U.S. NUCLEAR REGULATORY COMMISSION

REGULATORY GUIDE RG 5.62, REVISION 3

Issue Date: September 2024
Technical Lead: P. Brochman

PHYSICAL SECURITY EVENT NOTIFICATIONS, REPORTS, AND RECORDS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes methods and procedures that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use by licensees to comply with NRC regulations for implementing the provisions of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials" (Ref. 1).

Applicability

This RG applies to NRC licensees and Agreement State licensees who are subject to the provisions of 10 CFR 73.1200, "Notification of physical security events," 10 CFR 73.1205, "Written follow-up reports of physical security events," and 10 CFR 73.1210, "Recordkeeping of physical security events."

This includes licensees of facilities licensed under either 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 2), or 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 3).

This RG also applies to licensees possessing strategic special nuclear material (SSNM) or special nuclear material (SNM) at facilities licensed under 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material" (Ref. 4), and licensees of radioactive waste storage facilities licensed under 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste" (Ref. 5). In addition, this RG applies to licensees transporting SSNM, SNM, spent nuclear fuel (SNF), and high-level radioactive waste (HLW).

This RG contains a detailed discussion of the applicability of the specific provisions of 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210 to licensees who are subject to 10 CFR Part 50,

---

Written suggestions regarding this guide may be submitted through the NRC's public Web site in the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html., under Document Collections, in Regulatory Guides, at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html, and will be considered in future updates and enhancements to the "Regulatory Guide" series. During the development process of new guides suggestions should be submitted within the comment period for immediate consideration. Suggestions received outside of the comment period will be considered if practical to do so or may be considered for future updates.

Electronic copies of this RG, previous versions of RGs, and other recently issued guides are also available through the NRC's public web site in the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html/under Document Collections, in Regulatory Guides. This RG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under ADAMS Accession Number (No.) ML23299A176. The staff responses to the public comments on DG-5080 may be found under ADAMS Accession No. ML23299A187.

Part 52, Part 70, or Part 72 in Section B, "Discussion," in the subsection "Applicability to Specific Facilities, Materials, and Shipping Activities," and "Agreement State Licensees Not Subject to Notification, Reporting, and Recordkeeping Requirements."

Applicable Regulations

- 10 CFR Part 73 requires licensees to establish and maintain a physical protection system with capabilities for the protection of SSNM and SNM at fixed sites and in transit and of the plants or facilities in which SSNM and SNM are used. This applies to production and utilization facilities, including both operating and decommissioning production reactors, power reactors, non-power reactors, and other non-power production and utilization facilities. It also applies to facilities possessing, and to transportation activities involving, SSNM, SNM, SNF, and HLW.

    - 10 CFR 73.15, "Authorization for use of enhanced weapons and preemption of firearms laws," designates the classes of facilities, radioactive materials undergoing transport, and other property for which license holders are eligible to apply for either stand-alone preemption authority or combined preemption authority and enhanced weapons authority.[1] It contains the requirements for obtaining, possessing, and terminating either authority. These requirements apply only to licensees who voluntarily apply for such authority under Section 161A of the *Atomic Energy Act of 1954* (AEA), as amended (Ref. 6).

    - 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," requires licensees to ensure protection against the unauthorized disclosure of safeguards information (SGI).

    - 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements," identifies specific requirements for the creation, storage, handling, and transmission of SGI.

    - 10 CFR 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance," requires licensees to establish and maintain a physical protection system to minimize the unauthorized removal of SNM.

    - 10 CFR 73.1200 requires licensees to notify the NRC Headquarters Operations Center (HOC) of imminent or actual hostile actions, significant security events, security challenges, and security program failures.

    - 10 CFR 73.1205 requires licensees who have made a notification to the NRC (for most, but not all, of the security events listed under 10 CFR 73.1200) to also submit a written follow-up report on the event to the NRC within 60 days of the initial notification.

    - 10 CFR 73.1210 requires licensees to document certain less significant security events or conditions adverse to security in a written log or corrective action program within 24 hours of their occurrence.

[1] The NRC created the terms "stand-alone preemption authority" and "combined preemption authority and enhanced weapons authority" in 10 CFR 73.15 to clarify the differences and interrelationship between these two authorities under Section 161A of the AEA. RG 5.86, "Preemption Authority, Enhanced Weapons Authority, and Firearms Background Checks," provides further information.

