U.S. NUCLEAR REGULATORY COMMISSION June, 2007
OFFICE OF NUCLEAR REGULATORY RESEARCH Division 5

DRAFT REGULATORY GUIDE

Contact: B. Schnetzler
(301) 415-7883

DRAFT REGULATORY GUIDE DG-5019

(Proposed Revision 2 of Regulatory Guide 5.62, dated December 2006)

REPORTING OF SAFEGUARDS EVENTS

A. INTRODUCTION

This draft regulatory guide provides an approach acceptable to the NRC staff for use by licensees for reporting of security events. In 10 CFR Part 73, "Physical Protection of Plants and Materials," Section 73.71 requires licensees to report to the Operations Center of the Nuclear Regulatory Commission (NRC) or to record in a log certain security events. Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73 (Appendix G) describes reporting requirements in detail. Appendix E to 10 CFR Part 50 (Appendix E), "Emergency Planning and Preparedness for Production and Utilization Facilities," provides more detailed information for emergency planning and preparedness. The events to be reported or recorded are those that represent actual or potential threats, suspicious activities, external attacks, or internal tampering with equipment that threaten or affect safe plant operations or effective security operations. The events to be recorded are those that affect or lessen the effectiveness of the security systems, components, and procedures as established by security regulations and the licensee's approved security plans.

Licensee should consider obtaining access to NRC's Protected Webserver (PWS) in order to obtain routine threat bulletins and analyses from the Federal Bureau of Investigation (FBI) and U.S. Department of Homeland Security (DHS). Licensee should contact region and headquarters staff for further information on obtaining access to PWS.

This regulatory guide provides acceptable methods for use by licensees for determining when and how an event should be reported or recorded. The examples provided represent the types of events that should be reported but are not intended to be all inclusive. Should questions arise regarding the reporting or recording of an event or activities, the licensee may consider discussing the matter with appropriate region or headquarters NRC staff, if time permits. Otherwise, the report should be made and later discussed with the staff. The licensee is solely responsible for the decision and content of reports made to the NRC. Reporting or recording events under the provisions of this guidance should not be considered by licensee managers as indicative of performance failures. Rather, the NRC considers timely

and comprehensive communications of matters relating to threat assessment and protecting public health and safety as a primary and positive means of ensuring both.

Fitness-for-duty events are not addressed in this guide; licensees must report fitness-for-duty events under the provisions of 10 CFR 26.73.

Any information collection activities mentioned in this regulatory guide are included as requirements in 10 CFR Part 73.8, which provides the regulatory basis for this guide. The NRC considers the guidance contained herein to be the most current on acceptable approach for reporting.

The NRC issues regulatory guides to publically describe 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.

This draft regulatory guide relates to information collections that are covered by the requirements of 10 CFR Part 73 and that the Office of Management and Budget (OMB) has 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.

Table of Contents

B. DISCUSSION

Background

The information reportable under 10 CFR Section 73.71 is required to inform the NRC of security-related events that are, or have the potential to, endanger public health and safety or common defense and security, which provide threat-related information, or which could generate public inquiries. The required information also permits analysis of security system reliability and effectiveness, and potential changes in the local, State, and Federal threat environments.

The regulations in 10 CFR 73.71 provide the structure for reporting security-related information to the NRC. These reports require licensees to notify the NRC by telephone within 15 minutes, within 1 hour, or within 4 hours, as applicable. These reports also include events that licensees do not routinely transmit to the NRC but are recorded and maintained onsite for NRC review and analysis. The types of information to be reported generally are focused on event description, threat-related information, and security system reliability and effectiveness. This guidance follows the format of the revised rule. Appendix G provides a more detailed description of the types of events and information to be reported or recorded.

Certain significant security events warrant immediate involvement by the NRC. Therefore, licensees must report some events by telephone to the NRC within 15 minutes and others within 1 hour of initial discovery. Licensees should note that the required 15-minute notifications are, particularly important during a security-related event, and (1) support subsequent notifications to other licensees regarding a potential security threat and (2) inform other Federal organizations in accordance with the National Response Plan. Effective response by those affected could depends on the rapid and timely dissemination of information relating to imminent or actual security threats. Other significant security-related events continue to require prompt NRC notification within 1 hour. Additionally, licensees frequently become aware of activities at their facilities or in their communities that may be suspicious or indicative of potential pre-operational threat activities focused on their facilities. Suspicious activities are now required to be reported within 4 hours. Revisions to the rule and this guidance are intended to provide consistency in reporting among all applicable licensees.

Other security events not addressed above should be recorded by the licensee in a log within 24 hours of discovery and copies of the log are maintained as records for 3 years, from the date of the logged event. These log entries allow the NRC and licensees to analyze events at a particular site and similar events among licensees. In addition to providing valuable information regarding failures, degradations, or discovered vulnerabilities, an analysis of this information allows for the identification of generic issues that can be communicated to all.

The NRC intends that licensees report and record required information only. Consequently, in order to provide balanced guidance, this regulatory guide also provides information and examples of occurrences that are not be reportable or recordable. As with other portions of this Guide, the information contained in Section 3.4, “Examples of Security Events Not Expected to be Recorded in the Security Event Log,” is neither limiting nor constraining, and the responsibility for compliance with regulatory requirements is the licensees’.

For the purposes of this regulatory guide, and to assist in implementing the regulations, a glossary is provided at the end of this guide.

C. REGULATORY POSITION

1. Licensees Subject to 10 CFR 73.71

In order to clarify the applicability of the revised 10 CFR 73.71 and Appendix G to 10 CFR Part 73 (Appendix G) to categories of licensees, the staff notes the applicability of the following regulations:

- The regulations in 10 CFR 73.71(a) and paragraph I of Appendix G currently apply to power reactors subject to the provisions of 10 CFR 73.55.
- The regulations in 10 CFR 73.71(b) and paragraph II of Appendix G currently apply to licensees subject to the provisions of 10 CFR 73.25, 73.26, 73.27(c), 73.37, 73.67(e), or 73.67(g).
- The regulations in 10 CFR 73.71(c) and paragraph II of Appendix G currently apply to licensees subject to the provisions of 10 CFR 73.20, 73.37, 73.50, 73.51, 73.55, or 73.60.
- The regulations in 10 CFR 73.71(d) and paragraph III of Appendix G currently apply to power reactors subject to the provisions of 10 CFR 73.55.
- The regulations in 10 CFR 73.71(e) currently apply to various licensees and describe how licensees should make telephonic notification to the NRC.
- The regulations in 10 CFR 73.71(f) currently apply to licensees subject to the provisions of 10 CFR 73.20, 73.37, 73.50, 73.51, 73.55, or 73.60, and licensees possessing strategic special nuclear material (SSNM) subject to the provisions of 10 CFR 73.67(d).
- The regulations in 10 CFR 73.71(g) currently apply to all licensees who are required to submit a written report.

2. Telephonic Reportable Events

The regulations in 10 CFR 73.71(a), (b), (c), (d), and (e) require licensees to make a telephonic report to the NRC. Guidance regarding the types of information to be provided by telephone is discussed below. The purpose of a telephonic report is to ensure timely, direct, and accurate communication of information to the NRC relating to security matters that may require action on the part of licensees, the NRC, or other Government agencies. These actions may involve a change in the NRC Headquarters Operations Center response mode or response to media inquiries. Other methods of communication such as email or text messaging should not be used unless extreme conditions prohibit telephonic reporting. Some examples of these reports are also provided to assist licensees and the NRC in evaluating the reportability of security events and information received by licensees. The examples provided are not intended to be either limiting or all inclusive, but only illustrative.

Depending on the type of licensee, and the type of information required to be reported, the timeliness of telephonic reports differs, as described below. Timeliness in telephonic reporting is important to ensure effective communication among potential responders and within the threat analysis community. 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 should provide the most complete and accurate information available to them at the time telephonic reports are required to be made. It is recognized that information changes as events develop and as additional related information is received. Additional calls describing substantive changes, additions or modifications to the initial information provided should be made in a timely manner, but ***after*** immediate actions to

stabilize the plant have been taken in accordance with the licensee's emergency operations and imminent threat procedures.

