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

January 2011
Division 5

DRAFT REGULATORY GUIDE

Contact: P. Brochman
(301) 415-6557

DRAFT REGULATORY GUIDE DG-5019, Revision 1

(Proposed Revision 2 of Regulatory Guide 5.62, dated November 1987)

REPORTING AND RECORDING SAFEGUARDS EVENTS

A. INTRODUCTION

This draft regulatory guide (DG) describes methods that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for licensees and certificate holders to report and record safeguards (i.e., security) events. This guide applies to a range of facilities and activities licensed or certified by the NRC. These facilities and activities include reactor facilities; special nuclear material (SNM) production, use, and storage facilities; spent nuclear fuel (SNF) and high-level radioactive waste (HLW) storage and disposal facilities; and the transportation of SNM, SNF, and HLW to or from such facilities.

Title 10 of the *Code of Federal Regulations* (10 CFR) 73.71, "Reporting and Recording of Safeguards Events," requires licensees and certificate holders to report certain safeguards events to the NRC Headquarters Operations Center and to record certain security events in a safeguards event log. Appendix G, "Reportable and Recordable Safeguards Events," to 10 CFR Part 73, "Protection of Plants and Materials," (Ref. 1) provides additional detail on the specific security events to be reported or recorded. In support of 10 CFR 73.71, Appendix A to 10 CFR Part 73, "U.S. Nuclear Regulatory Commission Offices and Classified Mailing Addresses," contains contact information for the NRC Headquarters Operations Center and directions on communicating classified security events to the NRC.

This guide provides examples of security events that represent actual or potential threats, suspicious activities, challenges to security systems or processes, or internal tampering with equipment that threatens or affects the safe operation or the security of facilities and transportation activities. This guide also provides examples of security events that adversely impact the effectiveness of security systems, components, and procedures required by the NRC's security regulations under 10 CFR Part 73 or the licensee's or certificate holder's NRC-approved security plans. Finally, this guide provides examples of events that are indicative of imminent or actual hostile actions against reactor facilities, Category I strategic special nuclear material (SSNM) facilities, and the transportation of SSNM, SNF, and

HLW. This guide also describes required reports to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) and local law enforcement agencies (LLEAs) regarding lost or stolen enhanced weapons.

Licensees and certificate holders should consider obtaining access to the NRC's protected Web server (PWS) to obtain routine threat bulletins and analyses the NRC receives from the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) on critical national infrastructure and key resources. Licensees and certificate holders desiring access to the NRC's PWS should make their request through the security staff in their applicable NRC regional office.

This guide provides acceptable methods and examples for use by licensees and certificate holders to determine whether to report or record security events. The NRC staff does not consider the examples provided in this guide to be all inclusive. If a licensee or certificate holder has questions regarding the reporting or recording of a specific security event, they may, if time permits, discuss this matter with the NRC security staff in their applicable regional office or the staff from the Office of Nuclear Security and Incident Response in NRC Headquarters. Otherwise, the licensee or certificate holder should report the event and then discuss it with appropriate NRC staff. Licensees and certificate holders may subsequently withdraw a report of an invalid security event, without prejudice.

A licensee or certificate holder should not consider security events reported under this guide as indicative of performance failures. Rather, the NRC considers timely and comprehensive communication of matters relating to threats, attacks, or suspicious activities a vital component of its efforts to assess the current threat environment. Since our Nation's enemies have demonstrated the ability to attack multiple independent targets, timely reporting of non-threatening but suspicious activities is important to the NRC, law enforcement agencies, and the intelligence community in order to integrate potential adversary plans, intentions, and suspicious event reports into the ongoing assessment of the "current threat environment." The prompt reporting of actual or imminent hostile actions permits the NRC to execute its strategic missions of communicating hostile action against the facilities and activities it regulates to senior Federal officials and to other licensees and certificate holders; thereby protecting public health and safety, the common defense and security, and the environment.

The NRC's previous guidance on reporting and recording security events remains in effect until this revision to RG 5.62 is issued. Additionally, subsequent to the issuance of this revision to RG 5.62 the NRC plans to conduct a workshop on these revised security event reporting and recording requirements with the goal of producing Revision 1 to NUREG-1304, "Reporting of Safeguards Events." NUREG-1304 is based upon a workshop on reporting and recording safeguards events that was held in 1988 following the issuance of RG 5.62, Rev. 1. NUREG-1304 is structured in a question and answer format.

This draft regulatory guide is being issued for comment in support of the NRC's proposed revisions to the safeguards event reporting and recording requirements in 10 CFR 73.71 and Appendix G to 10 CFR Part 73 (Appendix G). However, this RG does not apply to licensees and certificate holders reporting fitness-for-duty events to the NRC.

The NRC issues regulatory guides to describe to the public the methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses 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.

This regulatory guide contains information collection requirements covered by 10 CFR Part 73 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002.

The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number. The NRC has determined that this Regulatory Guide is not a major rule as designated by the Congressional Review Act and has verified this determination with the OMB.

B. DISCUSSION

The reports and records made by licensees and certificate holders under 10 CFR 73.71 and Appendix G are intended to inform the NRC, and potentially other Federal intelligence and law enforcement agencies, of security-related events that could (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries. The required information also contributes to the NRC's analysis of the reliability and effectiveness of licensees' and certificate holders' security programs and systems.

The regulations in 10 CFR 73.71 and Appendix G require licensees and certificate holders to report certain security events to the NRC Headquarters Operations Center. These regulations require licensees and certificate holders to notify the NRC by telephone of the discovery of these security events. Additionally, the regulations in 10 CFR 73.71 and Appendix G require licensees and certificate holders to record certain other security events in a safeguards event log. NRC security inspectors periodically review and analyze the events listed in the safeguards event log as part of the NRC's routine security inspection, oversight, and enforcement programs. The regulations also require licensees and certificate holders to submit written followup reports to the NRC subsequent to certain verbal reports made under 10 CFR 73.71. The type of information to be reported to the NRC is generally focused on event descriptions, threat-related information, and security systems' performance, reliability, and effectiveness. This guide follows the structure of the proposed revision to 10 CFR 73.71 and Appendix G. Appendix G supports the regulations contained in 10 CFR 73.71 and provides a more detailed description of the types of events and information to be reported or recorded.

The timing of these reports can range from within 15 minutes of discovery to within 24 hours of discovery, depending on the significance and impact of the event being reported or recorded. Significant security events may warrant immediate NRC actions. For example, 10 CFR 73.71 requires licensees and certificate holders to report actual or imminent hostile actions within 15 minutes of discovery. Upon notification of such a hostile action, the NRC will rapidly communicate this information to other NRC licensees and certificate holders and to other Federal agencies to enable them to immediately increase the response level of their security defenses.

Other less serious, but still significant, events require reports within 1 hour of discovery. Events involving suspicious activities and potential tampering or unauthorized operation of components require reports within 4 hours and 8 hours of discovery, respectively. For certain events, the NRC may, upon its discretion, request the licensee or certificate holder to establish a continuous communications channel with the NRC Headquarters Operations Center (to facilitate the communication of information during an ongoing event).

With the addition of provisions to 10 CFR Part 73 permitting certain licensees and certificate holders to possess enhanced weapons (see glossary), the regulations require 1-hour or 4-hour notifications for reporting the discovery of stolen or lost enhanced weapons. The NRC requires licensees or certificate holders to report within 24 hours of the receipt of an adverse inspection or enforcement finding or other adverse notice from ATF regarding the licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons.

This revised guide explains the types of information that licensees and certificate holders should report to satisfy the requirements of the proposed rule and gives several examples to illustrate some of the events that may occur and should be reported. The NRC staff developed the examples, which illustrate the types of actual occurrences that should be reported. This draft guide contains many examples to help licensees, certificate holders, and NRC staff sort security-related events into the proper reporting categories. If these examples are interpreted as the only events to be reported, they may seem to be

contradictory or confusing. For virtually every example provided, the addition or subtraction of a single aspect not explicitly detailed in the example could easily move it into a higher or lower timeliness category. Accordingly, the use of these examples should be tempered with the texts of 10 CFR 73.71, Appendix G, and other guidance contained in this guide. When determining the reportability of a particular event, a licensee, certificate holder, or the NRC staff should review the basic rule language and the guidance and the specific examples contained in this guide.

The NRC intends that licensees and certificate holders only report and record information required by the agency's regulations. To assist licensee and certificate holders, this guide also provides information and examples of occurrences that the NRC staff does not consider recordable. As with other portions of this guide, the NRC staff considers the information that is contained in Regulatory Position 6, "Security Events that Are Not Considered Recordable," as being neither limiting nor constraining, and the licensee or certificate holder is ultimately responsible for ensuring compliance with the regulatory requirements.

C. REGULATORY POSITION

The NRC requires licensees and certificate holders to provide timely reports of security events. As soon as a security event is recognized, it becomes reportable within the timeframe specified. The time to report the event is based on the licensee's or certificate holder's "time of discovery," as opposed to the time a licensee or certificate holder concludes that a reportable event has occurred. A licensee's or certificate holder's initial analysis of an event could take several days to reach a conclusion on the reportability of a specific event. Therefore, the time period for reporting an event starts at the time of discovery. However, licensees and certificate holders may contact the NRC and withdraw an invalid report (based upon a subsequent analysis of the circumstances of an event). A licensee or certificate holder may make withdrawals without prejudice to its security performance indicators. Confusion, misinterpretation, erroneous determinations, and a reluctance to report security events in the past have caused difficulties for the NRC staff and a lack of consistency among licensees and certificate holders.

The NRC staff has developed this guide based on examples of previous events and interactions between NRC staff and licensee or certificate holders. This guide is intended to provide assistance to licensees and certificate holders in evaluating a broad range of potential security events on whether these events should be reported or recorded under the provisions of 10 CFR 73.71 and Appendix G. The NRC staff considers the specific events listed in this guide as examples of reportable or recordable security events. As such, the NRC staff does not consider these lists as exhaustive or exclusive. Many of the examples listed herein have been created from actual events at NRC-regulated facilities or from licensee and certificate holder discussions with NRC staff on whether a particular event was reportable, recordable, or neither.

The NRC staff encourages licensees and certificate holders to report security notifications and subsequently retract them, if appropriate (e.g., as invalid events) rather than delaying the initial report to gather more information and thus have greater confidence in whether or not to make a report. If a licensee or certificate has questions about whether to report or record an event, the licensee or certificate holder can, if time permits, discuss the event with their appropriate NRC regional or Headquarters security staff before making a report or record. However, if the questions cannot be resolved, licensees or certificate holders should report all security events to the NRC within the timeliness requirements of 10 CFR 73.71. However, if the licensee or certificate holder subsequently determines that the event did not require a report (e.g., the event was invalid), the licensee or certificate holder may retract the report in accordance with the provisions of 10 CFR 73.71(j)(8) and 10 CFR 73.71(m)(13).

In addition to examples of events regarding failures and challenges to the licensee's or certificate holder's security programs and systems, the requirements in 10 CFR 73.18 and Appendix G direct licensees and certificate holders to also report suspicious events to the NRC. The NRC staff use the information developed from reports of suspicious activity in assessing the current threat environment. In addition, the NRC forwards appropriate reports of suspicious activities to federal law enforcement agencies and the intelligence community as part of the National threat assessment process. Accordingly, the NRC staff has added examples of suspicious events that should be reported to the NRC. The U.S. government considers suspicious activity as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Licensees and certificate holders are considered "key resource owners and operators" and can find additional guidance on examples of suspicious events in the U.S. Department of Homeland Security's, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," (Ref. 8).

Although, the NRC staff views the overall goal of reducing unnecessary security event notifications as worthwhile, the NRC staff continues to believe that the time period for making notifications should begin at the licensee's or certificate holder's time of discovery of an issue, as opposed to the time when it concludes (following review and evaluation) that a reportable event has occurred. For example, a similar security event may have occurred at other facilities and may be related or indicate a broader trend. The timely integration of multiple intelligence or threat threads into the current threat assessment requires timely notification from licensees to develop this integrated assessment. For example, the NRC is concerned that a potentially innocuous event at a single site (that could indicate attempted reconnaissance or surveillance) is quite different from similar events occurring at multiple sites or across multiple sectors of the country. Because suspicious events (e.g., attempted reconnaissance or challenges to security systems) may be indicative of preoperational malevolent activities and our nation's enemies have demonstrated a capability to simultaneously attack multiple independent targets, the NRC has established requirements for reporting suspicious events. Analysis of individual events (at separate facilities or activities) may reveal to the NRC, law enforcement authorities, or the intelligence community potential threats or patterns that warrants increasing the security posture for NRC-regulated facilities and activities, other government facilities and activities, and other national critical-infrastructure facilities.

1. Applicability

This regulatory position provides information to licensees and certificate holders on the classes of NRC-regulated facilities and activities that are subject to specific reporting and recording provisions of 10 CFR 73.71 and Appendix G.

a. The regulations in 10 CFR 73.71(a) regarding 15-minute notifications for facilities apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20, "General Performance Objective and Requirements"; 10 CFR 73.45, "Performance Capabilities for Fixed Site Physical Protection Systems"; 10 CFR 73.46, "Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures"; and 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM and power reactor and production reactor facilities.

b. The regulations in 10 CFR 73.71(b) regarding 15-minute notifications for shipments apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20; 10 CFR 73.25, "Performance Capabilities for Physical Protection of Strategic Special Nuclear Material in Transit"; 10 CFR 73.26, "Transportation Physical Protection Systems, Subsystems, Components, and Procedures"; and 10 CFR 73.37, "Requirements for Physical Protection of Irradiated Reactor

Fuel in Transit." This includes the transportation of Category I quantities of SSNM, SNF, and HLW.

c. The regulations in 10 CFR 73.71(c) regarding 1-hour notifications for facilities apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20; 10 CFR 73.45; 10 CFR 73.46; 10 CFR 73.50, "Requirements for Physical Protection of Licensed Activities"; 10 CFR 73.51, "Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-Level Radioactive Waste"; 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"; 10 CFR 73.55; 10 CFR 73.60, "Additional Requirements for Physical Protection at Nonpower Reactors"; or 10 CFR 73.67, "Licensee Fixed Site and In-Transit Requirements for the Physical Protection of Special Nuclear Material of Moderate and Low Strategic Significance." This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, independent spent fuel storage installations (ISFSIs), monitored retrievable storage installations (MRSs), geologic repository operations areas (GROAs), power reactor facilities, production reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM.

d. The regulations in 10 CFR 73.71(d) regarding 1-hour notifications for shipments apply to licensees and certificate holders subject to the provisions of 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, and 10 CFR 73.67. This includes the transportation of SNF, HLW, or Category II and Category III quantities of SNM.

e. The regulations in 10 CFR 73.71(e) regarding 4-hour notifications for facilities apply to licensees and certificate holders subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, production reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM.

f. The regulations in 10 CFR 73.71(f) regarding 8-hour notifications for facilities apply to licensee and certificate holders subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, production reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM.

g. The regulations in 10 CFR 73.71(g) regarding 1-hour or 4-hour notifications for stolen or lost enhanced weapons apply to licensee and certificate holders that fall within the classes of facilities, radioactive material, and other property specified in 10 CFR 73.18(c), "Authorization for Use of Enhanced Weapons and Preemption of Firearms Laws"; and the licensee or certificate holder possesses enhanced weapons under 10 CFR 73.18.

h. The regulations in 10 CFR 73.71(h) regarding 24-hour notifications for the receipt of an adverse ATF inspection or enforcement finding or other adverse notices (regarding a licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons) apply to licensees and certificate holders possessing enhanced weapons under 10 CFR 73.18.

i. The regulations in 10 CFR 73.71(j) regarding the process for making telephonic notifications of reportable security events under 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), and (h) apply to the licensees and certificate holders listed under Regulatory Positions 1.a through 1.h above. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM. This includes the transportation of Category I quantities of SSNM, SNF, HLW, and Category II and III quantities of SNM. This also applies to notifications of stolen or lost enhanced weapons or inspection or enforcement findings or other adverse notices from ATF.

j. The regulations in 10 CFR 73.71(k) regarding the recording of security events in a safeguards event log apply to each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.37, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, and 10 CFR 73.67. This includes fuel cycle facilities authorized to possess and use Category I quantities of SSNM, hot cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research and test reactor facilities, and fuel cycle facilities authorized to possess and use Category II and Category III quantities of SNM. This also includes the transportation of Category I quantities of SSNM, SNF, HLW, and Category II and III quantities of SNM.

k. The regulations in 10 CFR 73.71(m) regarding the submission of written followup reports of security events under 10 CFR 73.71(a), (b), (c), (d), (e), (f), and (g) apply to the licensees and certificate holders described in Regulatory Positions 1.a through 1.g above.

l. The regulations in 10 CFR 73.71(n) regarding security events that also warrant an Emergency Classification apply to the reactor, fuel cycle, ISFSI, MRS, GROA, and gaseous diffusion facilities licensed or certified by the NRC.

m. The regulations in paragraphs I, II, and III of Appendix G apply to licensees and certificate holders subject to the provisions of 10 CFR 73.71(c), (e), and (j) (see Regulatory Positions 1.a, 1.c, and 1.j above).

n. The regulations in paragraphs I and III of Appendix G apply to licensees and certificate holders subject to the provisions of 10 CFR 73.71(c), (d), and (j) (see Regulatory Positions 1.c, 1.d, and 1.j above).

o. The regulations in paragraph IV of Appendix G apply to licensees and certificate holders subject to the provisions of 10 CFR 73.71(k) (see Regulatory Positions 1.a through 1.g above).

2. Telephonic Reportable Security Events

The regulations in 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), and (h) require licensees and certificate holders to make a telephonic notification to the NRC of certain security events. Events requiring telephonic notifications are considered significant and require clear, person-to-person communication. Regulatory Position 4 below contains guidance regarding the information to be provided during telephonic notifications. The NRC staff is using the phrase "telephonic notification" to refer to verbal reports made using a telephone (e.g., using a land line, cellular, satellite, voice over IP capability, etc.), rather than e-mails, faxes, or text messages. The NRC views that human-to-human communication is necessary for these types of event reports to provide for follow-up questions and clarifications, requests for information or action, and to facilitate NRC response activities. For some events, the NRC Headquarters Operations Center may request the licensee or certificate holder establish a continuous

communications channel with the NRC. Regulatory Position 3.7 below provides guidance to the licensee or certificate holder on establishing a continuous communications channel, if requested by the NRC.