- 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data" (Ref. 7), establishes procedures for obtaining facility security clearances and for safeguarding Secret and Confidential National Security Information (NSI) and Restricted Data (RD) received or developed in conjunction with activities licensed, certified, or regulated by the Commission.

    - 10 CFR 95.39, "External transmission of documents and material," provides specific requirements for the transmission of classified information.

    - 10 CFR 95.57, "Reports," requires, in part, that licensees report any alleged or suspected violation of the RD provisions of the AEA (Ref. 8), the Espionage Act (Ref. 9), or other Federal statutes related to protection of classified information (e.g., the loss or theft of classified NSI or RD, or the deliberate disclosure of classified NSI or RD to unauthorized persons).

- 10 CFR Part 150, "Exemptions and Continued Regulatory Authority in Agreement States and in Offshore Waters under Section 274" (Ref. 10), provides certain exemptions to persons in Agreement States from the licensing requirements contained in Chapters 6, 7, and 8 of the AEA and from the regulations of the Commission imposing requirements upon persons who receive, possess, use, or transfer byproduct material, source material, or SNM in quantities not sufficient to form a critical mass. It also defines activities in Agreement States and in offshore waters over which the regulatory authority of the Commission continues.

    - 10 CFR 150.11, "Critical mass," specifies the maximum quantity of SSNM or SNM that an Agreement State licensee may possess.

    - 10 CFR 150.14, "Commission regulatory authority for physical protection," specifies that Agreement State licensees possessing a Category III quantity of SSNM remain subject to the NRC's physical security requirements under 10 CFR 73.67.

- 32 CFR Part 2001, "Classified National Security Information" (Ref. 11), provides direction to agencies to implement Executive Order 13526, "Classified National Security Information" (Ref. 12).

    - 32 CFR 2001.52, "Emergency authority," provides direction on special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations.

Related Guidance

- NUREG-1304, "Physical Security Event Notifications, Reports, and Recordkeeping" (Ref. 13), issued February 1988, provides further guidance for licensees on notifications, reports, and recordkeeping related to physical security events as required under 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210.[2]

[2] The NRC staff has temporarily withdrawn NUREG-1304. The NRC staff intends to hold a question-and-answer workshop with the public, licensees, and other interested stakeholders following implementation of 10 CFR 73.1200, 73.1205, and 73.1210. This workshop and the development of a revised NUREG 1304 will occur subsequent to the 300-day compliance period for licensees to implement, or request exemptions from the new physical security event notification regulations.

- RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements (U)" (Ref. 14), provides guidance that the NRC staff finds acceptable for use by licensees to comply with the requirements in 10 CFR 73.1(a)(1) (*Not publicly available).*

- RG 5.70, "Guidance for the Application of the Theft and Diversion Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.45 and 73.46 Requirements (U)" (Ref. 15), provides guidance that the NRC staff finds acceptable for use by licensees to comply with the requirements in 10 CFR 73.1(a)(2) (*Not publicly available)*.

- RG 5.86, "Preemption Authority, Enhanced Weapons Authority, and Firearms Background Checks" (Ref. 16), provides guidance and sets forth methods and procedures that the NRC staff finds acceptable for use by licensees to comply with the requirements in 10 CFR 73.15 and 10 CFR 73.17, "Firearms background checks for armed security personnel," implementing the authority provided to the Commission under Section 161A of the AEA.

- RG 5.87, "Suspicious Activity Reports under 10 CFR Part 73" (Ref. 17), provides guidance and sets forth methods and procedures that the NRC staff finds acceptable for use by licensees to comply with the requirements in 10 CFR 73.1215, "Suspicious activity reports."