It is recognized that some of the required telephonic security reports may result in an emergency classification in accordance with Appendix E to 10 CFR Part 50. Licensees should understand that while dual-reporting (making two phone calls to report the same information) is not normally required, a reportable security event is to be communicated under the most immediate reporting requirements. This communication can be concurrent but should not delay reporting in accordance with 10 CFR 73.71. Telephonic reports should not interfere with actual response or summoning assistance; however, telephonic reports should be considered actions of the highest priority to ensure require action on the part the NRC, or other Government agencies. Specific guidance is provided in Section 4.2, "Dual Reporting."

The importance of telephonic reports is emphasized by the fact that 10 CFR 73.22(f)(3) exempts the information transmitted under the provisions of 10 CFR 73.71 from protection requirements. Security information must only be transmitted by secure telecommunications equipment except in emergencies or extraordinary conditions in accordance with 10 CFR 73.22(f)(3) . The NRC considers telephonic reports that must be made pursuant to 10 CFR 73.71 to be the type of emergency or extraordinary condition contemplated by 10 CFR 73.22(f)(3) , and therefore would be subject to the exceptions. However, licensees should endeavor to protect sensitive information whenever possible and as conditions permit.

It is recommended that the determination for reporting events should be made by on-site security managers, licensees' agent managers, or their equivalent when practical. It is also suggested that procedures be developed to assist managers and other site personnel in making decisions regarding reporting and to describe the specific method each facility uses to make required notification(s).

The method and content of telephonic and written follow-up reports are described in Section 4. The licensee is not expected to report information that has been already provided to them by the NRC, such as the threat warning system addressed in Appendix C, "Licensee Safeguards Contingency Plans," to 10 CFR Part 73.

2.1 Security Events to be Reported Within 15 Minutes

The regulations in 10 CFR 73.71(a) require that each licensee subject to the provisions of 10 CFR 73.55 notify the NRC Headquarters Operations Center as soon as possible but not later than 15 minutes after the discovery of an imminent threat or actual threat against the facility described in paragraph I of Appendix G. This requirement only applies to power reactors.

As noted in paragraph I of Appendix G, these reports involve threats that result in the initiation of a security response consistent with a licensee's physical security plan, safeguards contingency plan, or defensive strategy and which are based on an actual or imminent threat. Although many levels of security response are described in the plans and strategy, for the purposes of this reporting requirement, the security response means the substantive implementation of the armed response capabilities (security contingency event). Licensees need not report response information initiated as a result of information provided to them by the NRC (e.g., NRC Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," (Ref. 1) and RIS 2006-12, "Endorsement of Nuclear Energy Institute Guidance 'Enhancements to Emergency Preparedness Program for Hostile Action'," (Ref. 2)).

Reports made under the provisions of this section are applicable only to security events, either actual or imminent which are also security contingency events. In the first situation, a licensee has been

attacked - a hostile act toward a Nuclear Power Plant or its personnel has been committed or in progress that includes the use of violent force to destroy equipment, take hostages, and/or intimidate the licensee to achieve an end. It includes attack by air, land, or water using guns, explosives, projectiles, vehicles, or other devices used to deliver destructive force. For reporting under this section, an imminent security event is one that is believed to be real, believed to have characteristics as described above, and which will likely manifest itself within 1 hour. Because an actual or imminent security event is also a security contingency event, a very short reporting time is required. The information provided in these reports may ensure that threat-related information is made available to other entities, which have the potential to be affected, in a timely manner.

The purpose of this notification is to allow the NRC to warn other licensees and initiate Federal response through DHS in accordance with the National Response Plan, when applicable. In support of this notification process the NRC Operations Center will not request an "open communications line" for the initial (<15 minute) notification. See Section 4.1.1 of this regulatory guide for additional information regarding the suggested content of these calls. If the licensee has classified the event before this call and that information is provided to the NRC, then the initial notification to the NRC as required by 10 CFR 50.72(a)(1)(i) will be considered met. Following the prompt notification, licensees are expected to provide additional information in accordance with the requirements of 10 CFR 50.72(c) and the licensee may be requested to maintain "open communications" at that time. See Section 4 of this Regulatory Guide for additional information on the process for making telephonic reports.

2.2 Examples of Security Events to be Reported Within 15 Minutes

The following list provides, but is not limited to, some examples of security events to be reported within 15 minutes:

(1) an actual or imminent assault on a licensees' facility that has characteristics or components of the Design Basis Threat (DBT) or an assault that exceeds the DBT characteristics or components

(2) detonation of an explosive device (e.g., a land or water vehicle bomb) at or near the facility

(3) notification from law enforcement authorities or other reliable source that a vehicle bomb or assault force is imminent at the facility

(4) a vehicle that attempts to forcefully (a deliberate, malevolent act) gain access through site vehicle barriers

(5) shots being fired at the facility - a threat to the site is believed to exist, and a security contingency response is initiated

(6) site-specific imminent threats - an imminent threat has been reported to the site and security response has been initiated (including discovery of intent to commit such an act, when a person or organization claims responsibility, or there is a pattern of threats)

(7) observed malevolent actions taken by an insider or other individual(s) that interrupt normal operation of a nuclear power reactor (e.g., mis-positioned valves or hand switches, severed connections, adding foreign substances into lubricants)

(8) taking of hostage(s) (e.g., onsite or offsite hostage taking as related to site operations)

2.3 Security Events to be Reported Within 1 Hour

Licensees should note that 10 CFR 73.71(a) and (b) require prompt 1-hour reports. These requirements are detailed in paragraph II of Appendix G.

The regulations in 10 CFR 73.71(b) relate to the loss or recovery of any shipment of special nuclear material (SNM) or spent nuclear fuel. These events involve security events in which theft, loss, or diversion of a shipment of SNM or spent nuclear fuel has occurred or is believed by the licensee to have occurred.

In addition, 10 CFR 73.71(c) points to the reporting of events listed in paragraph II of Appendix G. These events generally relate to events not addressed in the 15-minute reports. These security events are reportable if the NRC or licensee staff believes that a person has committed, caused, attempted to cause, or made a threat to commit or cause the following:

(1) theft or diversion of SNM

(2) significant physical damage to a power reactor, SNM processing facility, or carrier equipment transporting SNM or spent nuclear fuel

(3) interruption of normal operation of any NRC-licensed power reactor through unauthorized use of or tampering with its components, controls, or security systems

(4) actual or attempted entry of an unauthorized person into an area that the licensee is required to control access

(5) any uncompensated for failure, degradation, or vulnerability in a security system that could allow undetected or unauthorized access to a controlled area

(6) actual or attempted introduction of contraband into an area which the licensee is required to control access

(7) for power reactor licensees, an actual or attempted introduction of contraband into the owner-controlled area (OCA) when the contraband has been determined to represent a threat capable of reducing the effectiveness of the physical security program[1]

These types of reports include security events or information not reported as a the 15-minute immediate reports (actual and substantial armed response) but which provide reason to believe that a person has caused or attempted to cause an event, or has made a threat to cause the types of events outlined in paragraph II(a) of Appendix G. In terms of this 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 which claims responsibility for the threat. "Attempts to cause" a threat means that reliable and substantive information exists that 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 which are less imminent in nature and which may not necessarily result in a substantive armed response or deployment of the security force or a contingency response. They may result, for example, in a commitment of staff to search a facility or the request of assistance from law enforcement authorities, or cause a search for an overdue shipment.

The types of actions that should be reported include (1) the theft or unlawful diversions of SNM or (2) physical damage to power reactors, SNM processing facility, or transportation equipment. Licensees should evaluate these security-related events to determine whether these events involve a

---

[1] This addition to paragraph II of Appendix G, Part 73, is being considered for final rule language of the proposed rule, "Power Reactor Security Requirements," published in the *Federal Register* on October 26, 2006, Pages 62664 - 62874. (Ref. 3)

threat or are non-threat-related, such as mechanical failure or obvious accidents. Nevertheless, licensees should report theft or diversion of SNM, regardless of the cause.

The interruption of normal operations of a nuclear power reactor that is the result of intentional tampering or unauthorized use of equipment or components is also reportable. This could include intentional tampering with systems or equipment that is normally in standby but would need to operate if called upon. Licensees should ensure that an appropriate preliminary evaluation of potential or actual interruptions of operations-related occurrences is initiated to determine whether the causes would likely be simple human error, mechanical failure, or intentional acts. This evaluation should include reasonable actions or information collected within 1 hour. At that time, licensees should make the decision whether the information indicates an actual or attempted threat and make a telephonic report as applicable. Should a licensee determine that the collected information does not represent an actual or attempted threat and later changes its determination, the licensee can make a report at that time, when the determination changes.