The purpose of a telephonic notification is to ensure timely, direct, and accurate communication of information to the NRC related to security matters that may require action by the licensee, certificate holder, the NRC, the intelligence community, or another government agency. These actions may involve a change in the NRC Headquarters Operations Center's and Regional Incident Response Center's response mode or a change in the need to respond to public or media inquiries about an event. Other methods of communication, such as e-mail or text messaging, should not be used unless extreme conditions prohibit telephonic reporting. This guide contains examples of reports to assist licensees and certificate holders and the NRC staff in evaluating the reportability of security events and information received from licensees and certificate holders. The NRC considers these examples to be neither limiting nor all-inclusive.

Telephonic notifications should be focused on occurring events, not their resolution, final analysis, suspected motivation of any participants, or technical evaluations. While those necessary actions should be considered part of the response function and should eventually be reported, they should not affect the timely telephonic communication of the event.

Depending on the type of licensee or certificate holder, and the type of information required to be reported, the timeliness of telephonic reports differ, as described below. Timeliness in telephonic reporting is important to ensure effective communication among potential responders, the intelligence and law enforcement communities, and other government agencies. The accuracy of information provided in telephonic reports is likewise important to ensure that decisions relating to potential response and threat analysis are appropriate. Licensees and certificate holders should provide the most complete and accurate information available to them when they make telephonic reports. Licensees and certificate holders should make additional calls describing substantive changes, additions, or modifications to the initial information in a timely manner after taking immediate actions to protect the facility or stabilize its operations, in accordance with their emergency operations and contingency response procedures.

In addition to notifications made to the NRC Headquarters Operations Center for security events under 10 CFR 73.71 and Appendix G, this guide describes notifications that should be made to LLEAs within 48 hours of discovery to report the theft or loss of an enhanced weapon under 10 CFR 73.18.

The NRC recognizes that some events that require telephonic security reports may also require the licensee or certificate holder to declare an emergency under the applicable provisions of 10 CFR 50.72, "Immediate Notification Requirements for Operating Power Reactors" (Ref. 2); 10 CFR 70.50, "Reporting Requirements" (Ref. 3); 10 CFR 72.75, "Reporting Requirements for Specific Events and Conditions" (Ref. 4); or 10 CFR 76.120, "Reporting Requirements" (Ref. 5). Licensees and certificate holders should be aware that, while dual reporting (making two separate phone calls to report the same information) is not required under 10 CFR 73.71, a reportable security event may have more restrictive timeliness requirements than an emergency declaration (e.g., the imminent attack notification requirements of 10 CFR 73.71(a) and (b)). Furthermore, telephonic reports should not interfere with the licensee's or certificate holder's actual response to an emergency or security event or to requesting offsite assistance from an LLEA; however, licensees and certificate holders should consider telephonic notifications a high priority task, to ensure that the NRC and other government agencies respond appropriately to events with potentially broader implications than a single facility. Regulatory Position 4.7 below contains specific guidance regarding dual reporting of security events.

Because of the importance of timely telephonic notifications, licensees and certificate holders making security event notifications that contain Safeguards Information may make such notifications to

the NRC Headquarters Operations Center without using a secure communications system under the exception of 10 CFR 73.22(f)(3) for emergency or extraordinary conditions. However, licensees or certificate holders should try to protect sensitive information whenever possible. If a license or certificate holder has provided Safeguards Information to the NRC Headquarters Operations Center over a nonsecure communications system, it should include this fact as part of the information conveyed to the NRC. Licensees and certificate holders should develop procedures to assist operations, security, and emergency response managers and other key personnel in evaluating events for their reportability, providing the necessary information to the NRC, and ensuring that the need for appropriate information security is balanced with the timeliness of providing information to the NRC.

For reports containing classified national security information or restricted data, licensees and certificate holders should make such telephonic notifications by using a secure communications system. Alternate provisions are discussed in Regulatory Position 4 below.

In addition to providing information on the physical security and information security events that are required to be reported and recorded under 10 CFR 73.71 and Appendix G, this guide includes information on reporting and recording cyber security events. However, cyber security event notifications only apply to licensees and certificate holders that are subject to the requirements of 10 CFR 73.54. This regulation requires power reactor licensees to establish and maintain a cyber security program at their facilities to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat, as described in 10 CFR 73.1, "Purpose and Scope" (Ref. 1).

2.1 Facility Security Events To Be Reported within 15 Minutes

The regulations in 10 CFR 73.71(a) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, or 10 CFR 73.55 to notify the NRC Headquarters Operations Center as soon as possible but not later than 15 minutes after the discovery of an imminent or actual hostile action against a Category I SSNM facility or a power reactor facility. This rapid notification is intended to provide the NRC with an abbreviated set of facts that can be immediately disseminated to other licensees, certificate holders, and government agencies, to enable them to rapidly increase their security posture.

The fundamental purpose of a 15-minute report is to allow the NRC to (1) warn other licensees and certificate holders of this ongoing event (to immediately increase their defensive posture) and (2) notify other Federal agencies. Accordingly, the NRC has reduced the amount of information licensees and certificate holders should provide in the report. Furthermore, the NRC may require the licensee or certificate holder to establish a continuous communications channel as soon as possible after making the 15-minute report (see Regulatory Position 3.7 below). This flexibility is intended to relieve licensees and certificate holders of a communications burden while they immediately respond to the event, direct personnel, request LLEA assistance, and staff the communicator position (for a continuous communications channel) with an appropriately trained individual.

A licensee's or certificate holder's request for immediate LLEA assistance should take precedence over the notification to the NRC. Protecting public health and safety and the common defense and security should always be the licensee's and certificate holder's first priority. Furthermore, this regulatory guide does not apply to aircraft threats and attacks. Guidance on licensee response to aircraft threats and attacks is found in Regulatory Guide 1.214, "Response Strategies for Potential Aircraft Threats" (Ref. 6).

These reports involve both the licensee's or certificate holder's discovery of an imminent or actual hostile action and the initiation of a security response in accordance with the safeguards contingency plan or protective strategy that is based upon an actual or imminent hostile action. Although the licensee's and certificate holder's plans and procedures typically describe many levels of security response, for the purposes of this reporting requirement, the security response means the substantive implementation (or deployment) of the facility's armed response capabilities to defensive positions or locking down normal access to the facility or within the facility (i.e., a security contingency event response). The regulations do not require licensees and certificate holders to report security responses that are initiated as a result of a threat or warning information communicated to them by the NRC.

Reports made under this provision apply only to ongoing security events, either actual or imminent. In the first circumstance, a licensee or certificate holder has been subject to a hostile action. A hostile action upon an applicable licensed facility or its personnel has either been committed or is in progress and includes the use of violent force to destroy equipment, take hostages, or intimidate the licensee or certificate holder. Hostile actions include attacks by air, land, or water, using weapons, explosives, projectiles, vehicles, or other devices to deliver destructive force. In the second circumstance, an imminent hostile action is one for which the licensee or certificate holder has received information on the potential action and it fits the characteristics (of a hostile action) described in this paragraph.

2.1.1 Notification Requirements

10 CFR 73.71(a) 15-minute notifications – facilities. Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.45, 73.46, or 73.55 shall notify the NRC Headquarters Operations Center, as soon as possible but not later than 15 minutes after —

(1) The discovery of an imminent or actual hostile action against a nuclear power or production reactor or Category I SSNM facility; or

(2) The initiation of a security response in accordance with a licensee's or certificate holder's safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against a nuclear power reactor or Category I SSNM facility;

(3) These notifications shall:

(i) Identify the facility name;

(ii) Include the authentication code; and

(iii) Briefly describe the nature of the hostile action or event, including:

(A) Type of hostile action or event (e.g., armed assault, vehicle bomb, credible bomb threat, etc.); and

(B) Current status (i.e., imminent, in progress, or neutralized).

(4) Notifications must be made according to paragraph (j) of this section, as applicable.

(5) The licensee or certificate holder is not required to report security responses initiated as a result of threat or warning information communicated to the licensee or certificate holder by the NRC.

(6) A licensee's or certificate holder's request for immediate local law enforcement agency (LLEA) assistance can take precedence over the notification to the NRC.

2.1.2 Examples of Reportable Events

The NRC staff considers that the following facility-security events are examples of the types of events that require notification under 10 CFR 73.71(a):

a. the licensee's or certificate holder's discovery of an imminent or actual hostile act against its nuclear power reactor or Category I SSNM facility

b. the detonation of explosives or an explosive device at or in close proximity (within site boundaries) to the licensee's or certificate holder's facility, including the use of explosives by ground assault force personnel and the use of land-based or waterborne vehicle bombs

c. unauthorized weapons being fired within any controlled area of licensee's or certificate holder's facility

d. weapons being fired at the licensee's or certificate holder's facility and projectiles hitting the facility that causes an immediate threat to the facility or to security personnel

e. the successful, forcible penetration of a protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA) by unauthorized personnel or vehicles

f. the taking of hostages onsite

g. the taking of hostages offsite that is reasonably determined to be related to facility operations or security functions (e.g., the kidnapping of family members in order to coerce facility employees into violating laws, NRC regulations, or the facility's license or certificate of compliance)

h. actual or believed theft of SSNM or SNF

i. the licensee's or certificate holder's notification from law enforcement authorities or another reliable source that an explosion or other assault on the facility is imminent

j. the licensee's or certificate holder's initiation of a security response in accordance with its safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against its nuclear power reactor or Category I SSNM facility

k. a vehicle demonstrating an actual or attempted violent breach or disablement of the vehicle barrier system (VBS) by overtly attempting to circumvent the barrier or by striking it violently, at a high rate of speed

The term "VBS" referred to in this regulatory position is the licensee's or certificate holder's engineered vehicle barrier system that is intended to stop vehicle-borne improvised explosive device (VBIED) attacks. The VBS is typically located at or beyond the exterior of the licensee's or certificate holder's protected area barrier. The VBS can consist of engineered security features or natural landform obstacles. The VBS uses these features to prevent vehicle progress and thus achieve a greater standoff distance between critical structures and personnel and the blast, shock, shrapnel, and impulse effects from the detonation of a VBIED. The NRC staff does not intend such reports under this regulatory position to include outer vehicle checkpoints located in the owner controlled area that are not part of the licensee's or certificate holder's VBS.

Licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 and Appendix G.

2.2 Transportation Security Events To Be Reported within 15 Minutes

The regulations in 10 CFR 73.71(b) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, or 10 CFR 73.37 to notify the NRC Headquarters Operations Center as soon as possible but not later than 15 minutes after the discovery of an imminent or actual hostile action against shipments of Category I SSNM, SNF, and HLW. This rapid notification is intended to provide the NRC with an abbreviated set of facts that can be immediately

disseminated to other licensees, certificate holders, and government agencies, to enable them to rapidly increase their security posture.

These reports involve both the licensee's or certificate holder's discovery of an imminent or actual hostile action and the initiation of a security response in accordance with its safeguards contingency plan or protective strategy that is based upon an actual or imminent hostile action. Although the licensee's and certificate holder's plans and procedures typically describe many levels of security response, for the purposes of this reporting requirement, the security response means the substantive implementation (deployment) of armed response capabilities (i.e., a security contingency event response). The regulations do not require licensees and certificate holders to report security responses that are initiated as a result of a threat or warning information communicated to them by the NRC.

A licensee's or certificate holder's request for immediate LLEA assistance should take precedence over the notification to the NRC. Protecting public health and safety and the common defense and security should always be the licensee's and certificate holder's first priority.

Reports made under this provision are applicable only to ongoing security events, either actual or imminent. In the first circumstance, a licensee or certificate holder has been subject to a hostile action. A hostile action upon an applicable shipment or its accompanying personnel has either been committed or is in progress and includes use of violent force to steal the SSNM; destroy the transport vehicle or the SSNM, SNF, or HLW; take hostages; or intimidate the licensee or certificate holder. Hostile actions include attacks by air, land, or water, using weapons, explosives, projectiles, vehicles, or other devices to deliver destructive force. In the second circumstance, an imminent hostile action is one for which the licensee or certificate holder has received information on the potential action and it fits the characteristics (of a hostile action) described in this paragraph.

The purpose of this notification is to allow the NRC to (1) warn other licensees and certificate holders and (2) notify other Federal agencies. Accordingly, the NRC has reduced the amount of information it should provide in the notification. Furthermore, the NRC may require the licensee or certificate holder to establish a continuous communications channel as soon as possible after making the 15-minute notification (see Regulatory Position 3.7 below). This flexibility is intended to relieve licensees and certificate holders of a communications burden while they immediately respond to the event, direct personnel, request LLEA assistance, and staff a trained individual in the communicator position (for the continuous communications channel).

The regulations permit licensees and certificate holders to directly report transportation events to the NRC themselves, or to use a contract service communications center to monitor and communicate with the shipment, contact LLEA if required, and report events to the NRC.

2.2.1 Notification Requirements

10 CFR 73.71(b) 15-minute notifications – shipments. Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.25, 73.26, or 73.37 shall notify the NRC Headquarters Operations Center or make provisions to notify the NRC Headquarters Operations Center, as soon as possible but not later than 15 minutes after —

(1) The discovery of an actual or attempted act of sabotage against shipments of spent nuclear fuel or high-level radioactive waste;

(2) The discovery of an actual or attempted act of sabotage or of theft against shipments of strategic special nuclear material; or

(3) The initiation of a security response in accordance with a licensee's or certificate holder's safeguards contingency plan or protective strategy, based on an imminent or actual

hostile action against a shipment of spent nuclear fuel, high-level radioactive waste, or strategic special nuclear material.

(4) These notifications shall:

(i) Identify the name of the facility making the shipment, the material being shipped, and the last known location of the shipment; and

(ii) Briefly describe the nature of the threat or event, including:

(A) Type of threat or event (e.g., armed assault, vehicle bomb, theft of shipment, etc.); and

(B) Threat or event status (i.e., imminent, in progress, or neutralized).

(5) Notifications must be made according to paragraph (j) of this section, as applicable.

(6) The licensee or certificate holder is not required to report security responses initiated as a result of threat or warning information communicated to the licensee or certificate holder by the NRC.

(7) A licensee's or certificate holder's request for immediate LLEA assistance can take precedence over the notification to the NRC.

2.2.2 Examples of Reportable Events

The NRC staff considers that the following transportation security events are examples of the types of events that require notification under 10 CFR 73.71(b).

a. the licensee's or certificate holder's discovery of an imminent or actual hostile action against its shipment of Category I SSNM, SNF, or HLW

b. the detonation of explosives or an explosive device at or near the licensee's or certificate holder's transport vehicle(s), including the use of explosives by ground assault force personnel and the use of land-based or waterborne VBIEDs

c. weapons being fired at the licensee's or certificate holder's transport vehicle(s) and projectiles hitting the transport vehicle(s) that cause an immediate threat to the shipment, security personnel, or vehicle operators

d. the successful, forcible penetration of a transport vehicle by unauthorized personnel

e. the taking of hostages onsite (e.g., shipping facility, receiving facility, or communications center) or offsite, related to shipment operations or security

f. the taking of hostages offsite that is reasonably determined to be related to shipment operations or security functions (e.g., the kidnapping of family members in order to coerce employees into violating laws, NRC regulations, or the shipping or receiving facility's license or certificate of compliance)

g. actual or believed theft or sabotage of a shipment of Category I SSNM, SNF, or HLW

h. the licensee's or certificate holder's notification by law enforcement authorities or another reliable source that an explosion or other assault against the shipment is imminent

i. the licensee's or certificate holder's initiation of a security response in accordance with its safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against its shipment of Category I SSNM, SNF, or HLW

Additionally, licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 and Appendix G.

2.3 Facility Security Events To Be Reported within 1 Hour

The regulations in 10 CFR 73.71(c) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 FR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 1 hour after the discovery of significant facility-security events specified in paragraph I of Appendix G to Part 73. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and Category III SNM facilities.

Generally, these events relate to committed or attempted acts and credible threats involving theft or diversion of SSNM or SNM; significant physical damage to the facilities identified above; interruption of normal operation of a facility caused by unauthorized operation or by tampering with controls, safety-related and nonsafety-related structures, systems, and components (SSCs); unauthorized entry of personnel into a PA, VA, MAA, or CAA; malevolent attempted entry of personnel into a PA, VA, MAA, or CAA; actual or attempted introduction of contraband into a PA, VA, MAA, or CAA; actual or attempted introduction of explosives or incendiaries beyond a vehicle barrier system; or an uncompensated vulnerability, failure, or degradation of security systems that could allow unauthorized access of personnel or contraband.

The NRC staff considers contraband to be unauthorized weapons, explosives, or incendiaries. Licensees and certificate holders may also identify "prohibited items" under their facility procedures. The staff considers contraband items and prohibited items as separate categories. Licensees and certificate holders are not required under these regulations to report attempted or actual introduction events involving prohibited items. In addition, items that are possessed by authorized persons for authorized purposes inside of the facility should not be considered contraband. For example, weapons possessed by the facility's security personnel as part of their official duties, weapons possessed by sworn law enforcement personnel visiting the facility, squib valves used in certain types of reactors, or explosives intended for authorized and controlled demolition or construction activities at the facility should not be considered contraband.

Reports made under this provision also apply to power reactor facilities that fall within the scope of 10 CFR 73.54 regarding the discovery that a cyber attack has occurred or has been attempted against systems, networks, or equipment that would compromise or has compromised the facility's safety, security, and emergency preparedness (SSEP) functions. These affected systems, networks, or equipment would be equal to or greater than a Level 3 or Level 4 network, as described in RG 5.71, "Cyber Security Program for Nuclear Facilities," (Ref. 7).

Reporting requirements include security events or information not otherwise reported as 15-minute notifications under 10 CFR 73.71(a) (i.e., an actual and substantial armed response to an imminent or actual hostile act) but that provide reason to believe that a person has caused or attempted to cause an event or has threatened to cause the types of events outlined in paragraph I of Appendix G. In terms of the 1-hour reporting requirement, "reason to believe" should be supported by reliable and substantive information that includes physical evidence supporting the threat; additional information independent of the threat; or the identification of a specific, known group, organization, or individual that claims responsibility for the threat. As used in Appendix G, "attempts" is defined in the glossary as reliable and substantive information that an effort was made to accomplish the threat, even though it has not occurred or has not been completed because it was interrupted or stopped before completion. These

reports include security events that are not imminent in nature and that may not necessarily result in the deployment of the security force or a contingency response. These events may result in a commitment of staff to search a facility at the request and with the assistance of law enforcement authorities.