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated events, and to describe information that the staff needs in its review of applications for licenses. RGs are not NRC regulations; and compliance with RGs is not required. Methods and solutions that differ from those set forth in RGs will be deemed acceptable if supported by a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Part 73 and NRC Form 366 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), approval numbers 3150-0002 and 3150-0104, respectively. Send comments regarding these information collections to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the OMB reviewer at: OMB Office of Information and Regulatory Affairs (3150-0002 and 3150-0104), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

TABLE OF CONTENTS

Page

B. DISCUSSION

Reason for Revision

The NRC staff is issuing Revision 3 to RG 5.62 to address issues raised by industry stakeholders following the publication of the "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications" final rule (Ref. 18, hereafter the enhanced weapons rule) and publication of Revision 2 to RG 5.62 (Ref. 19). The NRC issued Revision 2 to RG 5.62 after promulgating new and updated requirements under 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210 for physical security event notifications, written follow-up reports, and recordkeeping on less significant security events and conditions adverse to security.

After publishing the enhanced weapons rule and Revision 2 to this RG, the NRC staff conducted several public pre-implementation workshops with licensees. The NRC staff also participated in industry-led forums and symposiums in May and June 2023. In these meetings industry stakeholders raised questions about Revision 2 to this RG and identified potential inconsistencies, as well as areas requiring additional clarification to help licensees implement the enhanced weapons rule effectively and efficiently.

Background

The NRC initially issued RG 5.62, "Reporting of Physical Security Events," in February 1981 (Ref. 20). The 1981 RG provided acceptable methods and procedures for use by licensees when notifying the NRC of physical security events. It also provided guidance on the timeliness requirements for such notifications and suggested formats for the notifications and written follow-up reports. The 1981 version of the RG addressed only two classes of physical security events (referred to as safeguards events): "threat-related events" or "loss-of-physical-security-effectiveness events." Depending on the event, telephonic notification to the NRC HOC was required within 1-hour or 24 hours of the time of discovery.

The NRC issued Revision 1 of RG 5.62 in November 1987 (Ref. 21) in conjunction with the issuance of a final rule revising safeguards reporting requirements under 10 CFR 73.71, "Reporting of safeguards events" (52 FR 21651; June 9, 1987). The revised requirements increased the numbers and types of security events that required a 1-hour notification. It also converted the 24-hour telephonic notification requirement into a 24-hour recordkeeping requirement, under which licensees were to record events in a safeguards event log that NRC inspectors could review during onsite inspections. The regulations for physical security event notifications and the guidance in RG 5.62 have remained essentially unchanged since 1987.

Following the terrorist attacks of 2001, the NRC issued voluntary guidance to various licensees suggesting that they expeditiously notify the NRC HOC within 15 minutes of any imminent or actual hostile actions. This guidance highlighted the need for new regulations to address the changing threat environment. Additionally, a licensee's ability to possess enhanced weapons under Section 161A of the AEA resulted in new reporting and recordkeeping requirements under 10 CFR Part 73. For these reasons, the NRC issued Revision 2 of RG 5.62 in March 2023 to incorporate the new regulations for physical security event notifications, written follow-up reports, and recordkeeping for less significant security events or conditions adverse to security.

Timeliness Requirements Structure Based upon Security Significance

The NRC has organized the timeliness requirements for physical security event notifications under 10 CFR 73.1200 using a risk-informed approach that reflects the actual or potential security

significance of the event. This structure reduces impacts on licensees (i.e., in most instances, it gives licensees additional time to complete notifications based on the security significance of the event). The NRC has divided physical security events requiring notifications into two overall categories: those events affecting facilities and events affecting transportation activities. The NRC used broad characterizations to reflect the security significance of these notification requirements. The timeliness requirements for notifications are categorized as follows:

- 15-minutes – This timing enables the NRC to promptly notify other licensees and the U.S. Department of Homeland Security (DHS) National Operations Center of the discovery of:
    - An imminent or actual hostile action against a licensee's facility or shipment of material,
    - The initiation of a security response in accordance with a licensee's safeguards contingency plan or protective strategy based upon an imminent or actual hostile action against a licensee's facility or shipment of material, or
    - A notification to licensee of a potential hostile action or act of sabotage against a licensee's facility or shipment of material that is anticipated within the next 12 hours.
- 1-hour – This timing applies to events in which:
    - A licensee has a reason to believe that a person has committed or caused; or attempted or threatened to commit or cause; a significant security event against a licensee's facility or shipment of material, or
    - A licensee has been notified of a potential hostile action or act of sabotage against a licensee's facility or shipment of material, anticipated within greater than the next 12 hours (i.e., greater than 12 hours from the time the licensee was notified), or the timing is indeterminate.
- 4-hour – This timing applies to events that have caused a security impact at a licensee's facility or involving a licensee's shipment of material.
- 8-hour – This timing applies to events in which a licensee discovers a facility security program failure or a transportation security program failure.

