



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

JUL 08 1983

MEMORANDUM FOR: Those on Attached List

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

SUBJECT: PROPOSED REVISIONS TO 10 CFR §73.71,
SAFEGUARDS REPORTING REQUIREMENTS

Attached for your review is a proposed revision to 10 CFR §73.71, Reporting Requirements for Safeguards Events. Also enclosed is an Appendix to Part 73 describing the events to be reported and a draft guide.

The purpose of these revisions is to clarify the reporting requirements and to provide standardization of event categorization. Also, please note that the proposal extends the time period for the submission of written follow-up reports to 30 days, making it compatible with 10 CFR Part 50, Licensee Event Reports (LERs).

We would appreciate your written comments or concurrence by July 21, 1983. The NMSS contact on this matter is Julie Metzger, FTS-427-4010.

A handwritten signature in cursive script, appearing to read "Robert F. Burnett".

Robert F. Burnett, Director
Division of Safeguards, NMSS

Addressees:

Harold R. Denton, Director, NRR
Clemens J. Heltemes, Director, AEOD
Guy H. Cunningham, Director, ELD
Richard C. DeYoung, Director, IE
Thomas E. Murley, Regional Administrator, RI
James P. O'Reilly, Regional Administrator, RII
James G. Keppler, Regional Administrator, RIII
John T. Collins, Regional Administrator, Region IV
John B. Martin, Regional Administrator, Region V

Draft Rule Revision §73.71(a)

Comparative Text

§73.71 Reports of unaccounted for shipments, suspected thefts, unlawful diversion and other safeguards events.

- (a) Each licensee who conducts a trace investigation of a lost or unaccounted for shipment pursuant to §73.27(c) shall notify the NRC Operations Center via the Emergency Notification System as soon as possible, and in all cases within one hour, of the details and results of its trace investigation. If the Emergency Notification System is inoperative or unavailable, the licensee shall make the required notifications via commercial telephone service, other dedicated telephone systems, or any other method which will ensure a report being made promptly to the NRC Operations Center. Each licensee who conducts a trace investigation of a lost or unaccounted for shipment pursuant to §73.67(e)(3)(vi) or §73.67(g)(3)(iii) shall notify the NRC Operations Center via commercial telephone using the number provided in Appendix A as soon as possible, and in all cases within one hour of the details and results of its trace investigation. The licensee shall also file within a period of thirty (30) [~~fifteen (15)~~] days a written report to the appropriate NRC Regional Office setting forth the details and results of the trace investigation. A copy of this written report must be sent to the Director, Office of Inspection and Enforcement, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555.

Comparative Text

(b) Each licensee shall notify the NRC Operations Center via the emergency Notification System as soon as possible, and in all cases within one hour of any safeguards event as described in Appendix E of this Part. [~~incident in which an attempt has been made, or is believed to have been made, to commit a theft or unlawful diversion of special nuclear material which it is licensed to possess, or to commit an act of sabotage against its plant or transportation system.~~] If the Emergency Notification System is inoperative or unavailable, the licensee shall make the required notifications via commercial telephone service, other dedicated telephone systems, or any other method which will ensure a report being made promptly to the NRC Operations Center. The licensee shall, upon request of the NRC, maintain an open and continuous communication channel with the NRC Operations Center. The initial notifications must be followed within a period of [~~fifteen (15)~~] thirty (30) days by a written report....

* (c) Each licensee subject to the provisions of §§73.20, 73.37, 73.50, and 73.55 shall maintain a current log and record the following safeguards events within 24 hours of discovery:

- (i) any failure of the safeguards system as defined in Appendix E, paragraph (d) of this Part for which compensatory measures have been established in accordance with the licensee's physical protection plan or contingency plan, or
- (ii) any failure of the physical protection system not included in paragraph (d) of Appendix E provided that such failure decreases the operational effectiveness of the system.

*Due to substantial changes to paragraph (c), it is not in comparative text.

Each licensee shall provide quarterly copies of the log to the NRC Document Control Desk, U.S. Nuclear Regulatory Commission, Washington, DC, 20555.