Paragraph II(b) of Appendix G refers to the actual or attempted entry of an unauthorized person into any area that the licensee is required to control. This would include, for example, protected areas, vital areas, material access areas, controlled access areas, or transportation equipment. The delineation and control measures for each of these areas are described in applicable portions of 10 CFR Part 73. An actual entry refers to the penetration or the actual circumvention of those control measures by a person who is not, at the time, authorized into the area in question. "Attempts of entry by unauthorized persons, vehicles, or material" means 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. An attempt at entry that was stopped by responders or other security system elements would be included. Licensees should ensure that an appropriate evaluation is conducted within the reporting time to determine whether the entry or attempted entry was unauthorized. Power reactor licensees may have a situation that is an exception to the 1-hour reporting requirements of the regulation: personnel who attempt to enter or actually enter a controlled area (e.g., vital area) by tailgating into areas where they do not have current authorization but would have been authorized, if needed. For power reactor licensees, this event is not a threat to the plant. For power reactor licensees, unauthorized entry of personnel does not include the vehicle barrier system unless an actual or attempted entry was made that threatens security. See Sections 2.4 and 3.2 of this regulatory guide for more examples of security events.

The actual or attempted introduction of contraband material, such as weapons, explosives, incendiary devices, which represents a threat to the safe operation or security integrity of the facility, should be reported as noted in paragraph II(d) of Appendix G. Licensees should ensure that an appropriate evaluation is conducted within the reporting time to determine whether the actual or attempted introduction of contraband into a controlled area occurred. Power reactor licensees would not include the OCA in this evaluation unless an actual or attempted introduction of contraband is made that threatens security.

Uncompensated failures and degradations or discovered vulnerabilities of safeguard systems that could likely allow unauthorized or undetected access to an area required to be controlled should be reported within 1 hour, as described in paragraph II(c) of Appendix G. "Uncompensated" means compensatory measures included in security plans or procedures that have either not been implemented, were implemented incorrectly, or were ineffective. To clarify, for the uncompensated failures just discussed, licensees should report not only mechanical or electrical problems but also failures in procedures and personnel practices or performance. Exercises, testing, maintenance, audits, inspections, and recurring observations are intended to or may identify failures, degradations, or vulnerabilities in

security systems, and some may be required to be reported within 1 hour. However, it is not intended that all findings are reported. Only those types of security events that could actually allow undetected or unauthorized access should be reported within 1 hour. These types of events would usually affect multiple layers of physical security systems or an individual, critical, single-failure of a program element that would allow undetected or unauthorized access. Other failures, degradations, or discovered vulnerabilities of security systems not relating to unescorted or undetected access may need to be recorded as described in paragraph IV of Appendix G. To determine the appropriate reporting category for security events, licensees should review the lists for each category (e.g., Section 3.4, "Examples of Security Events Not Expected to Be Recorded in the Security Event Log").

See Section 4.1.2 of this regulatory guide for additional information regarding the suggested content of these calls.

2.4 Examples of Security Events to be Reported Within 1 Hour

The following list includes, but is not limited to, some examples of security events to be reported within 1 hour.

(1) The following are examples for theft or diversions of SNM:

- discovery of a suspicious vehicle following a licensed carrier transporting formula quantities of SSNM or spent fuel for which law enforcement authorities have been notified
- actual breakdown of transport vehicle for SSNM
- actual or believed theft, diversion, or loss of SNM or spent fuel
- mass demonstration near plant which could cause a threat to the facility

(2) The following are examples of significant physical damage to a power reactor, SNM processing facility, or carrier equipment transporting SNM or spent nuclear fuel:

- bomb or extortion threats that are considered reliable and substantive, when the event has not been reported under Section 2.2, "Examples of Security Events to be Reported Within 15 Minutes" (This includes the discovery of intent to commit such an act. In addition, the results of any bomb search should be made within 1 hour of completion. Unsubstantiated bomb or extortion threats which are part of a pattern of harassment should also be reported within 1 hour.)
- fire or explosion of suspicious or unknown origin within an OCA, protected area, controlled area, material access area, vital area, or target set area that has not been reported under the 15-minute guidelines

(3) The following are examples for interruption of normal operation of any NRC-licensed power reactor through unauthorized use of or tampering with its components, controls, or security systems:

- tampering with plant equipment or physical security equipment that is either confirmed to be suspicious or malevolent in origin or is determined not to be reasonable mechanical failure or human error (Events which are suspicious in nature and for which no general assessment can be made within 1 hour, should be reported)

- confirmed cyber attacks on or failures of computer systems that may adversely impact safety, security, and emergency preparedness
- an actual or imminent strike by the security force

(4) The following are examples of actual or attempted entry of an unauthorized person into an area that the licensee is required to control access:

- actual entry of unauthorized person into a controlled access area (for power reactor licensees, this does not include the OCA unless an actual or attempted entry was made that threatens security)
- discovery of a criminal act involving individuals granted unescorted access, which in the judgment of the licensee, could afford an opportunity to adversely effect plant safety or represents a threat
- discovery of falsified identification badges or key-cards that could allow access to controlled areas
- uncompensated for loss of all ac power to security systems that could allow unauthorized or undetected access to areas which are required to be controlled
- improper control of access control area or media (e.g., key-cards, passwords, cipher codes) that results in the use of the media during the time it is not controlled (e.g., tailgating into an area to which the individual would not have been authorized),
- incomplete or inaccurate preauthorization screening that would have resulted in the denial or suspension of unescorted access authorization had the screening been complete and accurate (this involves either the authorization or the granting of unescorted access)

(5) The following are examples of any uncompensated for failure, degradation, or vulnerability in a security system that could allow undetected or unauthorized access to a controlled area:

- discovery of lost or stolen classified documents (e.g., National Security Information or Restricted Data) pertaining to a facility or transportation
- discovery of lost or stolen unclassified safeguards information that would substantially assist in the circumvention of security systems or which has been lost in a manner that could allow a significant opportunity for compromise
- the unavailability of the minimum number of security response personnel are unavailable even after the appropriate recall procedure for the security force has been implemented
- loss of intrusion detection capability that is not compensated within NRC-approved security plan requirements
- failure to adequately compensate for an event or identified failure, degradation, or vulnerability that could allow undetected or unauthorized access (licensees need not report within 1 hour if the failure involves a very short period of time, i.e., 10 minutes or less, those events should be logged)
- loss of either the alarm capability or locking mechanism on a material access portal
- an uncompensated design flaw or vulnerability in a physical protection system that could have allowed unauthorized access or which could have substantively eliminated or significantly reduced response capabilities

- loss of all offsite communications

(6) The following are examples of actual or attempted introduction of contraband into an area which the licensee is required to control access:

- discovery of unaccounted, lost, or stolen keys (but not key-cards or badges) that allow access to controlled areas
- loss of a security weapon that is not retrieved within 1 hour

(7) An example for power reactor licensees is an actual or attempted introduction of contraband into the OCA when the contraband has been determined to represent a threat capable of reducing the effectiveness of the physical security program.[1]

2.5 Security Events of Suspicious Activities to be Reported Within 4 Hours

This telephonic reporting requirement applies only to power reactor licensees. Licensees should report suspicious activities, as these may indicate pre-operational surveillance, reconnaissance, or intelligence gathering targeted against the facility. The NRC intends that this category address the reporting of suspicious activities only and not other security events. The reporting of suspicious activities assists the NRC in evaluating threats and potential threats that may be directed at licensed nuclear power reactors. In some cases, the intelligence community has benefitted from followup investigations based on reports of what originally appeared to be innocuous activity, made under the NRC's advisory guidance. Additionally, experience in threat evaluation in recent years has shown that the intelligence and homeland security communities are assisted by the inclusion of reports that provide information regarding suspicious activities in evaluating threats across the critical infrastructure. Although these requirements apply only to power reactors, the NRC strongly encourages other licensees to report suspicious activities, in accordance with guidance previously provided.