Additionally, for licensees possessing enhanced weapons under 10 CFR 73.15, the NRC has established separate notification requirements for stolen or lost enhanced weapons and receipt of adverse inspection findings or enforcement actions from the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). These requirements include the following:

- 4-hour – This timing applies to notifications to the NRC of the theft or loss of enhanced weapons, after the licensee's immediate notification to the ATF of such theft or loss;
- 24-hour – This timing applies to notifications to the NRC of a licensee's receipt of an adverse inspection finding, enforcement finding, or other adverse notice from the ATF associated with the licensee's possession of enhanced weapons; and
- 48-hour – This timing applies to notifications to the appropriate local law enforcement agency (LLEA) of the theft or loss of enhanced weapons.

Licensees making notifications to the NRC must use the notification process specified in 10 CFR 73.1200(o). The telephone numbers for the NRC HOC are specified in Table 1 in 10 CFR Part 73, Appendix A "U.S. Nuclear Regulatory Commission Offices and Classified Mailing Addresses."

Applicability to Specific Facilities, Materials, and Activities

The regulations in 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210 apply to a range of NRC-licensed facilities, materials, and shipping activities subject to the various physical security program requirements in 10 CFR Part 73. However, not all of the provisions of these regulations apply equally to all of these classes of facilities, materials, and shipping activities. Accordingly, the following information describes the applicability of various provisions of these regulations to the various classes of facilities, materials, and shipping activities:

- The 15-minute notification requirements in 10 CFR 73.1200(a) for events at facilities apply to licensees subject to 10 CFR 73.20, "General performance objective and requirements"; 10 CFR 73.45, "Performance capabilities for fixed site physical protection systems"; 10 CFR 73.46, "Fixed site physical protection systems, subsystems, components, and procedures"; 10 CFR 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste"; or 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." These licensees include the following:

    - Production and utilization facilities licensed under 10 CFR 50.21, "Class 104 licenses; for medical therapy and research and development facilities," and 10 CFR 50.22, "Class 103 licenses; for commercial and industrial facilities" (including both operating and decommissioning production reactors and power reactors),

    - Facilities authorized to possess a Category I quantity of SSNM,

    - Independent spent fuel storage installations (ISFSIs),

    - Monitored retrievable storage installations (MRSs), and

    - Geologic repository operations areas (GROAs).

- The 15-minute notification requirements in 10 CFR 73.1200(b) for events associated with shipping activities apply to licensees who are subject to 10 CFR 73.20; 10 CFR 73.25, "Performance capabilities for physical protection of strategic special nuclear material in transit"; 10 CFR 73.26, "Transportation physical protection systems, subsystems, components, and procedures"; or 10 CFR 73.37, "Requirements for physical protection of irradiated reactor fuel in transit." These include licensees engaged in the following:

    - Transportation of a Category I quantity of SSNM,

    - Transportation of SNF, and

    - Transportation of HLW.

- The 1-hour notification requirements in 10 CFR 73.1200(c) for events at facilities apply to licensees who are subject to the provisions of 10 CFR 73.20; 10 CFR 73.45; 10 CFR 73.46; 10 CFR 73.50, "Requirements for physical protection of licensed activities"; 10 CFR 73.51; 10 CFR 73.55; 10 CFR 73.60, "Additional requirements for physical protection at nonpower reactors"; or 10 CFR 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance." These licensees include the following:

    - Production and utilization facilities licensed under 10 CFR 50.21 and 10 CFR 50.22 (including both operating and decommissioning production reactors, power reactors, and non-power reactors),
    - Facilities authorized to possess a Category I, Category II, or Category III quantity of SSNM,
    - Facilities authorized to possess a Category II or Category III quantity of SNM,
    - Hot cell facilities (for examination of irradiated SNM and SNF and HLW).
    - ISFSIs,
    - MRSs, and
    - GROAs.