Licensees and certificate holders should also report the interruption of normal operations resulting from intentional tampering or unauthorized use or manipulation of equipment or components. This could include intentional tampering with a system or equipment that is normally in a standby condition but would need to operate if called upon by personnel or automatic start signals. Licensees and certificate holders should initiate an appropriate preliminary evaluation of potential or actual interruptions of operations to determine whether the causes are human error, mechanical failure, or intentional acts. This evaluation should include reasonable actions or information collected within 1 hour of discovery of the event. Should a licensee or certificate holder initially determine that the collected information does not represent an actual or attempted threat and later changes its determination, it should notify the NRC of its change in determination.

Licensees or certificate holders may need to record other failures, degradations, or discovered vulnerabilities of security systems not related to unauthorized or undetected access, as described in paragraph IV of Appendix G.

Regulatory Position 3 provides guidance to the licensee or certificate holder if the Headquarters Operations Center requests a continuous communications channel or if followup notifications are needed.

2.3.1 Notification Requirements

10 CFR 73.71(c) One-hour notifications – facilities. (1) Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.60, or 73.67 shall notify the NRC Headquarters Operations Center within one hour after discovery of the facility safeguards events described in paragraph I of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

(3) Notifications made under paragraph (a) of this section are not required to be repeated under this paragraph.

Appendix G to Part 73, Paragraph I. Events to be reported within one hour of discovery.

(a) Significant security events. 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 threat to commit or cause:

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

(2) Significant physical damage to any nuclear reactor or facility possessing or using Category I strategic special nuclear material;

(3) Significant physical damage to any vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself;

(4) The unauthorized operation, manipulation, or tampering with any nuclear reactor's controls or with structures, systems, and components (SSCs) that results in the interruption of normal operation of the reactor; or

(5) The unauthorized operation, manipulation, or tampering with any Category I strategic special nuclear material (SSNM) facility's controls or SSCs that results in the interruption of normal operation of the facility.

(b) Unauthorized entry events.

(1) An actual entry of an unauthorized person into a facility's protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA).

(2) An actual entry of an unauthorized person into a transport vehicle.

(3) An attempted entry of an unauthorized person with malevolent intent into a PA, VA, MAA, or CAA.

(4) An attempted entry of an unauthorized person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(c) Contraband events.

(1) The actual introduction of contraband into a PA, VA, MAA, or CAA.

(2) The actual introduction of contraband into a transport.

(3) An attempted introduction of contraband by a person with malevolent intent into a PA, VA, MAA, or CAA.

(4) An attempted introduction of contraband by a person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(d) Authorized weapon events.

(1) The discovery that a standard weapon that is authorized by the licensee's security plan is lost or uncontrolled within a PA, VA, MAA, or CAA.

(2) Uncontrolled authorized weapons means weapons that are authorized by the licensee's or certificate holder's security plan and are not in the possession of authorized personnel or are not in an authorized weapons storage location.

(e) Vehicle barrier system events. For licensees and certificate holders with a vehicle barrier system protecting their facility, the actual or attempted introduction of explosives or incendiaries beyond the vehicle barrier.

(f) Uncompensated security events. Any failure, degradation, or the discovered vulnerability in a safeguard system, for which compensatory measures have not been employed, that could allow unauthorized or undetected access of—

(1) Explosives or incendiaries beyond a vehicle barrier;

(2) Personnel or contraband into a PA, VA, MAA, or CAA; or

(3) Personnel or contraband into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(g) Lost shipments of nuclear or radioactive material.

(1) The discovery of the loss of a shipment of Category I SSNM, Category II and III special nuclear material, spent nuclear fuel, or high-level radioactive waste.

(2) The recovery of or accounting for a lost shipment.

(h) Cyber security events.

(1) Any event in which there is reason to believe that a person has committed or caused, or attempted to cause, or has made a threat to commit or cause, an act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of § 73.54 of this part.

(2) Uncompensated cyber security events. Any failure, degradation, or the discovered vulnerability in systems, networks, and equipment that falls within the scope of § 73.54 of this part, for which compensatory measures have not been employed and that could allow unauthorized or undetected access into such systems, networks, or equipment.

(i) [Reserved]

(j) Loss or theft of classified information. The discovery of the loss or theft of classified material (e.g., documents, drawings, analyses, or data) that contains either National Security Information or Restricted Data.

(k) Loss or theft of Safeguards Information. The discovery of the loss or theft of material (e.g., documents, drawings, analyses, or data) that contains Safeguards Information –

(1) Provided that such material could substantially assist an adversary in the circumvention of the facility or transport security or protective systems or strategies; or

(2) Provided that such material is lost or stolen in a manner that could allow a significant opportunity for the compromise of the Safeguards Information.

2.3.2 Examples of Reportable Events

The NRC staff considers that the following facility-security events as examples of the types of events that require notification under 10 CFR 73.71(c) and paragraph I of Appendix G.

a. the successful, surreptitious penetration of a PA, VA, MAA, or CAA by unauthorized personnel

b. an actual entry (i.e., the unauthorized penetration or the actual circumvention of security control measures) by a person who is not authorized access to the specific area in question

   (1) This type of event is not intended to suggest that simple mistakes or other inadvertent entries should be reported within 1 hour.

   (2) Licensees and certificate holders should report actual entries that are the result of an intentional act or the failure of the security control to prevent the access of the person.

   (3) If licensees or certificate holders conclude that the entry of the individual was inadvertent and did not threaten facility security, they may record this event in the safeguards event log. However, if it represents a vulnerability or an uncompensated degradation in a security system that could allow intentional undetected or unauthorized access, the licensee should make a 1-hour notification.

c. entry attempts by unauthorized persons, vehicles, or material, meaning that reliable and substantive information indicates that (1) an effort to accomplish the entry, even though it has not yet occurred, is possible, or (2) the entry was not successful because it was interrupted or stopped before completion

d. an unauthorized entry attempt that was thwarted by responders or other security-system elements

e. absent other suspicious information licensees and certificate holders should not report personnel who attempt to enter or actually enter a controlled area by tailgating into areas where they are not authorized entry but could have been authorized, if necessary, and their entry is not considered a threat to the facility

f. the unauthorized entry of dismounted personnel onto or beyond the owner-controlled area (OCA) vehicle barrier system, reportable only when the actual or attempted entry threatens facility security; if there is an actual or attempted introduction of explosives or incendiaries beyond vehicle barriers, which are not designed to address dismounted individuals; or when the licensee or certificate holder identifies the entry as a threat

g. absent other suspicious information, licensees and certificate holders should not report hunters who inadvertently enter on to OCA as a 1-hour report, but should evaluate whether the event is appropriate for a 4-hour suspicious activity report

h. the actual or attempted introduction of contraband material (e.g., unauthorized weapons, explosives, or incendiaries)

(1) Licensees and certificate holders should conduct an appropriate evaluation within the reporting time to determine whether the actual or attempted introduction of contraband into a controlled area occurred.

(2) If the licensee or certificate holder concludes, within an hour, that the entry of the contraband was inadvertent and did not threaten facility security, they may record this event in the safeguards event log. However, if the event represents an uncompensated degradation or vulnerability that could allow intentional undetected or unauthorized access, the NRC requires a 1-hour report.

(3) An actual or attempted introduction of contraband into the OCA is reportable when the contraband has been determined to represent a threat capable of reducing the effectiveness of the physical security plan (e.g., firearms are discovered and the licensee or certificate holder determines they represent a threat to the facility). This example does not impose additional search requirements but addresses contraband that may be found pursuant to other activities.

i. the actual or attempted introduction of explosives or incendiaries beyond any vehicle barriers

j. a vehicle that strikes or challenges a component of the vehicle barrier system (VBS) in a manner that is more than a minor accident (i.e., the accident degrades the ability of the VBS to perform its intended functions)

k. uncompensated failures and degradations or discovered vulnerabilities of security systems that could allow unauthorized or undetected access to PAs, VAs, MAAs, or CAAs.

(1) Uncompensated means compensatory measures were included in applicable security plans or procedures that have not been implemented, were implemented incorrectly, or were ineffective. To clarify, for the uncompensated failures just discussed, licensees and certificate holders should report mechanical or electrical problems and failures or inadequacies in procedure implementation and personnel practices or performance.

l. the loss of intrusion detection and assessment capability that is not compensated in accordance with the facility's NRC-approved security plan

m. the loss of an alarm capability or locking mechanism at a material access portal that is not compensated in accordance with the facility's NRC-approved security plan

n. the failure to adequately compensate in a timely manner for an event or identified failure, degradation, or vulnerability that could allow undetected or unauthorized access to a PA, VA, MAA, or CAA

o. an uncompensated design flaw or vulnerability in a physical protection system that could have allowed unauthorized access to a PA, VA, MAA, or CAA or could have substantively eliminated or significantly reduced the licensee's or certificate holder's response capabilities

p. the uncompensated failure of all protected area lighting, when combined with any uncompensated outage of a PA perimeter intrusion detection, assessment, or delay systems

q. security events that could allow undetected or unauthorized access within 1 hour, usually affecting multiple layers of physical security systems or an individual, critical, single failure of a program element that would allow undetected or unauthorized access, or other failures,

degradations, or discovered vulnerabilities of security systems not relating to unauthorized or undetected access that may need to be recorded as described in paragraph IV of Appendix G

r. security events that involve an interruption of the normal operation of the licensee's or certificate holder's facility through the unauthorized use of, or tampering with, its components, controls, or security systems, as described below:

(1) Tampering with plant equipment or physical security equipment that is confirmed to be suspicious, destructive, or malevolent; is not a reasonable mechanical failure; or is related to willful human error is reportable. Licensees and certificate holders should report, within 1 hour, tampering that results in an interruption of the normal operations of the facility. They should report tampering that does not result in an interruption of normal operations under the 4-hour or 8-hour notification requirements. Licensees and certificate holders should report events that are suspicious in nature and where a general assessment cannot be made within 1 hour, under the 4-hour or 8-hour notification requirements.

(2) Confirmed cyber attacks on computer systems that may adversely affect safety, security, and emergency preparedness systems are reportable.

(3) An actual or imminent strike (labor work slowdown or stoppage) by the security force is reportable.

(4) A mass demonstration at or near the facility is reportable if the protesters do not have a demonstration permit from the appropriate local authorities or the demonstration is not overseen by LLEA personnel. The NRC staff considers a mass demonstration to consist of five or more individuals. A demonstration of less than five individuals for which the licensee or certificate holder has requested LLEA assistance would be reportable as a 4-hour notification under Regulatory Position 2.5 below.

(5) A mass demonstration at or near the facility with the appropriate demonstration permits and LLEA oversight presence is reportable if LLEA personnel loses control of the demonstration and demonstrators enter the facility's property.

(6) Bomb or extortion threats are reportable if the licensee or certificate holder considers them credible and substantive (this includes the discovery of intent to commit such an act). In addition, the results of any bomb search should be reported within 1 hour of completion.

(7) The loss of all offsite communications capabilities is reportable if they are required to meet regulatory requirements (i.e., specified in the licensee's or certificate holder's security plans).

(8) The loss or theft of a standard weapon from inside of the licensee's or certificate holder's PA, VA, MAA, or CAA. Reporting of the loss or theft of an enhanced weapon is discussed in Regulatory Position 2.7 below.

s. the discovery of a criminal act involving individuals granted unescorted access that could provide an opportunity to adversely affect facility safety or that represents a threat (e.g., crimes such as sabotage, arson, bombing, tampering with nuclear facilities, murder, being a member of a terrorist organization, or battery against plant staff; crimes involving nonviolent activities, such as espionage, drug trafficking, counterfeiting, conspiracy to commit a serious crime)

t. the discovery of falsified identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to controlled areas

u. the discovery of improper control over access-control equipment (e.g., badge fabrication, access-control computers, key cards, passwords, cipher codes), if the event results in actual or attempted use of the equipment or media where an unauthorized individual could or did gain entry into a controlled area

v. the uncompensated loss of all alternating current (ac) power to security systems that could allow unauthorized or undetected access to a PA, VA, MAA, or CAA

w. incomplete or inaccurate preauthorization screening that could have resulted in unescorted access authorization, had the screening been complete and accurate (involving either the authorization or the granting of unescorted access)

x. the discovery of lost or stolen classified documents containing either national security information or restricted data.

y. the discovery of lost or stolen Safeguards Information that would substantially assist an adversary in the circumvention of security systems or the loss of Safeguards Information in a manner that could allow a significant opportunity for the Safeguards Information to be compromised, where "substantially" refers to the characteristics and essential parts of the information (i.e., its composition or content) and "significant" refers to the importance or meaning of the information (i.e., its value)

z. the unavailability of the minimum number of on duty security personnel in a shift after implementation of the appropriate recall procedures

aa. the successful, surreptitious penetration or compromise of a critical digital asset (CDA) by unauthorized personnel

bb. an actual penetration or compromise of a CDA, where a person who is not authorized access circumvented the control measures

(1) The regulation for reporting this type of event is not intended to suggest that simple mistakes or other inadvertent entries should be reported within 1 hour.

(2) Licensees and certificate holders should report actual entries that are the result of an intentional act or breakdown of the security program or security measures.

(3) If the licensee or certificate holder concludes that the actions of the individual were inadvertent and did not threaten facility security, it may record this event in the safeguards event log. However, if the event represents an uncompensated degradation or vulnerability that could allow intentional undetected or unauthorized access to SSEP functions, the licensee or certificate holder should make a 1-hour notification.

(4) Attempts by unauthorized persons means that reliable and substantive information indicates that (1) an effort to accomplish the cyber attack, even though it has not yet occurred, is possible, or (2) the cyber attack was not successful because it was interrupted or stopped before completion.

(5) Licensees or certificate holders should report a cyber attack that was thwarted by responders or other security system elements if a successful attack would have had an adverse impact on SSEP functions.

cc. the discovery of malware, unauthorized software, or firmware installed on a CDA

dd. failures, degradations, or discovered vulnerabilities of CDAs or security measures that protect CDAs that would be likely to allow unauthorized or undetected access to those CDAS or that could result in compromising the CDA or an SSEP function when compensatory measures have not been employed (i.e., uncompensated)

ee. the theft of sensitive cyber security data

ff. the loss of cyber intrusion detection capability that is uncompensated in accordance with the facility's NRC-approved cyber security plan

gg. the failure to adequately compensate, in a timely manner, for an event or identified failure, degradation, or vulnerability that could allow undetected or unauthorized access or modification to a CDA

hh. an uncompensated design flaw or vulnerability in a cyber protection system that could have allowed unauthorized access to CDAs or could have substantively eliminated or significantly reduced the licensee's response capabilities

ii. cyber security events that could allow undetected or unauthorized access or modifications to CDAs within 1 hour, that usually affect multiple layers of cyber security systems or an individual, critical, single failure of a program element that would allow undetected or unauthorized access to CDAs

jj. the discovery of falsified identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to CDAs

kk. the discovery of improper control over access-control equipment (e.g., badge fabrication, access-control computers, key cards, passwords, cipher codes), if the event results in the actual or attempted use of the equipment or media where an unauthorized individual could or did gain entry to a CDA

ll. the uncompensated loss of all ac power to security systems that could allow unauthorized or undetected access to a CDA

mm. the discovery of lost or stolen Safeguards Information that would substantially assist an adversary in the circumvention of cyber security systems or the loss of Safeguards Information in a manner that could allow a significant opportunity for a CDA to be compromised, where "substantially" refers to the characteristics and essential parts of the information (i.e., its composition or content) and "significant" refers to the importance or meaning of the information (i.e., its value).

nn. the unavailability of the minimum number of cyber security response personnel after implementation of the appropriate recall procedures

oo. uncompensated failures, degradations, or discovered vulnerabilities with a CDA, personnel responses, communications, monitoring, or oversight that could increase the likelihood of an attempted attack on any CDA

Additionally, licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G.

2.4 Transportation Security Events To Be Reported within 1 Hour

The regulations in 10 CFR 73.71(d) require each licensee or certificate holder subject to the provisions of 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 1 hour after the discovery of significant transportation-security events specified in paragraph I of Appendix G. This regulation applies to licensees and certificate holders shipping Category I SSNM, Category II and III SNM, SNF, and HLW. These shipments may be made under any mode (including highway, rail, airborne, or water) by the licensee or certificate holder (i.e., private carriage) or by a transportation company under contract to the licensee or certificate holder (i.e., public carriage).

Licensees and certificate holders shipping materials by a U.S. Department of Energy (DOE) transportation system (e.g., the DOE Office of Secure Transportation) remain subject to the security event reporting and recording requirements of 10 CFR 73.71 and Appendix G. The NRC staff notes that, although licensees and certificate holders shipping materials are exempt under 10 CFR 73.6(d) from the applicable physical security requirements of 10 CFR Part 73, 10 CFR 73.6, "Exemptions for Certain Quantities and Kinds of Special Nuclear Material," does not exempt them from the security event reporting and recording requirements of 10 CFR 73.71 and Appendix G.

Generally, these events relate to committed or attempted acts and credible threats involving the theft or diversion of SSNM or SNM; significant physical damage to any vehicle transporting SNM, SNF, or HLW; significant physical damage to the SNM, SNF, or HLW itself; actual entry of an unauthorized person into a transport vehicle; attempted entry of an unauthorized person with malevolent intent into a vehicle transporting SNM, SNF, or HLW or into the SNM, SNF, or HLW itself; actual entry of contraband into a transport vehicle; and attempted introduction of contraband with malevolent intent into a vehicle transporting SNM, SNF, or HLW or into the SNM, SNF, or HLW itself.

Reporting requirements under this provision include security events or information not otherwise reported as 15-minute notifications under 10 CFR 73.71(b) (i.e., events requiring an actual and substantial armed response to an imminent or actual hostile act) but that provide reason to believe that a person has caused or attempted to cause an event or has threatened to cause the types of events outlined in paragraph I of Appendix G. In terms of the 1-hour reporting requirement, "reason to believe" should be supported by reliable and substantive information that includes physical evidence supporting the threat; additional information independent of the threat; or the identification of a specific, known group, organization, or individual that claims responsibility for the threat. As used in Appendix G, "attempts" is defined in the glossary to mean that reliable and substantive information exists regarding an effort to accomplish the threat, even though it has not occurred or has not been completed because it was interrupted or stopped before completion. These reports include security events that are not imminent in nature and that may not necessarily result in a substantive armed response or deployment of the security force or a contingency response. These events may result in a commitment of staff to search a transport vehicle at the request and with the assistance of law enforcement authorities.