When reporting events under these requirements, licensees also should consider the additional guidance that the NRC provided since the September 11, 2001, terrorist attacks on the United States (e.g., Regulatory Information Summaries, Information Assessment Team Advisories). Often these events are time-sensitive and transitory in nature so that, as noted in Section 4.3, written reports are not necessary. The NRC believes that the reporting interval of 4 hours should be sufficient to meet the broader goals of threat assessment. However, licensees should recognize that some suspicious activities, by their nature, may be more sensitive or significant than others and may need to be reported sooner. The licensee's security and plant management may decide to submit a report sooner than required by NRC regulations.

A suspicious activity may quickly lead to a response or event. Licensees should report that response or event in accordance with 10 CFR 73.71 and Appendix G and include the suspicious activity as factual information.

Suspicious activities to be reported should be concrete events and not based solely on speculation. Concrete events include observations by staff, local law enforcement personnel, evidence of the presence of unknown personnel, telephone contacts, documents obtained, and testimonies of credible witnesses.

Licensees should also recognize that NRC is neither requesting licensees to actively gather intelligence nor designating licensees with the authority to conduct law enforcement activities. The NRC

intends that licensees report information that comes to their attention. These reporting requirements provide for a consistent means of communicating this type of information to the NRC.

Licensees can obtain additional information regarding possible indicators of terrorist activities that may be encountered during the course of normal activities in a jointly published DHS–FBI report entitled, "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resources, Owners, and Operators," designated Unclassified and For Official Use Only. Licensees can obtain this 18-page document from the NRC, available as Event 2464 on the NRC's PWS.

2.6 Examples of Security Events to be Reported Within 4 Hours

The following list includes, but is not limited to, examples of security events to be reported within 4 hours:

(1) The following are examples for any security-related incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility:

- persons showing uncommon interest or inquiries in security measures or personnel, entry points or access controls, or perimeter barriers such as barriers, fences, or walls
- persons showing uncommon interest in facilities by photographing or videotaping
- suspicious attempts to recruit employees or persons knowledgeable about key personnel, facilities, or systems
- persons loitering for no apparent purpose who do not fit into the surrounding environment (e.g., such as persons wearing improper attire for the conditions)
- suspicious behavior (e.g., fleeing, staring, moving quickly away from personnel, unexpected vehicle movement when approached)
- secretive use of still cameras, video recorders, sketching, map making, or note-taking that is not usually associated with normal tourist interest or behavior
- elicitation of information from security or other site personnel regarding security systems and/or vulnerabilities[2]
- unauthorized attempts to probe or gain access to business secrets or other licensee-sensitive information or control systems, to include the use of social engineering techniques (e.g., impersonating users)
- theft or suspicious loss of official company identification documents, uniforms, or vehicles necessary for accessing plant facilities
- use of forged, stolen, or fabricated documents to support access control or authorization activities
- use of forged, stolen, or fabricated documents to gain access to the OCA for any purposes

---

[2] Care should be taken to recognize accredited working journalists conducting normal and recognizable research. If their interest is routine or typical and understandable, their elicitation of information should not be reported.

- boating activities conducted in atypical locations or attempts to loiter near restricted areas
- any unusual attempts to obtain information or documents relating to training in site security techniques, procedures, or practices
- discoveries of Web site postings which make violent threats relating to NRC-licensed facilities
- unusual threat- or terrorist-related activities ***that become known*** to plant security or management staff within the local community or other local critical infrastructure or key resources involving the following: (a) unusual surveillance, probing or reconnaissance, (b) attempts to gain unauthorized access, (c) attempts to gain access to or acquire hazardous or dangerous materials, (d) unusual use of materials, or (e) financing to support terrorist activities
- a stated threat against the facility

(2) An example for any security-related incident involving suspicious aircraft overflight activity is suspicious aircraft activity. (Appendix A of this regulatory guide outlines the guidance for reporting suspicious aircraft activity and for interfacing with Federal partners. In accordance with Appendix A, licensees are requested to continue to use previously established communications protocols.)

(3) An example for incidents resulting in the notification of local, State or national law enforcement, or law enforcement, or law enforcement response to the site not reported under other areas of this guidance is calls to law enforcement for support or response relative to events not already reported in 15 minutes or 1 hour. In particular, reports should be made of calls made to local law enforcement agencies requesting a security response. This does not include when law enforcement personnel are on-site for non-response official duties, training exercises, other scheduled activities, or sharing of information related to the 4 hour report category.

3. Recordable Events (Do Not Require Telephonic Notification)

Recordable or "loggable" events do not require telephonic notification to the NRC. Rather, licensees should record these events in a security event log that may be hard-copy or, preferably, a searchable electronic database. The event must be recorded in the licensee's chosen system within 24 hours of discovery.

Generally, these events are less significant than those required to be reported within 15 minutes, 1 hour, or 4 hours. However, analysis or follow-up to these logged events may result in the identification of system or performance vulnerabilities or deficiencies that may require corrective action and which may be generic in nature. The NRC expects that all loggable events be recorded regardless of who identifies them (i.e., licensee staff, contractors, the NRC or State inspectors, or independent auditors).

These events include any failures, degradations, or discovered vulnerabilities that could have allowed either unauthorized or undetected access to any area or transport controlled by NRC regulation (e.g., OCAs, protected areas, vital areas, material access areas, or controlled access areas) if compensatory measures had not been in place at the time of discovery.

Compensatory measures are described in facility security plans. Such 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 subsystem is not reduced by the failure or other contingency affecting the operation of the security-related equipment or structure. In order to consider compensatory measures in place, in terms of logging, they need to be implemented prior to the event or in a timely fashion as described in 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.

The significance and duration of a system defect or vulnerability are key factors in determining whether an event is reportable or simply recorded in the security event log. Even compensatory measures implemented promptly after discovery of the defect or vulnerability cannot provide protection for the period of time that the defect or vulnerability existed. Therefore, any failure, degradation, or discovered vulnerability that is known to have existed for a significant period of time and that should or could have been discovered in the course of patrols, surveillance, operational tests, or other means should be considered for reporting within 1 hour. "Uncompensated" means compensatory measures included in security plans or procedures have either not been implemented, were determined to be ineffective, or were implemented incorrectly. The aforementioned reports on failure and degradation should include not only mechanical or electrical problems but also failures in procedures or personnel practices or performance. Exercises, testing, maintenance, audits, inspections, and recurring observations are intended to identify failures, degradations or vulnerabilities in security systems, and may be required to be logged. Only those types of events that could actually allow undetected or unauthorized access should be reported by telephone. Loggable types of events would usually affect single elements of physical security systems or any individual, a critical single-failure program element that would not allow undetected or unauthorized access. Additionally, administrative errors could represent such failures. Other failures, degradations or discovered vulnerabilities of security system not relating to likely unescorted or undetected access should be recorded as described in paragraph IV(a) of Appendix G.

3.1 Security Events to be Recorded in the Security Log

Other less significant threatened, attempted, or committed acts or identified weaknesses/vulnerabilities not defined in previous sections of this guidance may have the potential to reduce the effectiveness of the physical protection below that described in physical security or contingency plans. Licensees should log these identified acts or vulnerabilities within 24 hours of identification or occurrence. For example, such an act is the failure to properly control security information that could not significantly assist in gaining access to a facility. Another example is a bomb threat in which the caller is easily identified as a child, with no specificity nor other corroborating information.