- The 1-hour notification requirements in 10 CFR 73.1200(d) for events associated with shipping activities apply to licensees who are subject to 10 CFR 73.20; 10 CFR 73.25; 10 CFR 73.26; 10 CFR 73.27, "Notification requirements"; 10 CFR 73.37; or 10 CFR 73.67. These include licensees engaged in the following:

    - Transportation of a Category I, Category II, or Category III quantity of SSNM,
    - Transportation of a Category II or Category III quantity of SNM,
    - Transportation of SNF, and
    - Transportation of HLW.

- The 4-hour notification requirements in 10 CFR 73.1200(e) for events at facilities apply to licensees who are subject to 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. These licensees include the following:

    - Production and utilization facilities licensed under 10 CFR 50.21 and 50.22 (including both operating and decommissioning production reactors, power reactors, and non-power reactors),
    - Facilities authorized to possess a Category I, Category II, or Category III quantity of SSNM,
    - Facilities authorized to possess a Category II or Category III quantity of SNM,
    - Hot cell facilities (for examination of irradiated SNM and SNF and HLW).

- ISFSIs,
- MRSs, and
- GROAs.

- The 4-hour notification requirements in 10 CFR 73.1200(f) for events associated with shipping activities apply to licensees who are subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, or 10 CFR 73.67. These include licensees engaged in the following:
  - Transportation of a Category I, Category II, or Category III quantity of SSNM,
  - Transportation of a Category II or Category III quantity of SNM,
  - Transportation of SNF, and
  - Transportation of HLW.
- The 8-hour notification requirements in 10 CFR 73.1200(g) for events at facilities apply to licensees who are subject to the provisions of 10 CFR 73.20, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. These licensees include the following:
  - Production and utilization facilities licensed under 10 CFR 50.21 and 10 CFR 50.22 (including both operating and decommissioning production reactors, power reactors, and non-power reactors),
  - Facilities authorized to possess a Category I, Category II, or Category III quantity of SSNM,
  - Facilities authorized to possess a Category II or Category III quantity of SNM,
  - Hot cell facilities (for examination of irradiated SNM and SNF).
  - ISFSIs,
  - MRSs, and
  - GROAs.
- The 8-hour notification requirements in 10 CFR 73.1200(h) for events associated with shipping activities apply to licensees who are subject to the provisions of 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, or 10 CFR 73.67. These include licensees engaged in the following:
  - Transportation of a Category I, Category II, or Category III quantity of SSNM,
  - Transportation of a Category II or Category III quantity of SNM,
  - Transportation of SNF, and

- Transportation of HLW.

- The 1-hour notification requirements in 10 CFR 73.1200(m) for notifications to the NRC of the theft or loss of enhanced weapons apply to those licensees possessing enhanced weapons under the provisions of 10 CFR 73.15.

- The 24-hour notification requirements in 10 CFR 73.1200(n) for notification to the NRC of a licensee's receipt of an adverse inspection finding, enforcement finding, or other adverse notice from the ATF apply to those licensees possessing enhanced weapons under the provisions of 10 CFR 73.15.

- The 48-hour notification requirements in 10 CFR 73.1200(m) for notification to the appropriate LLEA of the theft of loss of enhanced weapons apply to those licensees possessing enhanced weapons under the provisions of 10 CFR 73.15.

- The 60-day reporting requirement in 10 CFR 73.1205(a) for a written follow-up reports by licensees who have made telephonic notifications of security events to the NRC under 10 CFR 1200 apply to licensees who are subject to 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. These licensees include the following:

  - Production and utilization facilities licensed under 10 CFR 50.21 and 10 CFR 50.22 (including both operating and decommissioning production reactors, power reactors, and non-power reactors),

  - Facilities authorized to possess a Category I, Category II, or Category III quantity of SSNM,

  - Facilities authorized to possess a Category II or Category III quantity of SNM,

  - Hot cell facilities (for examination of irradiated SNM and SNF and HLW).

  - ISFSIs,

  - MRSs,

  - GROAs.

  - Licensees transporting a Category I, Category II, or Category III quantity of SSNM,

  - Licensees transporting a Category II or Category III quantity of SNM,

  - Licensees transporting SNF, and

  - Licensees transporting HLW.