The regulations permit licensees and certificate holders to directly report transportation events to the NRC themselves, or to use a contract service communications center to monitor and communicate with the shipment, contact LLEA if required, and report events to the NRC.

Regulatory Position 3 provides guidance to the licensee or certificate holder if the Headquarters Operations Center requests a continuous communications channel or if followup notifications are needed.

2.4.1 Notification Requirements

10 CFR 73.71(d) One-hour notifications - shipments. (1) Each licensee or certificate holder subject to the provisions of §§ 73.25, 73.26, 73.27, 73.37, and 73.67 shall notify the NRC Headquarters Operations Center within one hour after discovery of the transportation safeguards events described in paragraph I of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

(3) Notifications made under paragraph (b) of this section are not required to be repeated under this paragraph.

Appendix G to Part 73, Paragraph I. Events to be reported within one hour of discovery.

(a) Significant security events. 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 threat to commit or cause:

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

(2) Significant physical damage to any nuclear reactor or facility possessing or using Category I strategic special nuclear material;

(3) Significant physical damage to any vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself;

(4) The unauthorized operation, manipulation, or tampering with any nuclear reactor's controls or with structures, systems, and components (SSCs) that results in the interruption of normal operation of the reactor; or

(5) The unauthorized operation, manipulation, or tampering with any Category I strategic special nuclear material (SSNM) facility's controls or SSCs that results in the interruption of normal operation of the facility.

(b) Unauthorized entry events.

(1) An actual entry of an unauthorized person into a facility's protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA).

(2) An actual entry of an unauthorized person into a transport vehicle.

(3) An attempted entry of an unauthorized person with malevolent intent into a PA, VA, MAA, or CAA.

(4) An attempted entry of an unauthorized person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(c) Contraband events.

(1) The actual introduction of contraband into a PA, VA, MAA, or CAA.

(2) The actual introduction of contraband into a transport.

(3) An attempted introduction of contraband by a person with malevolent intent into a PA, VA, MAA, or CAA.

(4) An attempted introduction of contraband by a person with malevolent intent into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(d) Authorized weapon events.

(1) The discovery that a standard weapon that is authorized by the licensee's security plan is lost or uncontrolled within a PA, VA, MAA, or CAA.

(2) Uncontrolled authorized weapons means weapons that are authorized by the licensee's or certificate holder's security plan and are not in the possession of authorized personnel or are not in an authorized weapons storage location.

(e) Vehicle barrier system events. For licensees and certificate holders with a vehicle barrier system protecting their facility, the actual or attempted introduction of explosives or incendiaries beyond the vehicle barrier.

(f) Uncompensated security events. Any failure, degradation, or the discovered vulnerability in a safeguard system, for which compensatory measures have not been employed, that could allow unauthorized or undetected access of—

(1) Explosives or incendiaries beyond a vehicle barrier;

(2) Personnel or contraband into a PA, VA, MAA, or CAA; or

(3) Personnel or contraband into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(g) Lost shipments of nuclear or radioactive material.

(1) The discovery of the loss of a shipment of Category I SSNM, Category II and III special nuclear material, spent nuclear fuel, or high-level radioactive waste.

(2) The recovery of or accounting for a lost shipment.

(h) Cyber security events.

(1) Any event in which there is reason to believe that a person has committed or caused, or attempted to cause, or has made a threat to commit or cause, an act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of § 73.54 of this part.

(2) Uncompensated cyber security events. Any failure, degradation, or the discovered vulnerability in systems, networks, and equipment that falls within the scope of § 73.54 of this part, for which compensatory measures have not been employed and that could allow unauthorized or undetected access into such systems, networks, or equipment.

(i) [Reserved]

(j) Loss or theft of classified information. The discovery of the loss or theft of classified material (e.g., documents, drawings, analyses, or data) that contains either National Security Information or Restricted Data.

(k) Loss or theft of Safeguards Information. The discovery of the loss or theft of material (e.g., documents, drawings, analyses, or data) that contains Safeguards Information –

(1) Provided that such material could substantially assist an adversary in the circumvention of the facility or transport security or protective systems or strategies; or

(2) Provided that such material is lost or stolen in a manner that could allow a significant opportunity for the compromise of the Safeguards Information.

2.4.2 Examples of Reportable Events

The NRC staff considers that the following transportation-security events as examples of the types of events that require notification under the requirements of 10 CFR 73.71(d) and paragraph I of Appendix G.

a. the successful, surreptitious penetration of a transport vehicle by unauthorized personnel

b. a shipment of Category I SSNM, Category II or III SNM, SNF, or HLW that is believed to be lost

c. recovery of a lost Category I SSNM, Category II or III SNM, SNF, or HLW shipment

d. notification of law enforcement authorities subsequent to the discovery of a suspicious vehicle following a licensed carrier transporting Category I SSNM, Category II or III SNM, SNF, or HLW

e. the discovery of an attempted theft of a shipment of Category I SSNM, Category II or III SNM, SNF, or HLW

f. the actual or attempted introduction of contraband material (e.g., unauthorized weapons, explosives, or incendiaries) into the transport vehicle that is transporting the Category I SSNM, Category II or III SNM, SNF, or HLW or into the. nuclear or radioactive material itself

g. uncompensated failures, degradations, or discovered vulnerabilities with a transportation system's security hardware, equipment, and personnel responses, communications, monitoring, or oversight that could increase the likelihood of an attempted theft of a shipment of Category I SSNM, Category II or III SNM, SNF, or HLW.

Additionally, licensees and certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G.

2.5 Facility Security Events To Be Reported within 4 Hours

The regulations in 10 CFR 73.71(e) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 4 hours after the discovery of facility-security events specified in paragraph II of Appendix G. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and III SNM facilities.

Four-hour notifications fall within three categories—suspicious activities; unauthorized operation, manipulation, or tampering events that do not result in the interruption of facility operations, but could prevent the implementation of the protective strategy for protecting any target set; and notifications to and responses from LLEAs.

The reporting of suspicious activities is an important component of evaluating the threat against licensed facilities and material. The NRC reviews individual notifications of suspicious activities to evaluate whether potential preoperational activities (i.e., multiple events at a single site or multiple events at multiple sites) may be part of a larger plan and to integrate this information with other agencies in the homeland security and intelligence communities. The NRC is not requesting that the licensees and certificate holders actively gather intelligence, but rather that they report information they believe is relevant to the security of their facility or activity. The NRC staff has added examples of suspicious events that should be reported to the NRC. The U.S. government considers suspicious activity as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Additionally, licensees and certificate holders are considered "key resource owners and operators" and can find additional guidance on examples of suspicious events in the U.S. Department of Homeland Security's, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," (Ref. 8). This reporting guide is designated as "Unclassified and For Official Use Only."

Licensees or certificate holders should not report events based solely on speculation. They should report events that are believed to be real, including those substantiated by observations by licensee or certificate holder staff or local law enforcement personnel, evidence of the presence of unknown personnel, telephone contacts, suspicious documents, and testimony of credible witnesses. Licensees' and certificate holders' corporate and contractor personnel may also be sources of this information. Licensees and certificate holders can obtain additional information from the NRC, about terrorist activities or suspicious events they may encounter during the course of normal activities, on NRC's protected Web server under Event No. 2464.

The NRC staff recommends that licensees and certificate holders contact organizations in their local area (i.e., military, government, law enforcement, and private sector) that could conduct aircraft operations in airspace over or near their facilities. Licensees and certificate holders should identify respective points of contact with these organizations in order to coordinate advance notification of upcoming activities and to verify any ongoing suspicious aircraft activity that was not previously coordinated.

The unauthorized operation, manipulation, or tampering events reported under this notification includes events that fall outsides the 1-hour notification requirements (i.e., the event did not result in the interruption of facility operations) but that could prevent the implementation of the licensee's or certificate holder's protective strategy for the facility.

The NRC requires 4-hour notifications from licensees and certificate holders subject to 10 CFR 73.54, if they discover information that indicates that tampering; unauthorized access, use or modifications; or unauthorized gathering of information or data on systems has occurred or is occurring on networks or equipment within the scope of 10 CFR 73.54 or if the security measures that protect these SSEP functions are degraded.

The NRC's purpose in gathering notifications of communications to or from local law enforcement authorities is to enable the NRC to respond to any potential public and media inquires resulting from licensee, certificate holder, or LLEA actions at NRC-regulated facilities. This objective is similar to other 4-hour safety-related notifications regarding press releases and contact with other agencies that are found elsewhere in the NRC's regulations.

2.5.1 Notification Requirements

10 CFR 73.71(e) Four-hour notifications – facilities. (1) Each licensee subject to the provisions of §§ 73.20, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.60, or 73.67 shall notify the NRC Headquarters Operations Center, as soon as possible but not later than four hours after discovery of the safeguards events described in paragraph II of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

Appendix G, Paragraph II. Events to be reported within four hours of discovery.

(a) Suspicious events. Any information received by the licensee of suspicious or surveillance activities or attempts at access, including:

(1) Any event or incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility. This type of activity may include, but is not limited to—

(A) Attempted surveillance or reconnaissance activity. Commercial or military aircraft activity considered routine or non-threatening by the licensee or certificate holder is not required to be reported;

(B) Elicitation of information from facility personnel relating to the security or safe operation of the facility; or

(C) Challenges to security systems (e.g., willful failure to stop for security checkpoints, possible tests of security response and security screening equipment, or suspicious entry of watercraft into posted off-limits areas).

(2) Any event or incident involving suspicious aircraft activity over or in close proximity to the facility. Commercial or military aircraft activity considered routine or non-threatening by the licensee or certificate holder is not required to be reported.

(b) Unauthorized operation or tampering events. An event involving—

The unauthorized operation, manipulation, or tampering of any nuclear reactor's or Category I SSNM facility's SSCs that could prevent the implementation of the licensee's or certificate holder's defensive strategy for protecting any target set.

(c) Suspicious cyber security events.

(1) Any information received or collected by the licensee or certificate holder of suspicious activity that may be indicative of tampering, malicious or unauthorized access, use, operation, manipulation, modification, potential destruction, or compromise of the systems, networks, and equipment that falls within the scope of § 73.54 of this part, or the security measures that could weaken or disable the protection for such systems, networks, or equipment.

(2) An attempted but unsuccessful cyber attack or event that could have caused significant degradation to any system, network, or equipment that falls within the scope of § 73.54 of this part.

(d) Law enforcement interactions. (1) An event related to the licensee's or certificate holder's implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials and that does not otherwise require a notification under paragraph I or the other provisions of paragraph II of this appendix.

(2) An event involving a law enforcement response to the facility that could reasonably be expected to result in public or media inquiries and that does not otherwise require a notification under paragraphs I or the other provisions of paragraph II of this appendix.

2.5.2 Examples of Reportable Events

The NRC staff considers that the following security events as examples of the types of events that require notification under 10 CFR 73.71(e) and paragraph II of Appendix G.

The following are examples of security-related events involving suspicious activity that may indicate preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees, certificate holders, or their facilities:

a. individual(s) with non-routine interests or inquiries related to security measures, personnel or vehicle entry points and access controls, or vehicle barrier systems, including fences, walls, or other barriers

b. individual(s) conducting unapproved photographing or videotaping of licensed facilities on owner controlled property

c. individual(s) conducting unapproved photographing or videotaping of licensed facilities from public property or non-owner controlled property when combined with other suspicious information gathered by security personnel challenges to, or interviews of, the individuals

d. suspicious attempts to recruit or compromise employees or staff, including contractors, knowledgeable of key personnel, facilities, or systems, into providing classified information, Safeguards, information, or other sensitive physical security or cyber security information

e. loitering for no apparent purpose in areas where intelligence could be gathered or where preoperational reconnaissance could be performed

f. suspicious behavior (e.g., fleeing, moving quickly away from licensee or certificate holder personnel, unexpected vehicular movement)

g. secretive sketching, making maps, or taking notes on the owner controlled area

h. eliciting information from security or other site personnel regarding security systems or vulnerabilities

i. unusual challenges to security systems that could represent attempts to gather information on system performance or personnel or equipment response actions

j. unauthorized attempts to probe or gain access to the licensee's or certificate holder's business secrets or other sensitive information or to control systems, including the use of social engineering techniques (e.g., impersonating authorized users)

k. theft or suspicious loss of official company identification documents, uniforms, or vehicles necessary for accessing plant facilities

l. use of forged, stolen, or fabricated documents to support access control or authorization activities

m. boating activities conducted in unauthorized locations or attempts to loiter near facility restricted areas

n. unusual attempts to obtain information or documents related to site security training, techniques, procedures, or practices

o. discovery of Internet site postings that make violent threats related to specific licensed facilities or activities

p. unusual threats or terrorist-related activities that become known to facility security or management involving the following: (1) unusual surveillance, probing or reconnaissance, (2) attempts to gain unauthorized access, (3) attempts to gain access to or acquire hazardous or dangerous materials, (4) unusual use of materials, or (5) financing to support terrorist activities

q. stated threat(s) against the licensee's or certificate holder's facility or staff, unless they are determined to be unsubstantiated

r. unsubstantiated bomb or extortion threats that are considered to be related to harassment, including those representing tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations (such evens should be recorded in the safeguards log until a pattern is discovered)

s. fires or explosions of suspicious or unknown origin within an OCA, PA, VA, or MAA that have not been reported under the 15-minute or 1-hour notification requirements of 10 CFR 73.71 and do not represent an immediate or significant impact on the safe operation of the facility or disrupt its normal operations

The following are examples of aircraft overflight activities that do not represent an immediate threat to the facility but may be indicative of preoperational surveillance, reconnaissance, or intelligence-gathering activities directed against licensees, certificate holders, or their facilities:

t. Licensees or certificate holders should report to the NRC multiple sightings of the same commercial or general aviation aircraft, circling or loitering above or in close proximity to their facilities, or photographing the facilities or surrounding areas. Appendix A of this RG outlines additional guidance for reporting suspicious aircraft activity and recommendations for licensee or certificate holder precoordination efforts to reduce false positive (unnecessary) reports.

u. Licensees and certificate holders should exercise judgment and discretion in determining whether flight activity is suspicious with respect to normal air traffic patterns in their locality. Factors that may be considered in evaluating normal air traffic patterns include proximity of the facility to local public, private, and commercial airports; U.S. military bases; the use of rivers, coastal waterways, and prominent landmarks (e.g., cooling towers) for navigational purposes; local weather conditions; and other local circumstances.

v. Licensees and certificate holders are not required to notify the NRC of coordinated aircraft operations in airspace over or near their facilities.

w. Licensees and certificate holders are not required to notify the NRC of military, government, and law enforcement aircraft operations in the airspace over or near their facilities that were not previously coordinated, provided the licensee or certificate holder communicates with the preestablished point of contact and verifies that the aircraft operations were, in fact, planned but not previously coordinated with the licensee or certificate holder.

The following are examples of events involving the notification or unanticipated response of local, State, or Federal law enforcement agencies that do not involve the licensee's or certificate holder's implementation of its contingency response plan or protective strategy:

x. Licensees and certificate holders should notify the NRC of law enforcement personnel onsite to arrest a felon or fugitive from justice or to execute a search warrant.

y. Licensees and certificate holders should notify the NRC of law enforcement personnel's pursuit of subjects into the facility's OCA.

z. Licensees and certificate holders should notify the NRC of requests for law enforcement response to the facility because a crime may have been committed (e.g., assault and battery or discovery of controlled substances or unauthorized weapons).

aa. Licensees and certificate holders are not required to notify the NRC of law enforcement personnel onsite for nonresponse duties, training exercises, familiarization and coordination activities, other scheduled activities, or the sharing of information.

The following are examples of unauthorized use or tampering with components or controls, including the security system, that do not interrupt the normal operation of the plant but could prevent the implementation of the licensee's or certificate holder's protective strategy for protecting any target set. Licensees or certificate holders should report the act of tampering, rather than the effects of the tampering, because it is not known whether the tampering could create potentially significant equipment issues.

bb. the unauthorized operation, manipulation, or tampering with a nuclear reactor's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the reactor

cc. the unauthorized operation, manipulation, or tampering with a Category I SSNM facility's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the facility

dd. the unauthorized operation, manipulation, or tampering with security-related SSCs that could prevent the implementation of the licensee's or certificate holder's protective strategy for protecting the SSCs in a target set

ee. the intentional cutting of wires that does not affect the facility or security operations

ff. the overt changing of equipment or controls to settings that do not affect their intended function

gg. the tampering with, or the destruction of, equipment that does not affect plant operations (e.g., water coolers, office equipment, maintenance tools)

hh. the modification of security equipment that renders the equipment inoperable

ii. the lost or theft of standard security weapons from a location outside of the licensee's or certificate holder's PA or CAA, provided the weapon could affect the implementation of the licensee's or certificate holder's protective strategy (e.g., high-power weapons or long weapons); otherwise the event should be recorded in the Safeguards Event Log

jj. the loss or theft of enhanced security weapons from a location outside of the licensee's or certificate holder's PA or CAA is discussed in Regulatory Position 2.7

The following are examples of surveillance or reconnaissance of cyber systems; of tampering, malicious or unauthorized access, use, operation, manipulation, modification, potential destruction, or compromise of the systems, networks, and equipment that fall within the scope of 10 CFR 73.54; or of the security measures that could weaken or disable the protection for such systems, networks, or equipment:

kk. the discovery of individuals with uncommon interests or inquiries related to the facility's cyber security measures, personnel, or security controls

ll. the discovery of unauthorized personnel at or near the plant performing wireless reconnaissance of the licensee's wireless networks and communications systems

mm. the discovery of individuals eliciting or attempting to elicit information from security or other facility personnel regarding CDAs, security measures, or vulnerabilities for SSEP functions

nn. the discovery of the theft or suspicious loss of smart cards, tokens, or other "two factor" authentication systems necessary for accessing CDAs

oo. the discovery of the use of forged, stolen, or fabricated smart cards, tokens or other "two factor" authentication devices used to support access control to CDAs or authorization activities

pp. the discovery of unsubstantiated cyber attack threats that are considered to be related to harassment, including threats that could also represent tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations (to be recorded in the safeguards log until a pattern is discovered)

qq. the discovery of an active attack, virus, or worm on an network adjacent to CDAs that, if security barriers were not in place, could adversely affect CDAs or SSEP functions

rr. Information that a compromise of cyber systems has occurred but without the licensee or certificate holder experiencing any degradation of SSEP functions (although recommending that the licensee or certificate holder investigate the extent of the compromise to discover if any CDAs or SSEP functions have been affected)

ss. the discovery of the degradation or failure of a CDA that is of suspicious or unknown origin that has not been reported under the 15-minute or 1-hour notification requirements and does not have an immediate or significant impact on SSEP functions or the normal operation of the facility

Additionally, licensees and certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G.

