410	1-10-97/1405	Fence repaired (See Entry No. 2)	Compensatory post discontinued at 1405.

7.	1-12-97/1100	1-12-97/0812 1-12-97/0815 1-12-97/0817 1-12-97/0819 1-12-97/0823	Protected area fence alarms received from zone No. 4	Area searched by security patrol. No apparent cause for alarms. Guard posted after third alarm and maintenance called to check system. System function verified through test each occurrence. All actions completed 1035.
8.	1-12-97/1610	1-12-97/1443	CCTV failure, perimeter zone No. 2 (IDS operational)	Dedicated observer in place 1450 hrs. No alarms received. Camera replaced and operational at 1610.
9.	1-12-97/2015	1-12-97/2007	See No. 5 above.	Same as No. 5 above. System on-line at 2011 hours.
10.	1-12-97/2350	1-12-97/2230	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.

APPENDIX C

COMPENSATORY MEASURES

Credit may be taken for compensatory measures when deciding on the type of report and when it is due. The significance of the system defect or vulnerability is the key factor in determining whether the event should be reported in one hour or simply logged. Even compensatory measures implemented promptly after discovery of the defect or vulnerability cannot provide protection for the period of time that the defect or vulnerability existed. Therefore, any failure, degradation, or discovered vulnerability that is known to have existed for a significant period of time and that should or could have been discovered in the course of patrols, surveillance, operational tests, or other means should still be considered for reporting within one hour.

The following are examples of compensatory measures that could warrant credit for the licensee; these measures relate to the examples given in the text of this regulatory guide. Other compensatory measures may be used if they provide equivalent levels of protection.

Loss of alarm capability. With respect to material access areas or vital area portals, adequate compensation requires that a dedicated observer with appropriate communications capability be posted within 10 minutes of discovery of the loss and that the area be searched.

Failure of locking mechanism. With respect to material access area or vital area portals, adequate compensation requires that an armed security force member with appropriate communications capability be posted within 10 minutes of discovery and that the area be searched.

Loss of ability to monitor or remotely assess protected area alarms. Adequate compensation for such loss includes restoration of the original capability within 10 minutes of discovery of the event, or dedicated observers with appropriate communications capability posted within 10 minutes of the discovery if they are capable of observing each of the affected zones.

Loss of all power to security systems. The only compensatory measure that could reduce this event from a one-hour report to a loggable event is that the security system has been maintained throughout the event by standby power. The NRC does not consider immediate posting of guard personnel to be sufficient to relieve the need for a one-hour report of this event.

Loss of ability to detect intrusion at protected area perimeter. Adequate compensation for this failure would be (a) deployment of backup intrusion detection equipment within 10 minutes of discovery or (b) posting a dedicated observer capable of monitoring each affected zone with suitable communications equipment for contacting alarm stations.

Security computer failure. Compensatory measures for this failure include restoration of the computer, deployment of a backup computer system, or posting security personnel capable of providing an equivalent level of protection, all within 10 minutes of discovery of the failure.

Vital area card readers. An acceptable compensatory measure for this failure would be posting a security force member with appropriate access lists and communications capability at each door.

VALUE/IMPACT STATEMENT

A separate value/impact statement has not been prepared for this regulatory guide. The guide is being revised to provide additional guidance on reporting safeguards events in accordance with 10 CFR 73.71(a) through (c). A regulatory analysis was prepared for the proposed revisions to 10 CFR 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.

Federal Recycling Program

☆ U.S. GOVERNMENT PRINTING OFFICE: 1997 432-374/80006

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67