APPENDIX E

Pursuant to the provisions of §73.71(b) and (c) of 10 CFR Part 73, Reporting Requirements for Safeguards Events, licensees shall report the following safeguards events within one hour of discovery to the NRC Operations Center:

- (a) Any event in which there is reason to believe that a person has destroyed or caused physical damage to, or attempted to or threatened to destroy or cause physical damage to -
- 1) any production facility or utilization facility or fuel cycle facility
 - 2) any nuclear waste storage facility, or
 - 3) any nuclear fuel for such a utilization facility, or any spent fuel from such a facility.
- (b) Any event in which there is a reason to believe that a person has caused or attempted to cause or threatened to cause interruption of normal operation of any such facility through the unauthorized use of or tampering with the machinery, components or controls of any such facility. →
- (c) Any incident in which an attempt has been made or believed to have been made or is threatened to be made to commit a theft or unlawful diversion of special nuclear material which it is licensed to possess.
- (d) Any failure of the safeguards system that could allow unauthorized and undetected access to a material access area, vital island or protected area or to irradiated nuclear fuel at fixed sites and in transit, or SSNM at fixed sites, authorized to possess formula quantities of SSNM, or SSNM

in transit when such shipments involve formula quantities of SSNM, provided compensatory measures are not established in accordance with the licensee's physical protection plan or contingency plan. (If compensatory measures are established in accordance with these plans, then log entry is required.)

- (e) Complete loss of offsite communications ability. This event should be reported within one hour, if possible or immediately after the restoration of offsite communication ability.
- (f) Any safeguards event or situation not described above, related to the public health and safety for which a news release is planned or notification to other government agencies has been or will be made.

A. Introduction

Paragraphs 73.71(b) and (c) of 10 CFR Part 73 "Physical Protection of Plants and Materials" require that the licensees report to the Operations Center of the Nuclear Regulatory Commission certain events which threaten nuclear activities or lessen the effectiveness of their physical security systems as established by safeguards regulations or the approved security and/or contingency plan.

This regulatory guide provides an approach acceptable to the NRC staff for determining when and how an event should be reported.

B. Discussion

The Commission requires the data described in §73.71(b) and (c) for two reasons. First, the NRC needs to be informed of significant events with a potential to endanger public health and safety in order to respond promptly with the appropriate actions. This is especially important for events reportable under paragraph (b). Secondly, when the potential for harm is less severe, as for the events recorded under paragraph (c), the NRC needs the information to monitor trends in security systems effectiveness with the intention of determining ways to improve overall security operations at facilities.

Events in Appendix E are telephonically reported within one hour because the events are significant enough to warrant immediate involvement of the NRC and other government agencies such as the FBI. Events reportable under paragraph (c) have less stringent requirements because the potential for harm to the public is less severe.

Licensees subject to the provisions of §§ 73.20, 73.37, 73.50, and 73.55 are required to meet the provisions of § 73.71(b) and (c).

C. Regulatory Position

I. Safeguards Events Reportable Under § 73.71(b)

Events of concern under § 73.71(b) as described in Appendix E, fall into three categories: acts of tampering or destruction, acts of theft and safeguards systems failures. The first two categories include all incidents in which an attempt has been made, is believed to have been made or has been threatened. The third category includes all uncompensated safeguards systems failures that could be directly exploited to obtain access to material access areas, vital islands, protected areas, or to irradiated fuel at fixed sites and in transit or SSNM at fixed sites, authorized to possess formula quantities of SSNM, or SSNM in transit, when such shipments involve formula quantities of SSNM. All events described in § 73.71(b) must be reported telephonically to the NRC Operations Center within one hour, followed by a written report within 30 days. Reports made pursuant to § 73.71(b) can be transmitted over unprotected telephone lines as provided by the exemption in 73.21(g)(3). See Appendix A for the appropriate format for written reports.

Acts of Theft, Tampering or Destruction

As required by § 73.71(b) acts, attempts, and threats of theft or destruction as described in Appendix E of Part 73 should be reported within one hour to the NRC Operations Center, followed in thirty days by a written report.

*7.1
sample of act of tampering or destruction*

method of tampering or destruction

Acts of theft, tampering or destruction are described in paragraphs (a), (b) and (c) of Appendix E of Part 73. In all cases, the licensee should report the incident as a safeguards event and provide information as outlined in "Guidelines for Written Reports and Log Entries," Appendix B.