2.6 Facility-Security Events To Be Reported within 8 Hours

The regulations in 10 CFR 73.71(f) require each licensee or certificate holder subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67 to notify the NRC Headquarters Operations Center as soon as possible but not later than 8 hours after the discovery of facility-security events specified in paragraph III of Appendix G. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and Category III SNM facilities.

Eight-hour notifications fall into two categories—(1) the licensee or certificate holder detects unauthorized operation, manipulation, or tampering events that do not result in the interruption of facility operations and do not prevent the implementation of the protective strategy (i.e., these events are not reportable under the 1-hour or 4-hour notification requirements), or (2) the licensee or certificate holder detects an unauthorized operation or manipulation of, or tampering with, networks or equipment within the scope of 10 CFR 73.54 or the security measures that protect such networks and equipment, but such actions did not interrupt or degrade the facility's SSEP functions.

2.6.1 Notification Requirements

10 CFR 73.71(f) Eight-hour notifications – facilities. (1) Each licensee subject to the provisions of §§ 73.20, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.60, or 73.67 shall notify the NRC Headquarters Operations Center, as soon as possible but not later than eight hours after discovery of the safeguards events described in paragraph III of Appendix G to this part.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

Appendix G, Paragraph III. Events to be reported within eight hours of discovery.

Unauthorized operation or tampering events. An event involving—

(1) The unauthorized operation, manipulation, or tampering with any nuclear reactor's controls or SSCs that does not result in the interruption of the normal operations of the reactor;

(2) The unauthorized operation, manipulation, or tampering with any Category I SSNM facility's controls or SSCs that does not result in the interruption the normal operations of the facility; or

(3) The tampering, malicious or unauthorized access, use, operation, manipulation, or modification of any security measures associated with systems, networks, and equipment that falls within the scope of § 73.54 of this part, that does not result in the interruption of the normal operation of such systems, networks, or equipment.

2.6.2 Examples of Reportable Events

The NRC staff considers that the following facility-security events as examples of the types of events that require notification under 10 CFR 73.71(f) and paragraph III of Appendix G.

The following are examples of unauthorized use or tampering with components or controls, including the security system, that does not interrupt the normal operation of the plant and does not prevent the implementation of the licensee's or certificate holder's protective strategy (i.e., events that are reportable under the 1-hour or 4-hour notification requirements). The act of tampering should be reported, rather than the effects of the tampering, because it is not known whether the tampering could create potentially significant equipment issues.

a. the unauthorized operation, manipulation, or tampering with a nuclear reactor's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the reactor

b. the unauthorized operation, manipulation, or tampering with a Category I SSNM facility's controls, safety-related SSCs, or nonsafety-related SSCs that do not interrupt the normal operations of the facility

c. the unauthorized operation, manipulation, or tampering with the security-related SSCs that could prevent the implementation of the licensee's or certificate holder's protective strategy

d. the intentional cutting of wires that does not affect the facility or security operations

e. the modification of security equipment that renders the equipment inoperable

f. the overt changing of equipment or controls to settings that do not affect their intended function

g. the tampering with, or destruction of, equipment that does not affect plant operations or security (e.g., water coolers, office equipment, maintenance tools)

The following are examples of unauthorized operation or manipulation of, or tampering with, networks or equipment within the scope of 10 CFR 73.54 or the security measures that protect such networks and equipment but where such actions did **not** interrupt or degrade the facility's SSEP functions:

h. the discovery of a vulnerability in a CDA or security measures, but with compensatory measures in place to mitigate the issue

i. the discovery that a CDA is disabled or has failed but does not degrade any SSEP functions

j. the discovery of the loss of control of a mobile CDA but the device has adequate "data at rest" protection and automatically wipes itself after a period of inactive use

Additionally, licensees or certificate holders should evaluate an event that is not reportable under this requirement for reporting or recording under the other provisions of 10 CFR 73.71 or Appendix G to 10 CFR Part 73.

2.7 Enhanced Weapons—Stolen or Lost, To Be Reported within 1 Hour or 4 Hours

The regulations in 10 CFR 73.71(g) require each licensee or certificate holder subject to the provisions of 10 CFR 73.18 who possesses enhanced weapons to notify the NRC Headquarters Operations Center as soon as possible but not later than either 1 hour or 4 hours (see below) after the discovery that their enhanced weapon has been stolen or lost. This regulation applies to the classes of facilities, radioactive material, and other property designated by the Commission in 10 CFR 73.18(c).

Licensees and certificate holders must make a 1-hour notification to the NRC upon the discovery that an enhanced weapon is missing from inside the PA, VA, or MAA of a designated facility. Licensees and certificate holders must make a 4-hour notification to the NRC subsequent to notifying ATF upon the discovery that an enhanced weapon is missing from outside the PA, VA, or MAA of a designated facility. The NRC staff views uncontrolled enhanced weapons inside a facility authorized to possess them as a greater risk to the facility (i.e., potential insider issue) that should be treated the same as other significant security events that warrant a 1-hour notification. In contrast, uncontrolled enhanced weapons outside a facility are considered less of an immediate risk to the facility itself, and may instead present a law enforcement risk (i.e., the weapons could assist in the commission of a crime away from the facility). Examples include enhanced weapons being stolen or lost outside a PA, VA, or MAA (e.g., from a training facility or while the weapons were being transported back after escorting a designated shipment of radioactive material).

A licensee or certificate holder possessing enhanced weapons is required to notify ATF under 27 CFR 479.141 (Ref. 9) independent of any notifications made to the NRC of stolen or lost enhanced weapons. However, licensees and certificate holders should notify the NRC first of weapons that are stolen or lost from within their PA, VA, or MAA, because the NRC staff considers enhanced weapons lost or unsecured within a facility as posing a threat to the facility (e.g., their use by an active-violent insider). The NRC staff considers enhanced weapons that are discovered to be stolen or lost outside of these facility security areas to have a greater potential for criminal activity separate from the licensee's or certificate holder's facility. Therefore, the licensee or certificate holder should notify ATF first in those circumstances.

In addition to notifying the NRC, 10 CFR 73.71(g)(1) requires licensees and certificate holders to notify appropriate LLEA officials within 48 hours of the discovery of stolen or lost enhanced weapons.

The regulations in 10 CFR 73.18 provide a distinction between the transfer of enhanced weapons (between two registered or licensed owners) and the transportation of enhanced weapons by a single owner/registrant (to and from the facility). The following examples reflect this distinction.

2.7.1 Notification Requirements

10 CFR 73.71(g) Enhanced weapons – stolen or lost. (1) Each licensee or certificate holder possessing enhanced weapons in accordance with the provisions of § 73.18 shall —

(i) Notify the NRC Headquarters Operations Center, as soon as possible but not later than one hour after the discovery of any stolen or lost enhanced weapons possessed by the licensee or certificate holder. This notification applies to enhanced weapons that were stolen or lost from within a licensee's or certificate holder's protected area, vital area, or material access area.

(ii) Notify the NRC Headquarters Operations Center, as soon as possible but not later than four hours subsequent to the notification of the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) of the discovery of any stolen or lost enhanced weapons possessed by the licensee or certificate holder. This notification applies to enhanced weapons that were stolen or lost from outside of the licensee's or certificate holder's protected area, vital area, or material access area.

(iii) Notify the appropriate local law enforcement officials, as soon as possible but not later than 48 hours of the discovery of stolen or lost enhanced weapons. These notifications must be made by telephone to the appropriate local law enforcement officials. Licensees and certificate holders shall identify the appropriate local law enforcement officials for these notifications and include their contact phone number(s) in written procedures.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

(3) Independent of the requirements of this section, licensees and certificate holders possessing enhanced weapons in accordance with § 73.18 also have an obligation under ATF's regulations to immediately upon discovery notify ATF of any stolen or lost enhanced weapons (see 27 CFR 479.141).

2.7.2 Examples of Reportable Events

The NRC staff considers that the following security events as examples of the types of events that require notification under 10 CFR 73.71(g).

a. enhanced weapons are lost during shipment to or from the licensee's or certificate holder's facility (e.g., a training facility or during the transportation of weapons preceding or following escort duties of a designated shipment of nuclear or radioactive material) (4-hour notification)

b. enhanced weapons are lost during transfer to another authorized NRC licensee or certificate holder (4-hour notification)

c. enhanced weapons are lost during transfer to another Federal firearms license holder or government agency (4-hour notification)

d. enhanced weapons are discovered missing from their authorized storage location inside a PA, VA, or MAA during a periodic inventory (1-hour notification)

e. enhanced weapons are discovered missing from their authorized storage location that is located outside of a PA, VA, and MAA during a periodic inventory (e.g., a licensee's or certificate holder's firing range) (4-hour notification)

2.8 Enhanced Weapons—Adverse ATF Findings To Be Reported within 24 Hours

The regulations in 10 CFR 73.71(h) require each licensee or certificate holder subject to the provisions of 10 CFR 73.18 who possesses enhanced weapons to notify the NRC Headquarters Operations Center as soon as possible but not later than 24 hours after the receipt of an adverse inspection or enforcement finding or other adverse notice from ATF regarding the licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons. This regulation applies to the classes of facilities, radioactive material, and other property designated by the Commission in 10 CFR 73.18(c).

This requirement is intended to alert the NRC to action by ATF involving an adverse inspection or enforcement action affecting an NRC licensee or certificate holder possessing enhanced weapons. This notification is intended to permit the NRC to respond to potential inquires related to the ATF action.

2.8.1 Notification Requirements

10 CFR 73.71(h) Enhanced weapons – adverse ATF findings. (1) Each licensee or certificate holder possessing enhanced weapons in accordance with § 73.18 shall —

(i) Notify the NRC Headquarters Operations Center as soon as possible but not later than 24 hours after receipt of an adverse inspection or enforcement finding or other adverse notice from the ATF regarding the licensee's or certificate holder's possession, receipt, transfer, or storage of enhanced weapons; and

(ii) Notify the NRC Headquarters Operations Center as soon as possible but not later than 24 hours after receipt of an adverse inspection or enforcement finding or other adverse notice from the ATF regarding the licensee's or certificate holder's ATF issued federal firearms license.

(2) Notifications must be made according to paragraph (j) of this section, as applicable.

2.8.2 Examples of Reportable Events

The NRC staff considers that the following finding and notices as examples of the types of events that require notification under 10 CFR 73.71(h).

a. receipt of a notice of violation from ATF following an inspection of the licensee's or certificate holder's facility

b. receipt of an inspection finding from ATF of less than adequate (but not noncompliant) recordkeeping regarding the receipt or transfer of enhanced weapons

c. notification that ATF will issue a press release of an adverse inspection or enforcement finding regarding a specific licensee's or certificate holder's possession, receipt, or transfer of enhanced weapons

3. Telephonic Reporting Process

The regulations in 10 CFR 73.71(j) require licensees and certificate holders to make a telephonic notification to the NRC Headquarters Operations Center of certain security events specified in 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), and (h). Licensees and certificate holders should make these telephonic reports via any method that will ensure that a report is received by the NRC Headquarters Operations Center or other specified government officials within the timeliness requirements. Methods of communication include, but are not limited to, standard land phone circuits (wire or fiber optic), cellular phone circuits, satellite phone circuits, or licensee proprietary phone circuits (e.g., load dispatcher phone circuits).

Licensees and certificate holders should contact the NRC Headquarters Operations Center using the commercial telephone numbers that are specified in Table 1, "Mailing Addresses, Telephone Numbers, and E-mail Addresses," of Appendix A to Part 73 (Ref. 1).

Licensees and certificate holders are not required to make separate notifications for security events that also result in their declaration of an emergency. In such circumstances, licensees or certificate holders should make the necessary emergency notifications required by the various regulations applicable to their specific facility or activity. When making such a notification, the licensee or certificate holder should indicate to the NRC that the notification is also to report a security event under a specific paragraph of 10 CFR 73.71.

3.1 Telephonic Reporting Process Requirements

(j) Notification process. (1) Each licensee and certificate holder shall make the telephonic notifications required by paragraphs (a), (b), (c), (d), (e), (f), (g), and (h) of this section to the NRC Headquarters Operations Center via any available telephone system. Commercial telephone numbers for the NRC Headquarters Operations Center are specified in Table 1 of Appendix A of this part.

(2) Licensees and certificate holders shall make required telephonic notifications via any method that will ensure that a report is received by the NRC Headquarters Operations Center or other specified government officials within the timeliness requirements of paragraphs (a), (b), (c), (d), (e), (f), (g), and (h) of this section, as applicable.

(3) Notifications required by this section that contain Safeguards Information may be made to the NRC Headquarters Operations Center without using secure communications systems under the exception of § 73.22(f)(3) of this part for emergency or extraordinary conditions.

(4)(i) Notifications required by this section that contain classified national security information and/or restricted data must be made to the NRC Headquarters Operations Center using secure communications systems appropriate to the classification level of the message. Licensees and certificate holders making classified telephonic notifications shall contact the NRC Headquarters Operations Center at the commercial numbers specified in Table 1 of Appendix A to this part and request a transfer to a secure telephone, as specified in paragraph III of Appendix A to this part.

(ii) If the licensee's or certificate holder's secure communications capability is unavailable (e.g., due to the nature of the security event), the licensee or certificate holder shall provide as much information to the NRC as is required by this section, without revealing or discussing any classified information, in order to meet the timeliness requirements of this section. The licensee or certificate holder shall also indicate to the NRC that its secure communications capability is unavailable.

(iii) Licensees and certificate holders using a non-secure communications capability may be directed by the NRC Emergency Response management to provide classified information to the NRC over the non-secure system, due to the significance of the ongoing security event. In such circumstances, the licensee or certificate holder shall document this direction and any information provided to the NRC over a non-secure communications capability in the follow-up written report required in accordance with paragraph (m) of this section.

(5)(i) For events reported under paragraph (a) of this section, the NRC may request that the licensee or certificate holder maintain an open and continuous communication channel with the NRC Headquarters Operations Center as soon as possible. Licensees and certificate holders shall establish the requested continuous communication channel once the licensee or certificate holder has completed other required notifications under this section, § 50.72 of this chapter, Appendix E of part 50 of this chapter, or § 70.50 of this chapter; or completed any immediate actions required to stabilize the plant, to place the plant in a safe condition, to implement defensive measures, or to request assistance from the LLEA.

(ii) When established, the continuous communications channel shall be staffed by a knowledgeable individual in the licensee's security, operations, or emergency response organizations from a location deemed appropriate by the licensee.

(iii) The continuous communications channel may be established via any available telephone system.

(6)(i) For events reported under paragraph (b) of this section, the NRC may request that the licensee or certificate holder maintain an open and continuous communication channel with the NRC Headquarters Operations Center as soon as possible. Licensees and certificate holders shall establish the requested continuous communication channel once the licensee or certificate holder has completed other required notifications under this section, § 50.72 of this chapter, Appendix E of part 50 of this chapter, or § 70.50 of this chapter; or requested assistance from the LLEA.

(ii) When established, the continuous communications channel shall be staffed by a knowledgeable individual in the communication center monitoring the shipment.

(iii) The continuous communications channel may be established via any available telephone system.

(7) For events reported under paragraphs (c), (d), (e), (f), (g), and (h) of this section, the NRC may request that the licensee or certificate holder maintain an open and continuous communication channel with the NRC Headquarters Operations Center.

(8) Licensees and certificate holders desiring to retract a previous security event report that has been determined to be invalid shall telephonically notify the NRC Headquarters Operations Center in accordance with paragraph (j) of this section and shall indicate the report being retracted and basis for the retraction.

10 CFR 73.71(n) Declaration of emergencies. Notifications made to the NRC for the declaration of an emergency class shall be performed in accordance with §§ 50.72, 70.50, 72.75, and 76.120 of this chapter, as applicable.

10 CFR 73.71(o) Elimination of duplication. Separate notifications and reports are not required for events that are also reportable in accordance with §§ 50.72, 50.73, 70.50, 72.75, and 76.120 of this chapter. However, these notifications should also indicate the applicable § 73.71 reporting criteria.

3.2 Content of 15-Minute Reports

Licensees or certificate holders should include, at a minimum, the following information in their report:

a. name and location of the facility or activity

b. caller's name and callback number

c. authentication code (only for facility events reported under 10 CFR 73.71(a))

d. emergency classification (only if declared)

e. description of the imminent or hostile act (e.g., armed assault, vehicle bomb, or credible bomb threat)

f. current event status (e.g., imminent, in progress, neutralized, or unknown)

3.3 Content of 1-Hour, 4-Hour, and 8-Hour Reports

Licensees or certificate holders should include, at a minimum, the following information in their report:

a. name and location of the facility or activity

b. caller's name and callback number

c. emergency classification (only if declared)

d. event description including the following information:

(1) who was involved

(2) what occurred during the event

(3) time the event was discovered and when initiated and completed, if known

(4) location of the event (this may include plant or security systems or geographic locations affected)

(5) why the event occurred, if known

(6) how the event occurred

e. current event status (e.g., ongoing, neutralized, anticipated, unknown)

f. security response and corrective actions taken

g. offsite assistance (e.g., requested or not requested, arrived, status)

h. media interest, if any, including licensee or certificate holder issued press releases

3.4 Content of 4-Hour Suspicious Activity Reports

Licensees or certificate holders should include, at a minimum, the following information in their report:

a. name and location of the facility or activity

b. caller's name and callback number

c. event description

(1) who was involved

(2) what occurred during the event

(3) when the event was discovered and when initiated and completed, if known

(4) location of the event (this may include plant or security systems or geographic locations effected)

(5) why the event occurred, if known

(6) how the event occurred

d. source of the information (if a law enforcement agency, provide contact telephone number)

3.5 Reports Containing Safeguards Information

Licensees and certificate holders making notifications required by 10 CFR 73.71 that contain Safeguards Information may notify the NRC Headquarters Operations Center without using a secure communications system (to communicate the Safeguards Information). The NRC's regulations in 10 CFR 73.22(f)(3) (Ref. 1) provide an exception to the requirement to communicate Safeguards Information using a secure communications system under emergency or extraordinary conditions.