3.2 Examples of Security Events to be Recorded in the Security Log

The following list includes, but is not limited to, some examples of security events to be recorded in the Security Log:

(1) The following are examples of any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to any area or transport in which the licensee is required by Commission regulation to control access had compensatory measure not been established:

- properly compensated computer failures
- properly compensated card reader failures
- properly compensated loss of the ability to detect intrusion (a) at the protected area perimeter when the loss involves several zones or (b) within a single intrusion detection zone
- failure of search equipment for a short period which could have allowed un-searched personnel and packages from entering controlled areas
- an individual requiring escort becomes separated from his or her escort for a short period of time (e.g., less than about 10 minutes), and it is determined that no unauthorized areas were entered
- an individual is incorrectly issued a badge granting access to areas not authorized, but who does not or cannot enter those areas and, when corrected, may be granted access
- an individual who is incorrectly (i.e., through an error not amounting to falsification) authorized unescorted access, but who has not been granted access through the issuance of control media (e.g., badge)
- incomplete or inaccurate pre-access screening information, testing, and other procedures that would not have been required to support access authorization or result in denial of access
- 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 10 minutes)
- tailgating into an area to which an individual is authorized or could have been authorized

(2) The following are examples of any other threatened, attempted, or committed act not previously defined in Appendix G to Part 73, "Reportable Safeguards Events," with the potential for reducing the effectiveness of the physical protection program below that described in a licensee physical security or safeguards contingency plan, or the actual condition of such reduction in effectiveness:

- the failure or degradation of lighting below security plan requirements as long as the entire perimeter Intrusion Detection System (IDS) remains operational
- for power reactors, loss of the partial capability of one alarm station to remotely monitor, assess, or initiate response to alarms if the same capability remains operable in the other alarm station
- for shipments of formula quantities of SSNM, loss of intra-convoy communications when communications capability with the movement control center remains
- loss of control or protection of unclassified safeguards information when there does not appear to be evidence of theft or compromise, and is recovered within 1 hour
- loss of control or protection of unclassified safeguards information which would not have allowed unauthorized or undetected access or significantly affected contingency response
- loss of control of a security weapon that is retrieved within 1 hour of the discovery

- discovery of prohibited items inside a controlled area that is not a significant threat to the facility (see glossary for definition of prohibited items)
- access control feature failures that unlock a door, but with a continuing operable alarm, or a failed alarm with a secure door
- unsubstantiated bomb or extortion threats[3]
- frequent nuisance alarms caused by mechanical or environmental conditions and false alarms that meet or exceed the rates committed to in the licensee's approved physical security plans or procedures which may degrade system or staff performance but do not degrade the implementation of the site protective strategy
- unplanned missed security patrols
- the unfavorable termination of personnel whose job duties and responsibilities actively support insider threat mitigation
- discovery of contraband material outside the protected area or inside a designated vehicle barrier or control point that does not constitute a threat or potential threat to the facility

3.3 Security Events Not Expected to be Recorded in the Security Log

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

Licensees should use the guidance in this section to determine whether some events are required by the regulations to be reported or recorded. Nothing in this section should suggest that an event required by the regulations to be reported should not be reported. The NRC intends that this section clarifies reporting requirements. This section does not obviate, circumvent, or change reporting requirements. Licensees should use sound and reasonable technical judgement and experience when determining whether or not 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 not reporting or recording of an event, the licensees may consider discussing the matter with the appropriate region or headquarters NRC, if time permits.

Certain failures of the security system that do not and could not reduce the effectiveness of the system have little or no security significance, and should not be reported or logged.

3.4 Examples of Security Events Not Expected to Be Recorded in the Security Event Log

The following list includes, but is not limited to, some examples of security events not expected to be reported or recorded in the Security Event Log:

---

[3] An unsubstantiated bomb or extortion threat is a threat in which no specific organization or individual claims responsibility, is patently fake, and is not supported by evidence other than the threat message.

(1) failure, degradation, or compromise of security systems that are preplanned and for which adequate compensatory measures are in place before the event

(2) a child attempting but failing to climb a protected area fence

(3) a fire or explosion if the origin can be determined within 1 hour that is not suspicious and is consistent with normal mechanical or human error, and the facility sustains no significant damage (e.g., a fire in a trash bin, a lightening strike)

(4) infrequent nuisance alarms caused by mechanical or environmental problems and false alarms that do not exceed the rates committed to in the licensee's approved security plans, or their implementing procedures, or do not degrade system effectiveness

(5) suspected tampering with safety equipment that is determined, within 1 hour, not to be tampering

(6) discovery of prohibited material[4] outside the protected area, or inside a designated vehicle barrier or control point that does not constitute a threat or potential threat to the facility

(7) cuts or holes made through required barriers made by authorized persons for legitimate reasons (e.g., to install a pipe) with prior approval, coordination, and proper implementation of compensatory measures

(8) infrequent and nonrecurring failure of search equipment if the licensee discovers the failure before anyone enters unsearched

(9) lost, stolen, unaccounted, 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 determines could not be used to allow unauthorized or undetected access[5]

(10) an individual requiring an escort, becomes separated from the escort, who recognizes and reestablishes the escort in 5 minutes or less and the licensee determines that the individual did not enter any unauthorized areas

(11) an individual requiring escort enters a nonsensitive area with limited ingress/egress (such as a rest room) while the escort maintains observation of the ingress/egress point[6]

(12) infrequent and nonrecurring access control feature failures that unlock a door, but with a continuing operable alarm, or a failed alarm with a secure door, provided the licensee implements compensatory measures before anyone enters

(13) discovery of a suspicious vehicle following a licensed carrier transporting formula quantities of SSNM or spent fuel, for which the licensee notified law enforcement authorities, when the vehicle is determined, within 1 hour, not to be a threat

(14) individuals photographing facilities from tourist overlooks or stations, provided no other suspicious activity is involved

---

[4] Examples of prohibited items include but are not limited to illegal drugs, alcohol, large knives, ammunition for a firearm, and prescription medication not prescribed for the person in possession.

[5] Some similar events may be required to be logged or reported.

[6] Escort of visitors does not require intrusion into personal activities, but monitoring to ensure physical whereabouts of visitors is supervised.

(15) normal and routine inquiries from students or members of the public regarding facilities or activities,[7]

(16) routine, prearranged, or non-suspicious aircraft activity

(17) response information initiated due to information provided to licensees by the NRC

4. Procedures for Telephonic Reports and Dual Reporting

4.1 Telephonic Reports

All telephonic reports (15-minute reports, 1-hour reports, or 4-hour "suspicious activities" reports) are made to the NRC Headquarters Operations Center at (301) 816-5100. Telephonic notifications should be made via the NRC's Emergency Notification System (ENS), or other telephonic system that may be designated by the NRC, if the licensee is party to that system. If the ENS (or other designated system) is inoperable or unavailable, a commercial telephone or other effective means should be used to ensure that the required notification is received by the NRC Operations Center in the time required.

Should the use of other emergency notification systems replace or supplement the ENS, licensees should use those systems as directed by the NRC.

If pertinent new information or errors are uncovered after the initial telephone report, but prior to submittal of a written report (as required), the licensee should notify the NRC Headquarters Operations Center of the information or error by telephone, using the same timeliness guideline as the initial report.

Safeguards information must be transmitted only by secure telecommunications equipment except in emergencies or extraordinary conditions. The telephonic reports discussed herein are considered to be extraordinary conditions and regulations in 10 CFR 73.21(f)(3) exempt the information transmitted under the provisions of 10 CFR 73.71 from protection requirements, so telephone reports made pursuant to 10 CFR 73.71 may be transmitted over unprotected lines when necessary. However, licensees should endeavor to protect sensitive information whenever possible and as conditions permit.

4.1.1 15-minute Reports

Licensees should ensure that the 15-minute telephonic reports clearly but concisely communicate the nature, magnitude, imminency, or effect of the actual or imminent threat against the plant, known at the time of the report, to the on-duty NRC Headquarters Operations Officer. At a minimum, licensees should include the following information in the call:

(1) name and location of facility

(2) threat description including brief description of initiated response (see Section 2.1)

(3) current event status, e.g., ongoing, completed, imminent, unknown

(4) caller's name and call-back number

(5) emergency classification (only if already determined)

---

[7] Care should be taken to recognize accredited working journalists conducting normal and recognizable research. If their interest is common and understandable, their elicitation of sensitive information should not be reported.