The NRC will further categorize events when sufficient information has been gathered or when applicable, an investigation has been completed.

Examples of Threat-Related Events That Should be Reported

For events that have been "threatened," the licensee should establish reasonable belief that an act of theft, tampering or destruction will be attempted. Reasonable belief is established under the following circumstances: 1) when physical evidence exists that such an act may occur, or 2) when the licensee receives information that there is reason to believe an act of theft, tampering or destruction might be attempted.

The following list provides examples of events to be reported to the NRC within one hour of discovery because of their potential to result in an act of theft, tampering or destruction, or because of the indication that such acts may be imminent. (This list should not be considered all inclusive.)

- 1) Attempted or confirmed intrusions into vital islands, material access areas, protected area or controlled access areas.
- 2) Discovery of an attempted introduction of unauthorized weapons, explosives or incendiary devices into the protected area, vital islands, controlled access areas or material access areas
- 3) Bomb threats or extortion threats. Bomb threats should always be reported within one hour, however, if contingency plan provisions are

implemented and no bomb is discovered, then the licensee need only make the required log entry.

- 4) Mass demonstrations, picketing, or other job actions at the plant site.
- 5) Civil disturbances near the plant site.
- 6) Discovery of a criminal conspiracy involving licensee personnel or contractors, e.g., discovery of a drug-related events involving security personnel.
- 7) Discovery of falsified or unaccounted for identification badges, key cards, or locks and keys.
- 8) Theft of documents containing safeguards information.
(Classified information reportable under 95.57.)
- 9) Unexplained fire or explosion within the isolation zone, protected area, or controlled access area, vital island or material access area.

Examples of Threat-Related Events That Need To Be Logged

The following examples are incidents that do not need to be reported telephonically to the NRC: (This list should not be considered inclusive.)

- 1) Incidental, non hostile intrusion at vital island, material access areas, protected areas or controlled access areas. For example, a maintenance man cuts a hole through a vital island barrier for the purpose of installing pipes. If the licensee determines that there was no hostile intent, then the incident need not be reported. However, the licensee should provide compensatory measures in accordance with the physical protection plan or contingency plan.

- 2) Small controlled, peaceful demonstrations outside of protected area perimeters.
- 3) Attempted intrusions at protected area barriers by obviously non-hostile individuals, e.g., a child climbing the fence.
- 4) Theft of a security weapon at the site. (As an isolated incident.)

Safeguards Systems Failures

Paragraph 73.71(b) requires that the licensee report certain safeguards events to the NRC Operations Center within one hour of discovery. As addressed in Appendix E, included would be certain safeguards systems failures such that unauthorized access could be allowed to material access areas, or to vital islands, protected areas, or to irradiated nuclear fuel at fixed sites and in transit, or SSNM at fixed sites authorized to possess formula quantities of SSNM, or SSNM in transit, when such shipments involve formula quantities of SSNM. Safeguards systems failures include improper procedures which could result in any one of the above conditions.

Examples of Safeguards Systems Failures to Be Reported Within One Hour

- 1) Loss of both central and secondary alarm station ability to readout alarms.
- 2) Unavailability of minimum number of security personnel or an actual or imminent strike by the security force.
- 3) Failure of protected area safeguards system simultaneous with the loss of one aspect of the VA or MAA safeguards system such as one alarm station malfunction.

- 4) Loss of electrical power supply to security systems.

Other Safeguards Events

Any safeguards event or situation, which is not reportable under paragraphs a, b, c, d, or e of Appendix E to Part 73, but for which a news release or notification of other government agencies is planned, should be reported to the NRC Operations Center within one hour prior to such notification.

II. Safeguards Events Under §73.71(c)

The only events reportable under §73.71(c) are safeguards systems failures. All safeguards systems failures described in paragraph (d) of Appendix E of Part 73 which have been properly compensated for, need only be logged. Properly compensated for means that compensatory measures have been established in accordance with the licensee's physical protection plan or contingency plan.

Safeguards systems failures that would not be directly exploited to gain access, but do reduce the operational effectiveness of the safeguards system should be recorded in the licensee log. Improper personnel procedures which result in safeguards systems failures should be recorded in the log.