All licensee and certificate holder reports of security events made to the NRC under the provisions of 10 CFR 73.71 are considered emergency or extraordinary conditions (i.e., the use of a secure communications system to communicate is not required under the exception of 10 CFR 73.22(f)(3)). However, if the licensee or certificate holder has ready access to a secure communications system within the time limits of 10 CFR 73.71, then the licensee or certificate holder should use such a secure communications system to communicate information to the NRC and protect the Safeguards Information contained in the report from unintentional or inadvertent disclosure. Additionally, licensees and certificate holders should apply this exception to actual events only. As such, it should not be applied to simulated events communicated as part of a drill or exercise, or to routine events, e.g., the retraction of a previous security report as invalid.

3.6 Reports Containing Classified Information

Licensees and certificate holders making notifications required by 10 CFR 73.71 that contain classified National Security Information (NSI) or Restricted Data (RD) should notify the NRC Headquarters Operations Center using secure communications systems appropriate to the classification

level of the communication. Licensees and certificate holders making classified notifications should contact the NRC Headquarters Operations Center at the commercial telephone numbers specified in Table 1 of Appendix A to Part 73 and request a transfer to a secure telephone as specified in paragraph III of Appendix A.

If the licensee's or certificate holder's secure communications capability is unavailable (e.g., because of the nature of the security event), the licensee or certificate holder should provide as much information to the NRC as is required by 10 CFR 73.71, without revealing or discussing any classified information, to meet the time limits of 10 CFR 73.71. The licensee or certificate holder should also indicate to the NRC at the beginning of the notifications that its secure communications capability is unavailable, in order to prevent the inadvertent disclosure of classified information.

If the nature of the security event warrants, NRC Emergency Response Management may direct the licensee or certificate holder to use any available nonsecure communications method to immediately communicate classified information to the NRC (regarding security event notifications required by 10 CFR 73.71). If so directed, the licensee or certificate holder should provide the classified information to the NRC over the best available nonsecure system. For example, the NRC staff considers using an available nonsecure land line as preferable to using an available nonsecure cellular or satellite system. Additionally, licensees and certificate holders should apply this exception to actual events only. As such, it should not be applied to simulated events communicated as part of a drill or exercise, or to routine events, e.g., the retraction of a previous security report as invalid.

In the written followup report for the event (required by 10 CFR 73.71(m)), the licensee or certificate holder should document this direction from the NRC, the reason for the unavailability of a secure communications capability, and the specific classified information communicated to or from the NRC over a nonsecure communications capability (see also Regulatory Position 4 of this guide). The written followup report should be appropriately classified by the licensee or certificate holder. The NRC will use the information in the written followup report to assess the impact of the possible compromise of the specific classified information communicated by the licensee, certificate holder, or the NRC over a nonsecure system, as required by Executive Order 13526, "Classified National Security Information." (Ref. 10).

3.7 Continuous Communications Channel Requirements

The NRC may request licensees and certificate holders reporting security events under 10 CFR 73.71(a), (b), (c), (d), (e), (f), (g), or (h) to maintain an open and continuous communications channel with the NRC Headquarters Operations Center. When so requested by the NRC, licensees and certificate holders should establish a continuous communications channel using an appropriate individual who is able to continuously interact with the NRC from a location the licensee or certificate holder deems appropriate. Licensees and certificate holders should consider using as an "appropriate individual" persons from their security, operations, or emergency response organization who are both knowledgeable in their security programs and requirements and received training as a communicator.

3.8 Reporting Significant Additional Information

Licensees and certificate holders who discover significant supplemental information after the initial telephonic notification to the NRC Headquarters Operations Center (in accordance with 10 CFR 73.71(j)), or after the submission of the written followup report (in accordance with 10 CFR 73.71(m)), should report this significant supplemental information by telephone to the NRC Headquarters Operations Center in accordance with 10 CFR 73.71(j).

3.9 Emergency Declarations and Duplicate Reports

Licensees and certificate holders reporting security events, under 10 CFR 73.71, that also involve the declaration of an Emergency Classification (e.g., Alert, Site Area Emergency, or General Emergency), in accordance with the licensee's or certificate holder's NRC-approved Emergency Response plan, should follow the appropriate regulations regarding the declaration of an emergency (i.e., emergency declarations have primacy over security event reports). Consequently, to reduce unnecessary burden and duplication, licensees and certificate holders may make a single report of security events that are subject to both emergency response and security event notification regulations. Licensees and certificate holders should indicate in their telephonic report all of the applicable reporting requirements for the event. However, this provision does not obviate a licensee's or certificate holder's responsibility to report significant additional information (see Regulatory Position 3.8 above).

3.10 Retraction of Previous Telephonic Security Event Reports

Licensees and certificate holders desiring to retract a previous telephonic security event report that they have determined (through their analysis or investigation) to be invalid should notify the NRC Headquarters Operations Center by telephone, in accordance with 10 CFR 73.71(j), and should indicate the report being retracted and the basis for the retraction. Such retractions should not be made over a non-secure communications system (see Regulatory Positions 3.5 and 3.6 above).

Security events may be retracted at any time following the initial report to the NRC. However, see additional direction in Regulatory Position 4.2 below on documenting this retraction, if a 60-day written followup report has already been submitted.

4. Written Followup Reports

The regulations in 10 CFR 73.71(m) require licensees and certificate holders who have made a telephonic report to the NRC Headquarters Operations Center of security events specified in 10 CFR 73.71(a), (b), (c), (d), (e), (f), and (g) to submit a written followup report to the NRC within 60 days of the telephonic report. Licensees and certificate holders should submit the written followup report in accordance with the provisions of 10 CFR 73.4 (Ref. 1).

The NRC does not require licensees and certificate holders who have made a telephonic report to the NRC Headquarters Operations Center of security events specified in 10 CFR 73.71(h) to submit a written followup report for these events. Additionally, the NRC does not require licensees and certificate holders who have made a telephonic report to the NRC Headquarters Operations Center of security events specified in 10 CFR 73.71(e) involving suspicious-activity or law-enforcement events to submit written followup reports for these events. Events recorded in the safeguards event log under 10 CFR 73.71(k) also do not require a written followup report.

Licensees' and certificate holders' written followup reports should contain sufficient details and information to allow a knowledgeable individual to understand what occurred during the event, whether any personnel errors or equipment malfunctions occurred, whether any compensated or uncompensated vulnerabilities or degradations existed, and, if appropriate, whether any corrective actions to prevent recurrence were taken by the licensee or certificate holder. Licensees and certificate holders should retain a copy of any written reports submitted to the NRC for at least 3 years or until the termination of the license or certificate of compliance, whichever is longer.

Licensees and certificate holders who submit written reports to the NRC containing Safeguards Information should create, store, mark, label, handle, and transmit these written reports in accordance

with the applicable information security requirements of 10 CFR 73.21 and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements" (Ref. 1) Licensees and certificate holders should perform a safeguards designation of such reports in accordance with the NRC's Designation Guide for Safeguards Information (DG-SGI-1). Written reports should be portion marked to indicate the designation level of the report's information.

Licensees and certificate holders who submit written reports to the NRC containing classified NSI or RD should create, store, mark, label, handle, and transmit these reports in accordance with the applicable information security requirements of 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data" (Ref. 11). Licensees and certificate holders should perform a derivative classification of such reports in accordance with the classification guide(s) applicable to their facility or activity. Written reports should be portion marked to indicate the classification level of the report's information. If the follow-up report requires an original classification determination, then the licensee or certificate holder should make a provisional classification decision; mark, handle, store, and transmit the document according to that provisional decision; and forward the document to the NRC for an original classification determination.

4.1 Written Followup Report Requirements

10 CFR 73.71(m) Written reports. (1) Each licensee or certificate holder making an initial telephonic notification under paragraphs (a), (b), (c), (d), (e), (f), and (g) of this section shall also submit a written follow-up report to the NRC within 60 days of the telephonic notification, in accordance with § 73.4.

(2) Licenses and certificate holders are not required to submit a written report following a telephonic notification made under paragraphs (g) and (h) of this section.

(3) Licenses and certificate holders are not required to submit a written report following a telephonic notification made under paragraph (j) of this section involving suspicious event or law enforcement interaction specified in paragraph II(a), II(c), or II(d) of Appendix G.

(4) Each licensee and certificate holder shall submit to the Commission written reports that are of a quality that will permit legible reproduction and processing.

(5) Licensees subject to § 50.73 of this chapter shall prepare the written report on NRC Form 366.

(6) Licensees and certificate holders not subject to § 50.73 of this chapter shall prepare the written report in letter format.

(7) In addition to the addressees specified in § 73.4, the licensee or certificate holder shall also provide one copy of the written report addressed to the Director, Office of Nuclear Security and Incident Response (NSIR). The copy of a classified written report to the Director, NSIR, shall be provided to the NRC headquarters' classified mailing address specified in Table 2 of Appendix A to this part or in accordance with paragraph IV of Appendix A to this part.

(8) The report must include sufficient information for NRC analysis and evaluation.

(9) Significant supplemental information that becomes available after the initial telephonic notification to the NRC Headquarters Operations Center or after the submission of the written report must be telephonically reported to the NRC Headquarters Operations Center under paragraph (j) of this section and also submitted in a revised written report (with the revisions indicated) as required under paragraph (m) of this section.

(10) Errors discovered in a written report must be corrected in a revised written report with the revisions indicated.

(11) The revised written report must replace the previous written report; the update must be complete and not be limited to only supplementary or revised information.

(12) Each licensee and certificate holder shall maintain a copy of the written report of an event submitted under this section as a record for a period of three years from the date of the report or until termination of the license or the certificate of compliance.

(13)(i) If the licensee or certificate holder subsequently retracts a telephonic notification made under this section as invalid and has not yet submitted a written report required by paragraph (m) of this section, then submission of a written report is not required.

(ii) If the licensee or certificate holder subsequently retracts a telephonic notification made under this section as invalid, after it has submitted a written report required by paragraph (m) of this section, then the licensee or certificate holder shall submit a revised written report in accordance with paragraph (m) of this section.

(14) Each written report containing Safeguards Information or classified information must be created, stored, marked, labeled, handled, and transmitted to the NRC in accordance with the requirements of §§ 73.21 and 73.22 of this part or with Part 95 of this chapter, as applicable.

4.2 Retraction of Previous Written Followup Reports

If a licensee or certificate holder subsequently retracts a telephonic report made under 10 CFR 73.71(j) and has not yet submitted the followup written report required by 10 CFR 73.71(k), the NRC does not require the licensee or certificate holder to submit a written followup written report. However, if the licensee or certificate holder has already submitted a followup written report to the NRC before it retracts the telephonic report, the licensee or certificate holder should then submit a revised written report to the NRC indicating the initial event has been retracted and the basis for that conclusion. This supplemental written followup report is necessary because without the supplemental report (retracting the notification), the only NRC official agency record on the notification would be the initial written followup report.

4.3 Significant Additional Information and Correction of Errors

Licensees and certificate holders who discover significant supplemental information after the submission of a written followup report to the NRC should submit a revised written report, in accordance with the same processes as used to submit the initial written report. Licensees and certificate holders who discover errors in a written report previously submitted to the NRC should submit a revised written report, in accordance with the same processes as used to submit the initial written report. A revised written report should replace the previous written report (i.e., the updated report should be complete and should not be limited to only the supplementary or revised information). The revised report should indicate the revisions with revision bars to assist the reader.

4.4 Use of NRC Form 366

Reactor licensees should submit any written followup reports to the NRC required by 10 CFR 73.71 using NRC Form 366, "Licensee Event Report (LER)." All other licensees and certificate holders should submit any written followup reports to the NRC using a standard letter format.

4.5 Content of Written Followup Reports

Licensees and certificate holders preparing written followup reports should include sufficient information for the NRC to analyze the event. The NRC staff recommends that followup reports contain, at a minimum, the following information, as applicable:

a. date and time of the event, including chronological time line, if applicable; date and time of notifications to the NRC, State officials, or LLEA

b. locations of the actual or threatened event in a PA, VA, MAA, CAA, OCA, or other area

c. for power reactor licensees, the reactor's operating mode (e.g., shut down, operating, construction, decommissioning)

d. safety, security, or emergency response systems directly or indirectly affected, damaged, or threatened

e. type of onsite security force (i.e., proprietary or contract)

f. number and type of personnel involved or contacted, such as contractors; security personnel; visitors; plant staff; perpetrators or attackers; NRC personnel; local, State, or Federal responders; and other personnel (please specify)

g. method of discovery of the incident, event, or information, such as routine patrol or inspection, test, maintenance, alarm annunciation, chance, communicated threat, unusual circumstances (include details)

h. immediate actions taken in response to the event and any compensatory measures established

i. description of media interest and press releases

j. indications or records of previous similar events

k. procedural or human errors or equipment failures, as applicable

l. cause of the event or the licensee's or certificate holder's analysis of the event (including a brief summary in the report and references to any ongoing or completed detailed investigations, assessments, analyses, or evaluations)

m. corrective actions taken or planned, including dates of completion

n. name and phone number of a licensee's or certificate holder's point of contact

o. for reported uncompensated failures, degradations, or discovered vulnerabilities of security systems, licensees and certificate holders should also provide the following information, in addition to items a. through n. above:

    (1) description of failed, degraded, or vulnerable equipment or systems (e.g., manufacturer and model number, procedure number)

    (2) status of the equipment or system before the event (e.g., operating, being maintained secure, being implemented) and, as applicable, the compensatory measures put in place

    (3) description of the failure, degradation, or vulnerability identified (specify)

    (4) unusual conditions that may have contributed to the failures, degradations, or discovered vulnerabilities of the security system (e.g., environmental conditions, plant outage)

    (5) apparent cause of component or system failure, degradation, or vulnerability

    (6) secondary functions affected (for multiple-function components)

(7) effect on plant safety or emergency response capabilities

p. for threat-related incidents, licensees and certificate holders should also provide the following information, in addition to items a. through n. above (maintaining the integrity of any threat material, as it may become evidence in a law enforcement investigation):

(1) type of threat (e.g., bomb threat, extortion, tampering, interruption of normal operations, attempted diversion of SSNM, theft, armed assault)

(2) detailed description of perpetrators or attackers (e.g., number, armament, method of threat, appearance, personal characteristics)

(3) method or means of the threat's communication (e.g., letter, telephone, e-mail)

(4) text or transcript of the threat

(5) clear photocopy of threat letter and accompanying envelope, if applicable

5. Security Events To Be Recorded within 24 Hours

The regulations in 10 CFR 73.71(k) require licensees and certificate holders subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.37, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.54, 10 CFR 73.55, 10 CFR 73.60, and 10 CFR 73.67 to maintain a safeguards event log. The NRC requires licensees and certificate holders to record security events specified in paragraph IV of Appendix G in a safeguards event log within 24 hours of the discovery of the event. This regulation applies to Category I SSNM facilities, hot-cell facilities, ISFSIs, MRSs, GROAs, power reactor facilities, research reactor facilities, test reactor facilities, and Category II and III SNM facilities. This also includes the transportation of Category I quantities of SSNM, SNF, HLW, and Category II and III quantities of SNM.

The NRC requires licensees and certificate holders to retain the safeguards event log as an official record for a period of 3 years after the last entry is made in each log or until the termination of their respective license or certificate of compliance, whichever is greater. The NRC does not require licensees and certificate holders to record (i.e. duplicate), in a safeguards event log, any security events that they reported to the NRC under the telephonic notification provisions of 10 CFR 73.71, including the events listed under paragraphs I, II, and III of Appendix G.

In general, licensees and certificate holders should record events in the safeguards event log that are less significant than those required to be reported telephonically to the NRC. However, further analysis of these recordable events may result in the identification of system or performance vulnerabilities, deficiencies, or trends that may require corrective action and may be generic in nature. The NRC expects all recordable security events to be recorded in the safeguards event log, regardless of who identifies the issue (i.e., licensee or certificate holder staff or contractors, NRC or State inspectors, or independent auditors).

Events recorded in the safeguards event log include failures, degradations, or discovered vulnerabilities that could have allowed unauthorized or undetected access to any area (e.g., OCA, PA, VA, MAA, or CAA) if compensatory measures were not in place or implemented at the time of discovery. These events also include failures, degradations, or discovered vulnerabilities that could have allowed unauthorized or undetected access to a vehicle transporting fresh nuclear fuel, SNF, or HLW; or to the nuclear fuel, SNF, or HLW regulated by the NRC. These events may also include a compensated vulnerability, failure, or degradation of security systems that, except for the compensatory actions, could

have allowed unauthorized access or contraband into a PA, VA, MAA, or CAA, or explosives or incendiaries beyond a vehicle barrier. These events may include a compensated vulnerability, failure, or degradation of security systems that, except for the compensatory actions, could have allowed unauthorized access or contraband into a vehicle transporting fresh nuclear fuel, SNF, or HLW; or to the nuclear fuel, SNF, or HLW itself. Finally, these events may also include a threatened, committed, or attempted act that would degrade the licensee's or certificate holder's protective strategy.

Compensatory measures may include backup equipment, additional security personnel, or other measures taken to ensure that the effectiveness of the physical protection program and systems or subsystems is not reduced by the failure or other contingency affecting the operation of security equipment or structures. To determine whether an event should be recorded or reported, the compensatory measures need to be implemented before the event or within the time limits described in the licensee's or certificate holder's NRC-approved security plans. Compensatory measures should also provide a level of protection equivalent to the system or systems that were degraded or that protect against the identified vulnerability.

Events recorded in the safeguards event log also include those that decreased or degraded the effectiveness of the licensee's or certificate holder's cyber security program or allowed unauthorized or undetected access to any systems, networks, or equipment that falls within the scope of 10 CFR 73.54. Decreases in the effectiveness of the cyber security program include any other threatened, attempted, or committed act not previously specified in Appendix G that has resulted, or has the potential for a decrease in the effectiveness of the cyber security program in a licensee's or certificate holder's NRC-approved cyber security plan.

The significance of a system defect or vulnerability are key factors in determining whether an event is reportable or recordable. Even compensatory measures implemented promptly after discovery of the defect or vulnerability, which did not provide protection for the period of time that the defect or vulnerability existed, would be reportable. Therefore, any failure, degradation, or discovered vulnerability that is known to have existed for a significant period of time and was not discovered in the course of patrols, surveillance, operational tests, or other means, should be considered for reporting within 1 hour (see Regulatory Position 2.3 of this guide).