4.1.2 1-hour Reports

Licensees should ensure that the 1-hour telephonic reports clearly but concisely communicate all known, relevant information at the time of the report to the on-duty NRC Operations Officer. At a minimum, licensees should include the following information in the call:

(1) name and location of facility

(2) caller's name and call-back number

(3) event description including the following information:

  (a) who was involved

  (b) what comprised event or what happened

  (c) when the event initiated and when completed, if known

  (d) where the event occurred (this may include plant or security systems or geographic locations effected)

  (e) why the event occurred, if known

  (f) how the event occurred

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

(5) response or corrective actions taken

(6) offsite assistance or media interest

4.1.3 4-hour Reports (Suspicious Activity)

Licensees should ensure that the 4-hour telephonic reports clearly but concisely communicate all known, relevant information at the time of the telephonic report to the on-duty NRC Operations Officer. At a minimum, licensees should include the following information in the call:

(1) name and location of the facility reporting the activity

(2) facility type

(3) caller's name and call-back number

(4) event date and time

(5) description of information

(6) source of information (if law enforcement agency, provide telephone number)

4.1.4 Telephonic Followup Requirements

The guidance in this section is intended to provide a "bridge" between the initial report of an event and the communications protocols already established by emergency response plans and procedures. This establishes the possible use of an open, continuous communication channel with the NRC Operations Center. Many of the events required to be reported under 10 CFR 73.71 may have already resulted in the declaration of an emergency class by the licensee, and the communications protocols for those declarations should be used. Other events and information may not result in the

activation of emergency or contingency response communications protocols. The NRC Operations Center will not request an open communications line for the initial (<15 minute) notification. Questions from NRC during this call should be limited to those questions which would give the NRC an understanding of which facility is involved and the nature of the event. Subsequent to the initial report, licensees are expected to provide additional information in accordance with the requirements of 10 CFR 50.72(c) and at that time a licensee may be requested to maintain "open communications." The NRC does not require licensees to maintain an open, continuous means of communication for reporting suspicious activities.

The NRC emphasizes the importance of initially providing critical information in a timely manner. The NRC also recognizes that events can develop rapidly and information can significantly change over time. Consequently, providing telephonic followup is important to ensure that the NRC and licensees continue to make decisions based on a common set of facts.

4.1.5 Telephonic Followup Guidelines

The licensees should use the following guidelines when following up on telephonic reports:

(1) If pertinent information or errors are uncovered after the initial telephone report (for <15 minute reports and 1-hour reports) but prior to the submittal of the written report, the licensee should notify the NRC Operations Center of the information or error in a timely manner.

(2) It is anticipated that the suspicious activities reported within 4 hours of discovery will be transitory, and will usually not require followup telephonic notifications. However, if pertinent information or errors are uncovered after the initial telephone report, licensees may choose to contact the NRC Operations Center to ensure accuracy of the information already provided. For suspicious activity reports, a licensee should not be requested to provide a continuous communications channel. However, should the licensee later obtain additional information, or should any followup be necessary, communications should be handled through the NRC's threat assessment process and may be communicated directly with region or headquarters Information Assessment Team (IAT) members. Contact with IAT members may be established with assistance from the NRC Operations Center. Should suspicious activity lead to an event that requires response, established emergency response communications procedures should be used to determine reportability.

(3) An open, continuous communication channel with the NRC Operations Center may be requested for 15-minute reports of actual or imminent security threats, made in accordance with 10 CFR 73.71(a). Subsequent to the 15-minute report, this communications link may be requested at the time when the licensee is expected to provide additional information in accordance with the requirements of 10 CFR 50.72 (c). The establishment of a continuous communications channel would not supercede current emergency preparedness or security requirements to notify State and local officials or local law enforcement authorities, nor would it supercede requirements to take immediate action to stabilize the reactor plant. When established, the continuous communications channel should be staffed by a knowledgeable individual in the licensees security or operations organizations such as a security supervisor, alarm station operator, operations personnel. The location of this communicator should be designated in licensee procedures and should be appropriate to obtain and communicate information regarding the status of the event or response. The continuous communications channel may be established using the ENS (or other telephonic system that may be designated by the NRC) if the licensee has access, or by commercial telephone line with phone(s) identified for this purpose.

(4) An open, continuous communication channel with the NRC Operations Center may be requested for telephonic reports made within 1-hour of discovery in accordance with 10 CFR 73.27(b) and (c). These events relate to loss of any shipment of SSNM or spent nuclear fuel and events described in paragraph II of Appendix G. This communications link may be requested following the licensee's completion of other required notifications made in accordance with 10 CFR 50.72 or Part 50 Appendix E, and after any immediate actions needed to stabilize the plant. When established, the continuous communications channel should be staffed by a knowledgeable individual in the licensees security or operations organizations such as a security supervisor, alarm station operator, or operations personnel. The location of this communicator should be determined by the licensee and should be appropriate to obtain and communicate information regarding the status of the event or response. The continuous communications channel may be established using the ENS if the licensee has access, or by commercial telephone line with phone(s) identified for this purpose.

4.2 Dual Reporting

Events of a dual nature (i.e., having both safety and security implications and being subject to the requirements of 10 CFR 50.72, 50.73, and 73.71) do not require duplicate reports under the requirements of 10 CFR 73.71. If a power reactor licensee reports an event that is reportable in accordance with both 10 CFR 50.73 and 73.71, the licensee should follow the procedures described in 10 CFR 50.73 (i.e., NRC Form 366, "Licensee Event Report" (LER)). However, if an emergency classification declared per the station's emergency plan is not provided as part of the 15-minute notification per 10 CFR 73.71(a), then a separate notification shall be made in accordance with 10 CFR 50.72(a)(3).

The procedures contained in NUREG-1022, "Event Reporting Guidelines 10 CFR 50.72 and 50.73," (Ref. 4) describe how to indicate that an LER meets multiple reporting requirements. Similarly, SNM licensees need not report more than once for events covered under both 10 CFR 70.52 and 73.71, or under both 10 CFR 74.11 and 73.71. Licensees should ensure that sensitive unclassified non-safeguards information (SUNSI) is not included in documents unless the SUNSI is properly controlled both in electronic or hard-copy formats.

4.3 Written Reports

Licensees who are required to make a 15- minute or 1-hour report must, by regulation, followup the initial telephonic notification with a written report within 60 days of the initial telephonic notification. The purpose of these written reports is to ensure that all the facts of a reported event are captured and available for NRC review and analysis and evaluation. Because these followup written reports will be used by NRC for analysis and evaluation and may represent the final description of an event, the reports should thoroughly detail the facts of the event, its causes (if known), and the actions taken. This section outlines the information licensees should include in the followup written report.

Power reactor licensees should continue to use an LER format as in the past; other licensees should use a letter format. Unlike the initial telephonic notification, followup written reports are not exempt from the provisions of 10 CFR 73.21, and any unclassified safeguards information or other sensitive information contained in written reports must be protected as required. Electronic media using approved encryption software may be acceptable.

Some events, and the followup reports describing them, may be extensive, complicated, and multi-faceted and must be submitted within 60 days of the initial telephonic notifications. Subsequent to the submittal of the initial written report, the licensees may discover unintentional errors in the report or supplemental information may become available. As noted below, the licensee should submit a revised report as soon as possible which contains the previous information and adds the new information. To ensure clarity, the supplemental report should be a complete revised report, with revisions or changes highlighted.

Licensees are not required to submit followup written reports of suspicious activities made under the provisions of 10 CFR 73.71(d) and paragraph II of Appendix G. However, should additional investigation or fact gathering be necessary, licensees should be prepared to provide evidence (e.g., photographs, documents, routine voice recordings, voice mail, witness statements) in their possession if requested by investigating or regulatory authorities.

4.3.1 NRC Form 366

When submitting reports that are reportable solely under the provisions of 10 CFR 73.71, power reactor licensees should use the LER, NRC Form 366. Not all items included on NRC Form 366 may apply when security events are reported. Licensees should include all the information needed by the NRC as described in Section 4 and related subsections.

The provisions of 10 CFR 73.21(f) must be met when transmitting written safeguards information. Power reactor licensees should modify their LER procedures accordingly.

All other licensees should provide the report in a letter that contains the information indicated in the following section.

4.3.2 Content of Written Reports

All follow up written reports that must be submitted within 60 days of a telephonic notification should contain, at a minimum, the following information:

(1) date and time of the event, including chronological time line if applicable; date and time of NRC notifications

(2) locations of actual or threatened event in a protected area, material access area, controlled access area, vital area, OCA, or other area (specify area)

(3) for power reactors, the operating mode, e.g., shut down, operating

(4) safety or security systems directly or indirectly affected, damaged, or threatened

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

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

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

(8) immediate actions taken in response to the event and compensatory measures in place

(9) local, State, or Federal law enforcement agencies contacted

(10) description of media interest and press releases

(11) indications or records of previous similar events

(12) procedural errors, human errors, or equipment failures, as applicable

(13) cause of event or licensee analysis of event (including a brief summary in the report and reference any ongoing or completed detailed investigations, assessments, analyses, or evaluations)

(14) corrective actions taken or planned, including dates

(15) name and phone number of knowledgeable contact

For reported uncompensated failures, degradations, or discovered vulnerabilities of security systems, licensees should also provide the following information in addition to items 1 through 15 above:

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

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

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

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

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

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

(g) effect on plant safety

For threat-related incidents, licensees should also provide the following information in addition to items 1 through 15 above:

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

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

(c) method or means of threat communication, e.g., letter, telephone, email

(d) text or verbatim transcript of threat

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

Licensees should be aware that any media used to communicate a threat may become evidence in an investigation and the integrity of that material should be maintained.