- The 24-hour recordkeeping requirements in 10 CFR 73.1210 for less significant physical security events and conditions adverse to security apply to licensees who are subject to 10 CFR 73.20, 10 CFR 73.25, 10 CFR 73.26, 10 CFR 73.27, 10 CFR 73.37, 10 CFR 73.45, 10 CFR 73.46,

10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, 10 CFR 73.60, or 10 CFR 73.67. These licensees include the following:

- Production and utilization facilities licensed under 10 CFR 50.21 and 10 CFR 50.22 (including both operating and decommissioning production reactors, power reactors, and non-power reactors),
- Facilities authorized to possess a Category I or Category II quantity of SSNM,
- Hot cell facilities (for examination of irradiated SNM and SNF and HLW),
- ISFSIs,
- MRSs,
- GROAs,
- Licensees transporting a Category I or Category II quantity of SSNM,
- Licensees transporting SNF, and
- Licensees transporting HLW.

Exceptions and Exemptions to Reporting and Recordkeeping Requirements

The regulations in 10 CFR 73.1205(a)(2) provide licensees with exceptions to the requirement to submit certain written follow-up reports to the NRC following a notification made under 10 CFR 73.1200. These exceptions include the following:

- Notifications made under 10 CFR 73.1200(e)(2) and 10 CFR 73.1200(f)(2) regarding interactions with Federal, State, or local law enforcement agencies,
- Notifications made under 10 CFR 73.1200(m) regarding stolen or lost enhanced weapons (for licensees possessing enhanced weapons under 10 CFR 73.15), or
- Notifications made under 10 CFR 73.1200(n) regarding adverse findings issued by the ATF (for licensees possessing enhanced weapons under 10 CFR 73.15).

The regulations in 10 CFR 73.1205(a)(3) provide licensees with an exception to the written follow-up report requirement of 10 CFR 73.1205 following a notification made to the NRC under 10 CFR 73.1200 when the licensee has retracted that notification. This exception applies only if the licensee has not already submitted a written follow-up report.

The regulations in 10 CFR 73.1210(h) provide an exemption to the recordkeeping requirements of 10 CFR 73.1210 for licensees subject to 10 CFR 73.67, who possess or are transporting a Category III quantity of SSNM or a Category II or III quantity of SNM.

NRC Licensees Not Subject to Notification, Reporting, and Recordkeeping Requirements

The physical security program requirements of 10 CFR Part 73 do not apply to certain facilities, materials, and activities. Therefore, licensees involved with such facilities, materials, or activities. are also

not subject to the physical security event notification, written follow-up reporting, or recordkeeping requirements of 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210; and consequently, this RG does not apply to them. This exception covers the following categories of facilities, materials, and activities:

- Facilities, materials, and activities licensed by the NRC that involve the production, use, storage, or transportation of byproduct materials subject to the requirements of 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material" (Ref. 22);

- Facilities, materials, and activities licensed by the NRC that involve the production, use, storage, conversion, deconversion, or transportation of source materials subject to the requirements of 10 CFR Part 40, "Domestic Licensing of Source Material" (Ref. 23); and

- Facilities, materials, and activities licensed by the NRC that involve the production, receipt, possession, use, storage, or transportation of less than a Category III quantity of SSNM or SNM. This means less than 15.0 grams (g) of nuclear material containing uranium (U)-235 enriched to 20 percent or more, U-233, or plutonium (Pu); less than 1,000 g of U-235 enriched to between 10 to 20 percent; and less than 10,000 g of U-235 enriched to less than 10 percent. Additionally, certain types of nuclear materials listed under in 10 CFR 73.67(b) are exempt from the requirements of 10 CFR 73.67. Consequently, NRC licensees possessing, handling, or using such materials are also exempt from the requirements of 10 CFR 73.1200, 10 CFR 73.1205, or 10 CFR 73.1210.

Agreement State Licensees Not Subject to Notification, Reporting, and Recordkeeping Requirements

Agreement State licensees are not subject to the physical security event notification, written follow-up reporting, or recordkeeping requirements of 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210. Consequently, this RG does not apply to the following:

- Facilities, materials, and activities licensed by an Agreement State that involve the production, use, storage, or transportation of byproduct materials subject to the Agreement State's requirements that are compatible with 10 CFR Part 37;

- Facilities, materials, and activities licensed by an Agreement State that involve the production, use, storage, conversion, deconversion, or transportation of source materials subject to the Agreement State's requirements that are compatible with 10 CFR Part 40; and

- Facilities, materials, and activities licensed by the NRC that involve the production, receipt, possession, use, storage, and transportation of less than a Category III quantity of SSNM that is subject to the Agreement State's requirements that are compatible with 10 CFR Part 70.