Recordable events related to failures and degradations may include mechanical or electrical problems, procedural-related failures, or failures regarding personnel performance. Recordable events typically affect single elements of physical security systems or an individual, critical, single-failure program element that would not permit unauthorized access. However, for example, a properly compensated degraded barrier may involve multiple elements. Other failures, degradations, or discovered vulnerabilities of security systems not related to unescorted or unauthorized access should be recorded as described in paragraph IV of Appendix G.

5.1 Safeguards Event Log Record Requirements

10 CFR 73.71(k) Safeguards event log. Each licensee or certificate holder subject to the provisions of §§ 73.20, 73.25, 73.26, 73.37, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.60, or 73.67 shall maintain a safeguards event log.

(1) The licensee or certificate holder shall record the facility-based or transportation-based events described in paragraph IV of Appendix G of this part within 24 hours of discovery in the safeguards event log.

(2) The licensee or certificate holder shall retain the safeguards event log as a record for three years after the last entry is made in each log or until the termination of the license or certificate of compliance.

Appendix G, Paragraph IV. Events to be recorded in the safeguards event log within 24 hours of discovery.

(a) Compensated security events. Any failure, degradation, or discovered vulnerability in a safeguards system, had compensatory measures not been established, that could have—

(1) Allowed unauthorized or undetected access of—

(i) Explosives or incendiaries beyond a vehicle barrier;

(ii) Personnel or contraband into a PA, VA, MAA, or CAA; or

(iii) Personnel or contraband into a vehicle transporting special nuclear material, spent nuclear fuel, or high-level radioactive waste; or to the special nuclear material, spent nuclear fuel, or high-level radioactive waste itself.

(2) Degrade the effectiveness of the licensee's or certificate holder's cyber security program or allow unauthorized or undetected access to any systems, networks, or equipment that fall within the scope of § 73.54 of this part. Decreases in the effectiveness of the cyber security program include any other threatened, attempted, or committed act not previously defined in this appendix that has resulted in or has the potential for decreasing the effectiveness of the cyber security program in a licensee's or certificate holder's NRC-approved cyber security plan.

(b) Ammunition events.

(1) A discovery that ammunition that is authorized by the licensee's security plan has been lost or uncontrolled inside a PA, VA, MAA, or CAA.

(2) A discovery that unauthorized ammunition is inside a PA, VA, MAA, or CAA.

(3)(i) Uncontrolled authorized ammunition means ammunition authorized by the licensee's or certificate holder's security plan or contingency response plan that is not in the possession of authorized personnel or is not in an authorized ammunition storage location.

(ii) Uncontrolled unauthorized ammunition means ammunition that is not authorized by the licensee's or certificate holder's security plan or contingency response plan.

(iii) Ammunition in the possession of law-enforcement personnel performing official duties inside a PA, VA, MAA, or CAA is considered controlled and authorized.

(4) The discovery of lost or uncontrolled authorized or unauthorized ammunition under circumstances that indicate the potential for malevolent intent shall be reported under paragraph I(f) of this appendix.

(c) Loss of control or protection of classified information. A discovery that a loss of control over, or protection of, classified material containing National Security Information or Restricted Data has occurred, provided –

(1) there does not appear to be evidence of theft or compromise of the material, and

(2) the material is recovered or secured within one hour of the loss of control or protection.

(d) Loss of control or protection of Safeguards Information. A discovery that a loss of control over, or protection of, classified material containing Safeguards Information has occurred, provided –

(1) there does not appear to be evidence of theft or compromise of the material, and

(2) the material is recovered or secured within one hour of the loss of control or protection; or

(3) the material would not have allowed unauthorized or undetected access to facility or transport contingency response procedures or strategies.

(e) Decreases in the effectiveness of the physical security program or the cyber security program. Any other threatened, attempted, or committed act not previously defined in this appendix that has resulted in or has the potential for decreasing the effectiveness of the licensee's or certificate holder's physical security program or cyber security program below that committed to in a licensee's or certificate holder's NRC-approved physical security plan or cyber security plan.

(f) Non duplication. Events reported under paragraphs I, II, or III of this appendix are not required to be recorded under the safeguards event log.

5.2 Content of the Safeguards Event Log

Licensees and certificate holders should record the following information, as a minimum and as applicable, in the safeguards event log for recordable security events:

a. date and time of the event or condition

b. brief (one-line) description of the event

c. brief (one-line) description of compensatory measures implemented or corrective actions taken

d. area or security element affected (e.g., PA, VA, OCA, perimeter alarm system, response capability, vehicle barriers, transport vehicle, communications)

e. method of detection (e.g., alarm, patrol, test, informants, plant staff observations)

f. reference to more detail when applicable (e.g., Incident Report 09-1234, Surveillance Test 04-2348, plant condition report number)

5.3 Example of Facility Events To Be Recorded in the Safeguards Event Log

The NRC staff considers that the following facility-security events as examples of the types of events that require recording under 10 CFR 73.71(k) and paragraph IV of Appendix G.

The following are examples of events involving failures, degradation, or discovered vulnerabilities in a security system that could have allowed unauthorized or undetected access to a PA, VA, MAA, or CAA, had compensatory measures not been established:

a. properly compensated security computer or card reader failures

b. properly compensated loss of the ability to detect intrusion (1) at the protected area perimeter when the loss involves several zones, or (2) within a single intrusion detection zone

c. failure of search equipment for a short period (e.g., less than 1 hour), which could have allowed unsearched individuals or packages to enter controlled areas

d. an individual requiring escort who becomes separated from his or her escort for a short period of time (e.g., less than 10 minutes) but no unauthorized areas were entered

e. an individual who is incorrectly authorized access to areas not authorized but does not or cannot enter those areas and would have been granted access, if necessary

f. tailgating through a security barrier into an area when the individual is authorized or could have been authorized

g. an individual who is incorrectly (i.e., through an error not amounting to falsification) authorized unescorted access to a controlled area but was not actually granted access through the issuance of control media (e.g., badge, key, key card)

h. failure to adequately compensate for an event or identified failure, degradation, or vulnerability that would **not** have allowed undetected or unauthorized access or that has existed for only a very

short period of time (e.g., posting a compensatory officer in 12 minutes instead of the 10 minutes specified under the NRC-approved security plan)

i. failures, degradations, or discovered vulnerabilities that, had compensatory measures not been implemented, might have allowed explosives or incendiaries beyond a vehicle barrier or personnel or contraband into a PA, VA, MAA, or CAA

j. threatened, attempted, or confirmed acts, not previously defined in Appendix G, that have resulted in or have the potential for a decrease in the effectiveness of the licensee's or certificate holder's physical protection system

The following are examples of ammunition events that should be recorded in the licensee's or certificate holder's safeguards event log:

k. The licensee or certificate holder discovers that authorized ammunition has been lost or is uncontrolled within a PA, VA, MAA, or CAA. Uncontrolled authorized ammunition means ammunition authorized by the licensee's or certificate holder's security plan or contingency response plan that is not in the possession of authorized personnel or is not in an authorized ammunition storage location.

l. The licensee or certificate holder discovers that unauthorized ammunition is within a PA, VA, MAA, or CAA. Unauthorized ammunition means ammunition that is not authorized by the licensee's or certificate holder's security plan or contingency response plan. Ammunition in the possession of law-enforcement personnel performing official duties inside a licensee's or certificate holder's PA, VA, MAA, or CAA is considered controlled and authorized.

The following are examples of cyber security events that should be recorded in the licensee's or certificate holder's safeguards event log:

m. accidental deletion of security logs

n. properly compensated CDA failures

o. an individual who is incorrectly authorized access to a CDA but does not or cannot access that CDA and would have been granted access, if necessary

The following are examples of other threatened, attempted, or committed acts not previously defined in Appendix G that should be recorded in the licensee's or certificate holder's safeguards event log and that reduced or could have reduced the effectiveness of the physical protection program or cyber security program below that described in the licensee's or certificate holder's NRC-approved physical security plans or cyber security plans:

p. failure or degradation of lighting below security-plan requirements, as long as the entire perimeter intrusion detection system remains operational

q. loss of partial capability of one alarm station (for facilities with two alarm stations) to remotely monitor, assess, or initiate a response to alarms, as long as the same capability remains operable in the other alarm station

r. loss of control or protection over Safeguards Information when there does not appear to be evidence of theft or compromise and the information is recovered within 1 hour

s. loss of control or protection over Safeguards Information that would not have allowed unauthorized or undetected access or significantly affected a contingency response

t. loss of control or protection over classified information when there does not appear to be evidence of theft or compromise and the information is recovered within 1 hour

u. loss of control or protection over Safeguards Information that would not have allowed unauthorized or undetected access or significantly affected a contingency response

v. loss of control of an authorized standard security weapon within a PA, VA, MAA, or CAA that is retrieved within 1 hour of the discovery of its loss

w. theft or loss of standard security weapons from a location outside of the licensee's or certificate holder's PA or CAA, provided the weapon would not affect the implementation of the licensee's or certificate holder's protective strategy

x. access control failures that unlock a door but where alarms are operable, or where an alarm failure occurs with an operable secured door

y. unsubstantiated bomb or extortion threats, meaning a threat for which no specific organization or individual claims responsibility, it is determined to be fictitious, and it is not supported by any evidence other than the threat message itself

z. frequent nuisance alarms caused by mechanical, electrical, or environmental conditions and false alarms that meet or exceed the invalid rates, as specified in the licensee's or certificate holder's NRC-approved physical security plans or procedures

aa. unplanned missed security patrols which resulted in a failure to meet security requirements

bb. termination of personnel whose job duties and responsibilities actively support the licensee's or certificate holder's insider mitigation program

cc. discovery of contraband material outside the PA or inside a designated vehicle barrier or control point that does not constitute a threat or potential threat to the facility

dd. loss of partial capability to monitor, assess, or initiate response to cyber events as long as the same capability remains operable at another manned location

ee. unsubstantiated cyber threats, meaning a threat for which no specific organization or individual claims responsibility, is determined to be fictitious, and is not supported by evidence other than the threat message itself

ff. unplanned missed cyber vulnerability assessments

5.4 Examples of Transportation Events To Be Recorded in the Safeguards Event Log

The NRC staff considers that the following transportation-security events as examples of the types of events that require recording under 10 CFR 73.71(k) and paragraph IV of Appendix G.

The following are examples of failures, degradations, or discovered vulnerabilities in a security system that could have allowed unauthorized or undetected access into a vehicle transporting Category I SSNM, Category II or III SNM, SNF, or HLW; or to the Category I SSNM, Category II or III SNM, SNF, or HLW, had compensatory measures not been established:

a. failures, degradations, or discovered vulnerabilities that, had compensatory measures not been implemented, might have allowed explosives or incendiaries into a vehicle transporting Category I SSNM, Category II or III SNM, SNF, or HLW; or into the Category I SSNM, Category II or III SNM, SNF, or HLW itself

b. loss of intra-convoy communications for SSNM, SNF, or HLW transport when the ability to communicate with the movement control center remains intact

c. unplanned loss of the ability to monitor a transporter's remote position

d. unplanned loss of the ability of the movement control center to monitor a transporter's position

e. unplanned loss of the ability to communicate with the movement control center

f. unplanned (i.e., inadvertent) activation of immobilization or intrusion delay systems

6. Security Events that Are Not Considered Reportable or Recordable

In general, reporting and recording security events should provide relevant, timely, and factual information regarding events, system failures, or vulnerabilities, as well as information that may be of value in assessing the significance of the threat. The NRC staff recognizes that there may be other failures that would not reduce security system effectiveness or would have little or no security significance. The NRC staff has evaluated previous security reports and determined that some were not needed, causing unnecessary burdens on licensees, certificate holders, and the NRC.

Licensees and certificate holders should use the guidance in this regulatory position to determine whether or not an event should be reported or recorded. Licensees and certificate holders should use sound and reasonable judgment when determining whether to record or report an event. The examples provided below represent the types of events that need not be reported and are not intended to be all-inclusive or limiting. Should questions arise regarding whether to report or record an event, the licensee or certificate holder may consider discussing the matter with the appropriate NRC regional or Headquarters staff, if time permits.

6.1 Examples of Events that are Not Required to be Reported

The NRC staff considers the following as examples of the type of security-related events that are not required to be reported under 10 CFR 73.71 and Appendix G:

a. discovery of prohibited items that are found during entrance searches to a facility

b. discovery of prohibited items that are found inside the controlled area of a facility or inside a transport

c. discovery of weapons that are found during entrance searches to a facility, provided the licensee concludes the individual had no malevolent intent

Prohibited items are identified by the licensee or certificate holder as banned from its site by its written procedures or policies. However, prohibited items do not include contraband items that are reportable under Regulatory Position 2.3 above.

Licensees and certificate holders discovering weapons contraband during the entrance search to a facility should evaluate whether malevolent intent is present and the individual legally possesses the

weapon under State law (e.g., the individual has a permit for the weapon). If the licensee or certificate holder suspects malevolent intent is present, the licensee or certificate holder should report the event as a 1-hour event. If the licensee or certificate holder concludes that malevolent intent is not present, the licensee or certificate holder should record the event the Safeguards Event Log. Licensees and certificate holders discovering explosive and incendiary contraband during the entrance search to a facility should report such events as a 1-hour event in all circumstances. NRC staff considers that while an individual may legally possess a weapon outside of an NRC-regulated facility, they typically are never authorized to possess explosives and incendiaries. Therefore, the NRC staff presumes that malevolent intent is present in such cases. Moreover, licensees and certificate holders identifying instances where contraband has actually entered a PA, VA, MAA, or CAA should report such events as 1-hour events (see Regulatory Position 2.3 above).

A licensee's or certificate holder's discovery of prohibited items inside of controlled areas should be evaluated under the licensee's or certificate holder's corrective action program, particularly if the event indicates weaknesses or failures in licensee's or certificate holder's security screening processes (to detect and prevent the entry of the prohibited items).

6.2 Examples of Events that are Not Required to be Recorded in the Safeguards Event Log

The NRC staff considers the following as examples of security-related events that are not required to be recorded under 10 CFR 73.71 and Appendix G:

a. failure, degradation, or compromise of security systems that are preplanned, as long as adequate compensatory measures are in place prior to the failure

b. a non-threatening individual (e.g., a child) attempting but failing to climb a PA fence

c. a fire or explosion, if it can be determined, within 1 hour, that it is not suspicious (e.g., a fire in a trash bin, a lightning strike, or a transformer fault)

d. infrequent nuisance alarms caused by mechanical, electrical, or environmental problems and false alarms that do not exceed the invalid rates, as specified in the licensees' or certificate holders' NRC-approved security plans or their implementing procedures, or that do not degrade system effectiveness

e. suspected tampering with safety equipment that is determined, within 1 hour, not to be tampering

f. cuts or holes made through required barriers by authorized persons for legitimate reasons (e.g., to install a pipe), as long as there is prior approval, coordination, and proper implementation of compensatory measures prior to the work commencing

g. infrequent and nonrecurring failure of search equipment (with compensatory measures properly implemented), if the licensee or certificate holder discovers the failure before entry of the person or vehicle into a controlled area

h. lost, stolen, unaccounted for, or improperly controlled (to include unauthorized, offsite removal) access-control devices, including picture badges, keys, key cards, or access-control computer codes that the licensee or certificate holder determined could not be used to allow unauthorized or undetected access to controlled areas

i. an individual requiring an escort who becomes separated from his or her escort, when the escort recognizes and immediately reestablishes escort duties, provided the licensee or certificate holder determines that the individual did not enter any unauthorized areas

j. an individual requiring an escort who enters a nonsensitive area with limited entry and exit (such as a restroom), while the escort maintains observation of the exit (not intruding into a visitor's personal activities but ensuring supervision of the physical whereabouts of the visitor)

k. individuals photographing facilities from tourist areas, provided no other suspicious activity is involved

l. normal and routine inquiries from students or members of the public regarding facilities or activities

m. normal and routine inquiries from members of the media regarding facilities or activities, recognizing that accredited working journalists may conduct normal and recognizable research on the licensee's or certificate holder's security performance and protection capabilities, and thus, if the inquires are common and understandable, their elicitation of sensitive information should not be reported or recorded

n. routine, prearranged, and unsuspicious aircraft overflight activity

o. responses to information provided to the licensee or certificate holder by the NRC (e.g. threat warnings)

7. Training of Nonsecurity Staff on Reporting and Recording Requirements

The discovery or identification of reportable or recordable events is not limited to members of the licensee's or certificate holder's security organization. All site employees with unescorted access should receive training on this subject to foster awareness and to understand their responsibility to immediately notify site security or management personnel of anomalies, failures, degradations, or vulnerabilities of security systems, or of suspicious activities. Licensees and certificate holders may provide this training during general plant training and periodic refresher training. The NRC staff notes that some licensees or certificate holders have also found it beneficial to include training "tips" or elements of the training program in recurring plant publications, such as newsletters, electronic signs, or other organizational reminders.

In accordance with 10 CFR 73.55(i)(5), the NRC requires power reactor licensees to ensure that their physical protection program includes surveillance, observation, and monitoring, as needed, to satisfy the design requirements of 10 CFR 73.55(b), identify indications of tampering, or otherwise implement the physical protection program. This specific regulatory requirement does not exist for other classes of licensees and certificate holders. However, regardless of regulatory requirements, the NRC staff considers it prudent for all licensees and certificate holders subject to 10 CFR 73.71 to include guidance for all employees regarding the observation or discovery of possible tampering, unusual activities, or unusual equipment conditions, as well as the prompt reporting of such information to facility or security management.

D. IMPLEMENTATION

The purpose of this regulatory position is to provide information to applicants, licensees, and certificate holders regarding the NRC's plans for using this draft regulatory guide. The previous version of this document, RG 5.62, Revision 1, remains in effect until Revision 2 is issued. Supporting guidance document NUREG-1304, "Reporting of Safeguards Events," issued February 1988 (Ref. 12), also remains in effect. NUREG-1304 is based upon a workshop on reporting and recording safeguards events that was held in 1988 following the issuance of RG 5.62, Rev. 1. NUREG-1304 is structured in a question and answer format. However, given the changes to the regulations and this regulatory guidance, the NRC plans to conduct a workshop on these revised safeguards event reporting and recording requirements (approximately 6 to 9 months after the effective date for a final rule and the issuance of RG 5.62, Rev. 2) with the goal of issuing Revision 1 to NUREG-1304.