4.3.3 Submittal of Written Reports

In accordance with proposed 10 CFR 73.71(f)(2)(a)(4), 73.71(g)(3), 73.71(g)(6), 73.71(g)(8), and (g)(11), licensees should perform the following when submitting a written report:

(1) Submit one copy of each written report to NRC Headquarters.

United States Nuclear Regulatory Commission
Attn: Director, Office of Nuclear Security and Incident Response
11555 Rockville Pike
Rockville, MD 20852-2738

(2) Send a second copy to the appropriate NRC Regional Office listed in Appendix A to 10 CFR Part 73.

(3) Submit revised reports (i.e., subsequent to the initial written report) to both NRC headquarters and the Regional Office.

(4) Ensure that event reports are legible and of a quality to permit reproduction and processing.

(5) Maintain copies of the report in accordance with 10 CFR 73.71(g)(11) for a period of 3 years from the date of the report.

Licensees are not required to submit followup written reports of suspicious activities made under the provisions of 10 CFR 73.71(d) and paragraph II of Appendix G.

4.4 Security Event Log

Events reportable under the provisions of 10 CFR 73.71(f) and Appendix G, paragraphs IV(a) and (b), should be logged or recorded rather than reported by telephone. These events should be entered in the log as soon as practical after the licensee becomes aware of them, but always within 24 hours, as required. The licensee should initially log the information as received and then summarize it when the event or condition terminates. Since licensees are required to investigate, correct, or respond to any event or condition that threatens nuclear activity or lessens the effectiveness of the security system, the licensee should have included the event details when the entry was made in the log. The events that should be logged are discussed in Section 3 of this guidance.

The NRC does not specify the format and method for maintaining the security event log in regulatory requirements. Events should be included in a security event log that may be hard-copy or preferably in a searchable electronic database. The NRC prefers the use of electronic log maintenance so that the events recorded may be more easily evaluated and analyzed. Licensees should take care in assuring that the protective requirements of 10 CFR 73.21 and 73.22 are maintained for the data records.

Each log must be retained for 3 years after the last entry to that log. Licensees should maintain the following information in the log:

(1) date and time of the event or condition

(2) brief (one-line) description of the event

(3) brief (one-line) description of compensatory measures or corrective actions taken

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

(5) how the event was detected (e.g., alarm, patrol, test, informants, plant staff observations)

(6) reference to more detail when applicable (e.g., Incident Report 06-1234, Surveillance Test 04-2348, plant condition report number)

4.5 Training of Non-Security Staff

Discovery of reportable or recordable events is not limited to members of the security organization. All site employees with unescorted access should receive training to foster awareness and be briefed on their responsibility to immediately notify site security or management personnel of anomalies, failures, degradations, or vulnerabilities of security systems, or suspicious activities. Licensees may provide this training during general plant training and periodic refresher training. Several licensees 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.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC's plans for using this regulatory guide. No backfit is intended or approved in connection with its issuance.

The NRC has issued this draft guide to encourage public participation in its development. Except in those cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the methods to be described in the final guide will reflect public comments and will be used in evaluating (1) submittals in connection with applications for construction permits, standard plant design certifications, operating licenses, early site permits, and combined licenses; and (2) submittals from licensees who voluntarily propose to initiate system modifications if there is a clear nexus between the proposed modifications and the subject for which guidance is provided herein.

REGULATORY ANALYSIS

The regulatory analysis prepared for the amendment of 10 CFR 73.71 and Appendix G of 10 CFR Part 73 provides the regulatory basis for this guide and examines the costs and benefits associated with implementing the rule as described in this guide. A copy of that regulatory analysis is available for inspection and copying (for a fee) at the NRC's Public Document Room (PDR), which is located at 11555 Rockville Pike, Rockville, Maryland. The PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4209, by fax at (301) 415-3548, and by email to PDR@nrc.gov.

BACKFIT STATEMENT

This draft regulatory guide provides licensees and applicants with new guidance that the NRC staff considers acceptable for reporting of safeguards events as set forth in proposed amendments to 10 CFR 73.71 and Appendix G to Part 73. The application of this guide is voluntary. Because certain portions of this regulatory guide do not impose a new or different regulatory position for meeting NRC regulations, the NRC has determined, pursuant to 10 CFR 50.109(a)(3), that the backfit rule does not apply, and that a backfit analysis is therefore not required. For the portions of this regulatory guide provides an acceptable method for implementation of new or different regulatory requirements that would be imposed by proposed 10 CFR 73.71 and Appendix G to Part 73, the NRC has determined, and concluded that the proposed rule and guidance would provide safety and security-related benefits of a substantial increase in the overall protection of the public health and safety, the environment, and the common defense and security. Therefore, the benefits derived from the backfit and that the direct and indirect cost of implementation are justified in view of this increased protection.

GLOSSARY

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

Any failure, degradation, or discovered vulnerability – The performance of a security safeguards measure 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 10 CFR Part 73 requirements, or a discovered defect in such equipment, personnel, or procedures that degrades function or performance which could be exploited for the purpose of committing acts described in Appendix G to 10 CFR Part 73.

Attempts to cause – This means that reliable and substantive information exists that an effort to accomplish the threat, even though it has not occurred or has not been completed because it was interrupted, stopped before completion, or which may occur in more than 2 hours.

Contraband – Materials banned from the protected area by security regulations. Contraband consists of unauthorized firearms, explosives, and incendiary devices that may be carried or concealed by personnel, packages, materials or vehicles.

Credible threat – Credible means information received from a source determined to be reliable (e.g. law enforcement, government agency, etc.) or has been verified to be true. A threat can be verified to be true or considered credible when —

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

Dedicated observer – A person, not necessarily a member of the security force, posted as a temporary compensatory measure for a degraded assessment or detection capability of both. While performing this function, duties must be limited to detection and assessment. As a minimum, the person must be able to view the entire area affected by the degradation and must be able to communicate with the alarm stations. Use of optical and/or electronic surveillance devices is recommended.

Discovery (time of) – A specific time at which a supervisor, or manager makes a determination that a verified degradation of a security safeguards measure or contingency situation exists.

Diversion of SNM (at any level) – Unauthorized removal or control of SNM.

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

Hostile Action – An act directed against an NRC-licensed facility or its personnel that includes the use of violent force to destroy equipment, take hostages, and/or intimidate the licensee to achieve an end. This includes attack by air, land, or water using weapons, explosives, projectiles, vehicles, or other devices used to deliver destructive force. Other acts that satisfy the overall intent may be included.

Interruption of normal operation – A departure from normal operation or condition that, if accomplished, would result in a challenge to the plant safety systems. This may also include an event that causes a significant redistribution of security or safety resources. This could include intentional

tampering with systems or equipment that is normally in standby but would need to operate if called upon.

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

Lost SNM – This means that SNM it is no longer in the possession or control of the party authorized to possess it during a specific time.

Memorandum of Understanding (MOU) – A document detailing the agreement between the licensee and outside Law Enforcement Agencies (at all levels) or Emergency Service agencies (e.g., firefighting, decontamination, medical) for augmentation of site security/safety emergency response or compensatory actions taken to appropriate onsite events (e.g., personnel, equipment, professional assistance).

Nuisance alarm – An 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, lightning) or mechanical conditions (e.g., natural objects such as animals or tall grass).

Prohibited Items – Are items that are not relative to the conduct of work or that do not serve a purposeful function within the environment and are considered contrary to safety and security, which could be used to adversely affect personnel, systems or equipment required to protect SNM. Examples of prohibited items include but are not limited to illegal drugs, alcohol, large knives, ammunition for a firearm, and prescription medication not prescribed for the person in possession (i.e., non-related, prescription drugs).

Properly compensated – Measures, including backup equipment, additional security personnel, or specific procedures, taken to ensure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security-related equipment, 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 may have reason to believe received information 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 which claims responsibility for the threat.