An Agreement State licensee cannot be authorized to receive, possess, use, or transport Category II or III quantities of SNM containing low enriched uranium (LEU) or quantities of LEU exceeding the critical mass limit of 10 CFR 150.11(a). An NRC license is required to receive, possess, use, or transport such quantities of LEU, and the holder of such a licensee would nominally be subject to 10 CFR 73.67; and therefore, to the event notification regulations under 10 CFR 73.1200.

However, under 10 CFR 150.14, an Agreement State licensee may be authorized to receive, possess, use, or transport a Category III quantity of SSNM. Such an Agreement State licensee is subject to the security requirements of 10 CFR 73.67 and remains under NRC jurisdiction with respect to security

issues. Accordingly, such a licensee is also subject to the requirements of 10 CFR 73.1200 and 10 CFR 73.1205.

A Category III quantity of SSNM consists of greater than 15 g of U-235 (contained in uranium enriched to 20 percent or greater in the U-235 isotope), U-233, or Pu; but is less than the critical mass limit of 10 CFR 150.11(a).

The critical mass limit means a quantity of SNM that is less than 350 g of U-235, less than 200 g of U-233, less than 200 g of Pu, or less than any combination of these three nuclides using the following unity formula.

$$\left[\left(\frac{grams\ U^{235}}{350}\right)+\left(\frac{grams\ U^{233}}{200}\right)+\left(\frac{grams\ Pu}{200}\right)\right] \leq 1.0$$

Agreement State licensees who are not subject to the requirements of 10 CFR 73.67 (e.g., licensees meeting the exemption criteria in 10 CFR 73.67(b)) are also not subject to the requirements of 10 CFR 73.1200 and 10 CFR 73.1205. Additionally, under 10 CFR 73.1210(h), Agreement State licensees possessing or transporting a Category III quantity of SSNM (pursuant to 10 CFR 73.67) are exempt from the recordkeeping requirements in 10 CFR 73.1210.

Establishment of a Communications Channel with the NRC

Under 10 CFR 73.1200(o)(5) and (o)(7), when a licensee notifies the NRC about events affecting a facility, the NRC HOC may request that the licensee establish and maintain an open and continuous communications channel. If the NRC makes such a request, then the licensee must provide an individual who is knowledgeable about the licensee's security, operations, or emergency response organizations to monitor and respond to the channel. The licensee may staff the channel from a location it deems appropriate and may relocate the individual to another appropriate location, if necessary.

Under 10 CFR 73.1200(o)(6) and (o)(8), when a licensee or its movement control center (MCC) notifies the NRC about events affecting a shipment of material, the NRC HOC may request that the licensee or its MCC establish and maintain an open and continuous communications channel. If the NRC makes such a request, the licensee must provide an individual who is knowledgeable about the licensee's security, operations, or emergency response organizations, or about the MCC, to monitor and respond to the channel. The individual should be knowledgeable about the shipment and the security measures taken to protect it. The licensee or its MCC may staff the channel from a location it deems appropriate and may relocate the individual to another appropriate location, if necessary.

The individual monitoring the communications channel may perform other assigned duties, provided the individual is able to respond to NRC requests for information on the channel.

Notification of Significant Supplemental Information

Under 10 CFR 73.1200(p), a licensee or its MCC who have notified the NRC of a physical security event under 10 CFR 73.1200(a)-(h) and (m)-(n) must notify the NRC of any significant supplemental information that has subsequently been identified, using the notification process specified in 10 CFR 73.1200(o).

Retraction of Previous Physical Security Event Notifications

Under 10 CFR 73.1200(q), a licensee or its MCC may retract a physical security event notification if it subsequently determines the event to be invalid or not reportable under 10 CFR 73.1200, or recharacterizes the event as recordable under 10 CFR 73.1210. If the licensee decides to retract the event, then the licensee or its MCC must notify the NRC HOC of the retraction and the basis for the retraction in accordance with the notification procedures in 10 CFR 73.1200(o).