The NRC has issued this draft guide to encourage public participation in its development. The NRC will consider all public comments received in the development of the final guidance document. Applicants, licensees, or certificate holders may propose an alternative or use a previously established acceptable alternative method for complying with the specified portions of the NRC's regulations. Otherwise, the NRC will use the methods described in this guide in evaluating compliance with the applicable regulations for license and certificate applications, license and certificate amendment applications, and amendment requests.

GLOSSARY

This glossary is intended to aid the reader in implementing this guide to meet the requirements set forth in 10 CFR 73.71 and Appendix G. Definitions for certain security terms are also found in 10 CFR 73.2 (Ref. 1).

Any failure, degradation, or discovered vulnerability—the performance of a system or component or security measure that has been reduced to the degree that it is rendered ineffective for the intended purpose. This includes cessation of proper functioning or performance of equipment, personnel, or procedures that are part of the physical protection program necessary to meet the requirements in 10 CFR Part 73, or a discovered defect in such equipment, personnel, or procedures that degrades a function or performance that could be exploited for the purpose of committing acts described in Appendix G to 10 CFR Part 73.

Attempts—reliable and substantive information exists that an effort to accomplish the threat has taken place. This includes events that have not occurred or have not been completed because they were interrupted or stopped before completion, or would have occurred in more than 2 hours.

Contraband—materials banned from a protected area, vital area, material access area, or controlled access area. Contraband consists of unauthorized firearms, explosives, and incendiary devices that can be used to commit acts of sabotage as specified under Section 236 of the *Atomic Energy Act of 1954*, as amended (AEA) (42 U.S.C. § 2284). Contraband may be carried or concealed on personnel or in packages, materials or vehicles.

Covered weapons—any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semiautomatic assault weapon, machine gun, ammunition for any such weapon, or a large capacity ammunition feeding device, as specified under Section 161A of the AEA (42 U.S.C. § 2201a). Covered weapons include both enhanced weapons and standard weapons.

Credible threat—credible information that has been received from a source determined to be reliable (e.g. law enforcement, government agency), or has been verified to be true. A threat can be verified to be true or considered credible under the following conditions:

(1) physical evidence supporting the threat exists,
(2) information independent from the actual threat message exists that supports the threat, or
(3) a specific known group or organization claims responsibility for the threat,

or when the information is considered so significant that, regardless of the absence of (1), (2), or (3), licensee or certificate holder management has determined that action is required.

Critical digital asset (CDA)—the electronic systems, networks, or equipment that fall within the scope of 10 CFR 73.54 (i.e., within the Level 3 or 4 boundaries described in Regulatory Guide 5.71). Such systems, networks, and equipment have the ability to compromise the facility's safety, security, or emergency response (SSEP) functions.

Dedicated observer—a trained person, not necessarily a member of the security force, who is posted as a temporary compensatory measure for a degraded assessment or detection capability, or both. While performing this function, the person's 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 stations. Regulations permit the use of optical or electronic surveillance devices.

Discovery (time of)—the specific time at which the licensee or certificate holder determines that a verified degradation of a security safeguards measure, contingency situation, or reportable event exists.

Diversion of special nuclear material (SNM) (at any level)—the unauthorized removal or control of SNM from an NRC-licensed or -certified facility or authorized transport vehicle.

Enhanced weapons—any short-barreled shotgun, short-barreled rifle, or machine gun. Enhanced weapons do not include destructive devices as defined in 18 U.S.C. § 921(a). Enhanced weapons do not include standard weapons.

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

High-level radioactive waste (HLW)—(1) the highly radioactive material resulting from the reprocessing of spent nuclear fuel, including liquid waste produced directly in reprocessing and any solid material derived from such liquid waste that contains fission products in sufficient concentrations; and (2) other highly radioactive material that the Commission, consistent with existing law, determines by rule requires permanent isolation.

Hostile action—an act directed against an NRC-licensed or -certified facility, or its personnel, that includes the use of violent force to destroy equipment, take hostages, or intimidate the licensee or certificate holder to achieve an end. This includes an attack by air, land, or water, using weapons, explosives, projectiles, vehicles, or other devices to deliver destructive force. This may also include other acts, not involving the use of overt violent force, such as tampering or covertly causing damage, that satisfy the overall intent of this term.

Interruption of normal operation—a departure from normal operations or conditions that, if accomplished, would result in a challenge to the facility's safety, security, or emergency response systems. This may also include an event that causes a significant redistribution of security, safety, or emergency response resources. This could include intentional tampering with systems or equipment that is normally in a standby mode, but would need to operate if called upon in an abnormal or emergency situation. Section 236 of the AEA (42 U.S.C. § 2284) treats as sabotage the 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, or attempting or conspiring to carry out such an act.

Items relied on for safety—means structures, systems, equipment, components, and activities of personnel [at SNM facilities licensed under 10 CFR Part 70] that are relied on to prevent potential accidents at a facility that could exceed the performance requirements in 10 CFR 70.61 or to mitigate their potential consequences. This does not limit the licensee from identifying additional structures, systems, equipment, components, or activities of personnel (i.e., beyond those in the minimum set necessary for compliance with the performance requirements) as items relied on for safety.

Loss of SNM—a failure to measure or account for SNM by the material control and accounting system approved for the facility, when the material is authorized to be possessed and is not confirmed to be stolen or diverted. This also means an accidental (i.e., unplanned) offsite release or dispersal of SNM, that is known or suspected to be 10 times greater than normal losses, or the discovery of empty or missing SNM containers or fuel elements.

Lost SNM—SNM that is no longer in the possession or control of the authorized licensee or certificate holder.

Malevolent intent—any perceptible actions, statements, observations, or circumstances that are considered by the licensee or certificate holder to indicate rancor, enmity, or a desire to cause harm. Any manifestations of harm or injury focused toward a licensee's or certificate holder's facility, personnel, equipment, or security systems is considered malevolent. This includes events demonstrating ill will, spite, or maliciousness (malice-in-fact).

Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA)—a document detailing the agreement between a licensee or certificate holder and any local law enforcement agencies (at all levels) or emergency service agencies (e.g., firefighting, decontamination, medical) to increase site security, safety, emergency response, or compensatory actions taken in response to onsite events (including, but not limited to, personnel, equipment, and professional assistance).

Nuisance alarm—a detection or monitoring system alarm generated by an identified input to a sensor or monitoring device that does not represent a safeguards threat and is not a result of normal authorized activity. Nuisance alarms may be caused by environmental conditions (e.g., rain, sleet, snow, lightening) or natural objects (e.g., animals or tall grass).

Properly compensated—measures, including backup equipment, additional security personnel, or specific procedures put in place 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, structures, or processes. Preplanned compensatory measures are normally described in NRC-approved security plans and their associated implementing procedures.

Reason to believe—as mentioned in "credible threat," a licensee or certificate holder may have reason to believe information received should be considered reliable when substantive information includes physical evidence supporting the threat, additional information independent of the threat, or the identification of a specific known group, organization, or individual that claims responsibility for the threat.

Reliable source—a source of information considered trustworthy or authentic, or that is consistent in performance or results.

Safeguards—the term "safeguards" historically refers to the two major components of NRC and international programs for the protection of special nuclear material. These programs include material control, material accounting, physical security, and information security functions. The term "security" usually refers to physical or procedural means of protecting this special nuclear material, or the facility possessing such material, from malevolent acts. However, common usage frequently interchanges the terms "security" and "safeguards." The NRC staff notes that under NRC regulations and guidance documents, the term "safeguards" may also have a specific contextual meaning, e.g., "Safeguards Information" in 10 CFR 73.21, 10 CFR 73.22, and 10 CFR 73.23, or "Safeguards Event Log" in 10 CFR 73.71 and Appendix G to Part 73.

Safeguards event log—a written or electronic compilation of entries for security events that meet the criteria described in paragraph III of Appendix G to 10 CFR Part 73,

Safety-related structures, systems, and components (SSCs)—for production and utilization facilities licensed under 10 CFR Part 50 or 10 CFR Part 52, those structures, systems, and components that are relied on to remain functional during and following design-basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in a potential offsite exposure comparable to the guidelines in 10 CFR 50.34(a)(1).

Security event—any incident representing an attempted, threatened, or actual breach of the security system; or a reduction in the physical protection program.

Security-related SSCs—for the purposes of 10 CFR 73.71 and Appendix G to 10 CFR Part 73, those SSCs that the licensee or certificate holder would rely upon to implement the physical protection program, including the physical security plan, training and qualification plan, and safeguards contingency plan.

Security response—the licensee's or certificate holder's implementation of its armed response capabilities; or the request to local law enforcement for armed response or assistance.

Security system—the compilation of all elements in the physical protection program that are necessary to meet 10 CFR Part 73 requirements, including, but not limited to, equipment, procedures, and personnel practices.

Significant physical damage—physical damage that occurs to the licensee's or certificate holder's facility, equipment, transport vehicle or equipment, or reactor fuel, so that it is not able to perform its normal function (this applies to a power reactor, a facility possessing SSNM or its equipment, carrier equipment transporting nuclear or spent nuclear fuel (SNF), or the nuclear fuel or SNF that the facility or carrier possesses).

Spent nuclear fuel or spent fuel (SNF)—the nuclear fuel that has been withdrawn from a production, power, research, or test reactor following irradiation and that has not been chemically separated into its constituent elements by reprocessing. Spent fuel includes the special nuclear material, byproduct material, source material, and other radioactive materials associated with a fuel assembly.

Standard weapon—any handgun, rifle, shotgun, semiautomatic assault weapon, or a large capacity ammunition feeding device. Standard weapons do not include enhanced weapons.

Tampering—altering equipment, for improper purposes or in an improper manner, or intentional unauthorized manipulation of equipment. This may include deliberately damaging, disabling, or altering plant or security equipment specified in security plans. Tampering also refers to the unauthorized operation, manipulation of, or tampering with reactor controls or controls for other facilities belonging to licensees or certificate holders, or with safety-related SSCs or nonsafety-related SSCs.

Unaccounted for SNM—SNM that has not been received at its delivery point 4 hours or more after its estimated, expected arrival.

Unauthorized Person—any person who gains unescorted access to any area for which the person has not been authorized access. This includes otherwise authorized persons gaining access in an

unauthorized manner, such as circumventing established access-control procedures by tailgating behind an authorized person.

Uncompensated—compensatory measures included in security plans or procedures that have either not been implemented, were ineffective, or were implemented incorrectly.

REFERENCES[1]

1. 10 CFR Part 73, "Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

2. 10 CFR 50.72, "Immediate Notification Requirements for Operating Power Reactors," U.S. Nuclear Regulatory Commission, Washington, DC.

3. 10 CFR 70.50, "Reporting Requirements," U.S. Nuclear Regulatory Commission, Washington, DC.

4. 10 CFR 72.75, "Reporting Requirements for Specific Events and Conditions," U.S. Nuclear Regulatory Commission, Washington, DC.

5. 10 CFR 76.120, "Reporting Requirements," U.S. Nuclear Regulatory Commission, Washington, DC.

6. Regulatory Guide 1.214, "Response Strategies for Potential Aircraft Threats," U.S. Nuclear Regulatory Commission, Washington, DC.

7. Regulatory Guide 5.71, "Cyber Security Program for Nuclear Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

8. "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," U.S. Department of Homeland Security, Washington, DC, January 24, 2005.[2] [For Official Use Only]

9. 27 CFR 479.141, "Stolen or Lost Firearms," U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives, Washington, DC.

10. Executive Order 13526 - Classified National Security Information Memorandum of December 29, 2009 - Implementation of the Executive Order "Classified National Security Information" Order of December 29, 2009 – Original Classification Authority, *Federal Register*, Volume 75, Number 2, pp. 705-731, January 5, 2010, Washington, DC.

11. 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," U.S. Nuclear Regulatory Commission, Washington, DC.

12. [Placeholder for revision to] NUREG-1304, Revision 1, "Reporting and Recording Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, (DATE subsequent to issuance of final rule).

---

[1] Publicly available NRC published documents are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. The documents can also be viewed on-line or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail pdr.resource@nrc.gov.

[2] Copies of the non-NRC documents included in these references may be obtained directly from the publishing organization.

13. 76 FR xxxx (10 CFR Part 73), "Proposed Rule—Enhanced Weapons, Firearms Background Checks, and Security Event Notifications," *Federal Register*, Volume 76, Number xxx, pages yyyy-zzzz, Month xx, 2011, Washington, DC.

14. 74 FR 13925 (10 CFR Parts 50, 52, 72, and 73), "Final Rule—Power Reactor Security Requirements," *Federal Register*, Volume 74, Number 58, pages 13925-13993, March 27, 2009, Washington, DC.

15. Regulatory Issue Summary 2009-10, "Communications Between the NRC and Reactor Licensees During Emergencies and Significant Events," U.S. Nuclear Regulatory Commission, Washington, DC, June 19, 2009.

16. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

17. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.

18. 10 CFR Part 60, "Disposal of High-Level Radioactive Waste in Geologic Repositories," U.S. Nuclear Regulatory Commission, Washington, DC.

19. 10 CFR Part 63, "Disposal of High-Level Radioactive Waste in a Geologic Repository at Yucca Mountain, Nevada," U.S. Nuclear Regulatory Commission, Washington, DC

20. 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," U.S. Nuclear Regulatory Commission, Washington, DC.

21. 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste," U.S. Nuclear Regulatory Commission, Washington, DC.

22. 10 CFR Part 76, "Certification of Gaseous Diffusion Plants," U.S. Nuclear Regulatory Commission, Washington, DC.

23. 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," U.S. Nuclear Regulatory Commission, Washington, DC.

SUPERSEDED REFERENCES

1. Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," U.S. Nuclear Regulatory Commission, Washington, DC, July 18, 2005.

2. Regulatory Issue Summary 2006-12, "Endorsement of Nuclear Energy Institute Guidance 'Enhancements to Emergency Preparedness Program for Hostile Action,'" U.S. Nuclear Regulatory Commission, Washington, DC, July 19, 2006.

3. Generic Letter 1991-03, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, March 6, 1991.

4. NUREG-1304, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, February 1988.

APPENDIX A

REPORTING SUSPICIOUS AVIATION-RELATED ACTIVITIES AND COORDINATION WITH THE FEDERAL AVIATION ADMINISTRATION

The purpose of this appendix is to provide further guidance on (1) reporting of suspicious aviation-related activities (required to be reported in 4 hours) that occur within the airspace in proximity to a licensee's or certificate holder's facility; and (2) coordination with the Federal Aviation Administration (FAA). Suspicious activity is defined as behavior that may be indicative of intelligence-gathering or preoperational planning (surveillance) related to terrorism, criminal, espionage, or other illicit intentions. This appendix also provides guidance on activities that need not be reported.

In 2004, the FAA issued the following Notice to Airmen (NOTAM). This NOTAM advises pilots to avoid not only the airspace above or in proximity to U.S. nuclear power plants but also includes other key infrastructure facilities. The following is the published language contained in the most current NOTAM:

> FDC 4/0811 FDC … Special Notice … This is a restatement of a previously issued advisory notice. In the interest of national security and to the extent practicable, pilots are strongly advised to avoid the airspace above, or in proximity to such sites as power plants (nuclear, hydro-electric, or coal), dams, refineries, industrial complexes, military facilities and other similar facilities. Pilots should not circle as to loiter in the vicinity over these types of facilities.

The NRC staff recommends that licensees and certificate holders contact their nearest FAA Air Traffic Control (ATC) facility to discuss this NOTAM and its relevance to their facility, and to maintain a rapport with ATC personnel. Information on FAA Air Traffic Organization, Air Traffic Control Towers, Terminal Radar Approach Control facilities, Air Route Traffic Control Centers, and Flight Standards District Offices are available on the FAA Web site at http://www.faa.gov.

Licensees and certificate holders should immediately report suspicious flight activity above, or in close proximity to, nuclear power plants and other NRC-licensed facilities to their local FAA ATC facility in an attempt to identify suspicious aircraft. Licensee and certificate holder security managers should exercise judgment and discretion in determining whether a flight activity is suspicious with respect to normal air traffic patterns, proximity of the facility to local airports and U.S. military bases, the use of rivers and coastal waterways for navigational purposes, local weather conditions, and other unforeseen local circumstances. However, licensees and certificate holders should report multiple sightings of the same commercial or general aviation aircraft, circling or loitering above or in close proximity to facilities, or photographing the facility or surrounding area.

To allow for effective followup of these events by law enforcement agencies, a licensee's or certificate holder's incident reporting should be timely and should include, to the extent available, key information on the aircraft (e.g., aircraft registration number (N-number), physical description of aircraft, observed flight activity, date and time of incident, altitude, and direction of flight). The use of special photographic or visual sighting equipment may enhance the ability to capture pertinent information more accurately. (Several Web sites are available to identify N-numbers: http://registry.faa.gov/aircraftinquiry/NNum_inquiry.asp, http://registry.faa.gov/aircraftinquiry, and http://www.landings.com.)

If contact with the local FAA facility results in a determination that the aircraft is associated with a municipal, State, or Federal entity, or if the FAA can provide a valid explanation for the flight deviation that satisfies the facility security manager, then the licensee or certificate holder should not report the flight activity further. However, if the FAA cannot identify the aircraft or provide a valid flight plan or explanation of activity, then the licensee or certificate holder should immediately report the suspicious flight activity to local law enforcement.

There is no need for a licensee or certificate holder to notify the NRC Headquarters Operations Center in the event of an aviation-related activity involving government aircraft unless the licensee or certificate holder deems the activity suspicious in nature and it cannot be resolved at the local level. Otherwise, licensees or certificate holders should report suspicious aviation-related activity and incidents to the NRC Headquarters Operations Center in accordance with 10 CFR 73.71 and Appendix G. The NRC continues to work closely with FAA, the Transportation Security Administration, the U.S. Northern Command, and the North American Aerospace Defense Command, with respect to these types of suspicious aviation incidents, and will conduct additional coordination, if necessary.

Licensees and certificate holders should contact and coordinate with the following organizations with respect to suspicious aviation-related activities or incidents, in this order of priority:

1. their local FAA ATC facility or office,
2. their local law enforcement agency, and
3. the NRC Headquarters Operations Center, in accordance with 10 CFR 73.71.

The NRC will continue to forward information it has received on precoordinated overflight operations to affected licensees and certificate holders (e.g., waterfowl surveillance operations, power line surveys).

Licensees and certificate holders should contact organizations (i.e., military, government, and private sector) in their local area that could conduct aircraft operations in airspace over or near their facility, to coordinate and establish a link for advance notification of upcoming activity and for verification of ongoing activity that was not previously coordinated.