Examples of Events That Should be Recorded In the Licensee's Log

- 1) Security computer failures that do not result in major safeguards systems failures as described in Appendix E (d).
- 2) Card reader failures alone

- 3) Single alarm station failure alone
- 4) CCTV camera failure in a single zone alone
- 5) Failure of perimeter lighting alone
- 6) Loss of intrusion detection system alone

Reporting Requirements Chart

One Hour Telephonic Report
 Thirty Day Written Follow-Up Report

Recorded in Licensee's Log
 Submitted Quarterly to the NRC

All events described in
 Appendix E to Part 73 which
 would include:

Events described in §73.71(c).

- | | |
|---|--|
| <ol style="list-style-type: none"> 1) Acts, attempts or threats of destruction. 2) Acts, attempts or threats that could or do interrupt normal operations. 3) Acts, attempts or threats of theft. 4) Safeguards systems failures that could allow access to material access areas, vital islands, protected areas, or to irradiated nuclear fuel at fixed sites and in transit or SSNM at fixed sites, authorized to possess formula quantities of SSNM, or SSNM in transit, when such shipments involve formula quantities of SSNM, provided that compensatory measures are not established. 5) Loss of offsite communications ability. 6) Safeguards events for which a news release or notification of other government agencies is planned. | <ol style="list-style-type: none"> 1) Safeguards systems failures described in Appendix E (d) for which prompt compensatory measures have been established in accordance with the licensee's physical protection plan or contingency plan. 2) Safeguards systems failures that decrease the operational effectiveness of the system. |
|---|--|

Guidelines for Written Reports and Log Entries

The licensee should include the information listed below (if applicable and known) in their written reports to the NRC and in their §73.71(c) event log. The occurrence of repeated similar events can be consolidated in a single log entry within 24 hours as long as all information required in the "Guidelines for Written Reports and Log Entries" is included. For example, if a security computer fails three times within 24 hours, for the same reasons only one log entry is needed. Written reports can also be handled in this manner.

I. For all events the licensee should:

- 1) Identify the facility where the event took place.
- 2) Provide a clear narrative description of the occurrence including the following information:
 - (a) Date and approximate time of the event (military time local to the event)
 - (b) Event duration
 - (c) Plant operating conditions before the event
 - (d) The specific area in which the event took place or was threatened, e.g. controlled access area, vital island, or protected area.
 - (e) Safety systems failures -- any vital equipment or systems important to safety that were threatened either directly or indirectly.
 - (f) Actions taken in response to event.
 - (g) Type and number of personnel involved, e.g., contractors, security personnel, operators, etc.

- (h) Method of discovery of incident, e.g., through routine inspection, test, maintenance, alarm, unusual circumstance, chance, informant, or communicated threat
- (i) A description of any corrective actions taken or planned as a result
- (j) The name and telephone number of a contact with the licensee's organization who is knowledgeable about the event and could provide additional information.

II. For Security Systems Failures

- 1) The description provided in Part I above should also include the following information:
 - a) The cause of each component or system failure, e.g., mechanical problems or personnel error.
 - b) The manufacturer, model numbers and a brief description of the failed or malfunctioned component.
 - c) The effect of the failure, including any impact or threat to plant safety.
 - d) For failures of components with multiple functions a list of secondary functions that were affected. Include any safety components or systems that may have been affected.
 - e) Any unusual characteristics of the work location that may have been contributed to the failure, e.g, heat.

III. Threat-Related Incidents

- 1) The description provided in Part I should also include the following information:
 - a) Type of threat
 - b) Means of conveyance, e.g., letter, telephonically
 - c) Text of threat
 - d) Number of perpetrator(s), including any background information excluding that information requiring protection under the Privacy Act.
 - e) Mode of operation of perpetrator(s).

YELLOW TICKET 83-236

DISTRIBUTION: *w/incoming

Document Control*

NRC PDR*

L PDR*

PRC*

SSPB Reading*

C. Thomas

E. McPeck

P. Anderson*

D. Eisenhower/R. Purple

F. Miraglia/Lee

M. Jambor

Attorney, OELD

M. Garver (83-236)

M. Bridgers, EDO (83-236)

E. L. Jordan, IE

J. M. Taylor, IE

SECY (3)

H. Denton/E. Case

PPAS

R. Vollmer

R. Mattson

H. Thompson

T. Speis

B. Snyder

N. Grace