Reliable Source – The source of information is considered trustworthy, authentic or consistent in performance or results.

Security Response – As used in this guide this means the substantive implementation of the armed response capabilities.

Safeguards – This term has historically referred to the two major components of NRC and international required protective components: material control, accounting, and security. The term security usually refers to physical or procedural means of preventing harm to the assets of a facility. Common usage

frequently interchanges the words security and safeguards. The term may also have specific contextual meaning such as "safeguards information" or "Safeguards Event Log."

Security event – Any incident representing an attempted, threatened, or actual breach of the security system or reduction of the operational effectiveness of that system.

Security Event Log – A compilation of log entries for the events described in Paragraph II of Appendix G to 10 CFR Part 73.

Security system – The compilation of all elements that make up the physical protection program necessary to meet 10 CFR Part 73 requirements, such as, equipment, personnel, procedures, and personnel practices to include the way in which each element interacts with and effects other elements.

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

Tampering – Altering for improper purposes or in an improper manner, or intentional unauthorized manipulation of equipment.

Theft of SNM – The unauthorized taking, or controlling of SNM for unauthorized use.

Unaccounted for SNM – This means that material has not been received at its delivery point 4 hours or more after its estimated arrival at the delivery point

Unauthorized person – Any person who gains unescorted access to any area to which the person has not been properly authorized or granted unescorted access. This includes otherwise authorized persons who gain access in an unauthorized manner such as circumventing established access control procedures by tailgating another authorized person.

Uncompensated – This means compensatory measures included in security plans or procedures have either not been implemented, were ineffective, or were implemented incorrectly. To clarify, the aforementioned reports on failure and degradation should include not only mechanical or electrical problems but also failures in procedures or personnel practices or performance.

REFERENCES

1. Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," U.S. Nuclear Regulatory Commission, July 18, 2005.[8]

2. RIS 2006-12, "Endorsement of Nuclear Energy Institute Guidance 'Enhancements to Emergency Preparedness Program for Hostile Action'," U.S. Nuclear Regulatory Commission, July 19, 2006.[9]

3. 71 FR 62644, "Power Reactor Security Requirements," *Federal Register*, Volume 71, Number 207, pp. 62664-62874, Washington, DC, October 26, 2006.[10]

4. NUREG-1022, "Event Reporting Guidelines 10 CFR 50.72 and 50.73," U.S. Nuclear Regulatory Commission, Washington, DC, October 2000.[11]

---

[8] All bulletins listed herein were published by the U.S. Nuclear Regulatory Commission and are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; and email PDR@nrc.gov.

[9] All regulatory issue summaries (RISs) listed herein were published by the U.S. Nuclear Regulatory Commission and are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; and email PDR@nrc.gov.

[10] All *Federal Register* notices listed herein were issued by the U.S. Nuclear Regulatory Commission, and are available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov. Many are also available electronically through the Federal Register Main Page of the public GPOAccess Web site, which the U.S. Government Printing Office maintains at http://www.gpoaccess.gov/fr/index.html.

[11] All NUREG-series reports listed herein were published by the U.S. Nuclear Regulatory Commission,. Most are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/ reading-rm/doc-collections/nuregs/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov. In addition, copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328, telephone (202) 512-1800; or from the National Technical Information Service (NTIS), at 5285 Port Royal Road, Springfield, Virginia 22161, online at http://www.ntis.gov, by telephone at (800) 553-NTIS (6847) or (703)605-6000, or by fax to (703) 605-6900.

BIBLIOGRAPHY

10 CFR Part 73, Appendix G, "Reportable Safeguard Events," U.S. Nuclear Regulatory Commission, Washington, DC.[12]

Generic Letter (GL) 91-03, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, March 6, 1991.[13]

NUREG-1304, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, February 1988.[14]

Regulatory Guide 5.62, "Reporting of Safeguards Events," U.S. Nuclear Regulatory Commission, Washington, DC, November 1987.[15]

---

[12] All NRC regulations listed herein are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/cfr/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov.

[13] The generic letter listed herein was published by the U.S. Nuclear Regulatory Commission, and is available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/nuregs/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov. In addition, copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328, telephone (202) 512-1800; or from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161, online at http://www.ntis.gov, by telephone at (800) 553-NTIS (6847) or (703) 605-6000, or by fax to (703) 605-6900.

[14] All NUREG-series reports listed herein were published by the U.S. Nuclear Regulatory Commission,. Most are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/ reading-rm/doc-collections/nuregs/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov. In addition, copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328, telephone (202) 512-1800; or from the National Technical Information Service (NTIS), at 5285 Port Royal Road, Springfield, Virginia 22161, online at http://www.ntis.gov, by telephone at (800) 553-NTIS (6847) or (703)605-6000, or by fax to (703) 605-6900.

[15] The regulatory guide listed herein was published by the U.S. Nuclear Regulatory Commission. All other regulatory guides are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov. Active guides may also be purchased from the National Technical Information Service (NTIS) on a standing order basis. Details on this service may be obtained by contacting NTIS at 5285 Port Royal Road, Springfield, VA 22161,online at http://www.ntis.gov, by telephone at (800) 553-NTIS (6847) or (703) 605-6000, or by fax to (703) 605-6900. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room (PDR), which is located at 11555 Rockville Pike, Rockville, Maryland; the PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4205, by fax at (301) 415-3548, and by email to PDR@nrc.gov.

Appendix A

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

The purpose of this appendix is to provide further guidance on reporting of suspicious aviation-related activities (required to be reported in 4 hours) that occurs within the airspace in proximity of licensee facilities. Suspicious activity is defined as behavior that may be indicative of intelligence gathering or pre-operational 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 Federal Aviation Administration (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.**

It is recommended that licensees contact their nearest FAA Air Traffic Control (ATC) facility in order to discuss this NOTAM and its relevance to the facility, and to maintain a rapport. [FAA Air Traffic Organization – Air Traffic Control Towers, Terminal Radar Approach Control facilities (TRACON), Air Route Traffic Control Centers (ARTCC) – and Flight Standards District Offices are available on the FAA Web site at http://www.faa.gov.]

Licensees are urged to 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 security managers should exercise judgment/discretion in the determination of whether flight activity is suspicious with respect to normal air traffic patterns, proximity of the facility to local airports and US military bases, the use of rivers and coastal waterways for navigational purposes, local weather conditions, and other unforeseen local circumstances. However, multiple sightings of the same commercial or general aviation aircraft, circling or loitering above or in close proximity to facilities, and/or photographing the facility or surrounding area, should be reported.

It is important that incident reporting be timely and include key information (i.e., aircraft registration number (N-number), physical description of aircraft, observed flight activity, date/time of incident, altitude and direction of flight). The use of special photographic or visual sighting equipment may enhance the capability to more accurately capture pertinent information. (Several websites 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 Government entity — or if it can provide a valid explanation for the flight deviation that satisfies the facility security manager — **then the flight activity need not be reported**

further. However, if the FAA cannot identify the aircraft or a valid flight plan/explanation of activity, then the suspicious flight activity should be immediately reported to local law enforcement and the Federal Bureau of Investigation. **There is no need for licensees to notify the NRC Operations Center in the event of aviation-related activity involving Government aircraft unless deemed suspicious in nature and it cannot be resolved at the local level**. Otherwise, it is requested that suspicious aviation-related activity and incidents be reported to the NRC Operations Center. The NRC continues to work closely with FAA, the Transportation Security Administration and U.S. Northern Command (NORTHCOM)/North American Aerospace Defense Command (NORAD) with respect to these types of suspicious aviation incidents and will conduct additional coordination, if necessary.

Consistent with previous NRC advisories, protocols, and the above guidance, licensees are requested to continue to contact and coordinate with the following organizations with respect to suspicious aviation-related activities or incidents:

(1) local FAA ATC facility/office

(2) local law enforcement agency

(3) local FBI Field Office/Resident Agent

(4) NRC Headquarters Operations Center at 301-816-5100

The NRC will continue to forward pre-coordinated overflight operations to licensees (i.e., waterfowl surveillance operations, power line surveys). Licensees are encouraged to contact organizations in their local area (military, Government, and private sector) that might have activities which impact the airspace in proximity to their facility in order to coordinate and establish a link for advance notification of upcoming activity.