Reporting of an Emergency Declaration

Under 10 CFR 73.1200(r), a licensee or its MCC who has declared an emergency related to a facility or a shipment of material must make the notifications required by 10 CFR 50.72, "Immediate notification requirements for operating nuclear power reactors"; 10 CFR 63.73, "Reports of deficiencies"; 10 CFR 70.50, "Reporting requirements"; or 10 CFR 72.75, "Reporting requirements for specific events and conditions." The NRC staff expects reporting of an emergency declaration to take precedence over any physical security event notifications required under 10 CFR 73.1200 (e.g., notification of State officials of an emergency declaration) (see also Staff Regulatory Guidance position 7.3 of this RG). Additionally, under 10 CFR 73.1200(s), a licensee with multiple notification obligations (e.g., in an event requiring both an emergency declaration and a physical security event notification) may make all such notifications in a single communication to the NRC HOC.

Elimination of Duplication

A licensee or its MCC must notify the appropriate State authorities and the NRC HOC when declaring an emergency in accordance with the requirements in 10 CFR 50.72, 10 CFR 63.73, 10 CFR 70.50, or 10 CFR 72.75. A licensee or its MCC must also notify the NRC HOC of nonemergency, safety-based events in accordance with the requirements in 10 CFR 50.72,10 CFR 63.73, 10 CFR 70.50, or 10 CFR 72.75. Such events may also include a physical security event requiring notification to the NRC in accordance with 10 CFR 73.1200. As good practice, and consistent with 10 CFR 73.1200(s), the licensee or its MCC may combine these multiple notifications into a single communication to the NRC HOC to eliminate duplication and reduce burden. This flexibility applies only to duplicate notifications to the NRC HOC and does not affect a licensee's or its MCC's responsibility to make required notifications to appropriate State authorities.

Security Events Associated with or Involving Classified Information

The unauthorized disclosure, theft, loss, compromise, or possible compromise of classified NSI or RD must be reported to the NRC HOC in accordance with 10 CFR 95.57. However, a single event may involve both a report of unauthorized disclosure of classified information under 10 CFR 95.57 and a physical security event notification under 10 CFR 73.1200. Licensees and MCCs must communicate any classified details related to physical security event notifications in accordance with 10 CFR 73.1200(o) and Section III of Appendix A to 10 CFR Part 73. Consistent with guidance above on the elimination of duplication, the licensee or its MCC may provide both communications events in a single classified notification to the NRC HOC.

Written Follow-Up Reports

After a licensee or its MCC has made a physical security event notification, the licensee must submit a written follow-up report within 60 days, in accordance with 10 CFR 73.1205. The classes of licensed facilities, material, and transportation activities subject to this regulation are discussed above.

Licensees must comply with the submission criteria of 10 CFR 73.1205(b) when submitting written follow-up reports to the NRC. The licensee must submit such reports through the processes specified in 10 CFR 73.4, "Communications." These submission criteria include the following:

- Licensees subject to 10 CFR 50.73, "Licensee event report system," must submit a written follow-up report using NRC Form 366, "Licensee Event Report (LER)" (Ref. 24).

- Licensees not subject to 10 CFR 50.73 must submit a written follow-up report using a letter format.

- The written follow-up report must contain sufficient information to enable the NRC to analyze and evaluate the event to determine whether follow-up action is needed.

- If significant supplemental information becomes available after a licensee has submitted an initial written follow-up report, then the licensee must submit a revised report. The revised report must include indications of the revisions made and must replace the initial report in its entirety (i.e., the revised report must be complete and not limited to only the supplementary or new information).

- Licensees who have identified errors in a written follow-up report must submit a revised report correcting the errors and indicating the changes made.

Licensees must comply with the content requirements of 10 CFR 73.1205(c) for written follow-up reports. The report must include, at a minimum, the following information:

- A brief abstract describing the major occurrences during the event or condition, including all component or system failures that contributed to the event or condition, and any significant corrective actions taken or planned to prevent recurrence.

- A clear, specific narrative description of what occurred so that a knowledgeable reader conversant with security program requirements can understand the event or condition, including, at a minimum, the following information, as applicable:

    - The date and time the event or condition was discovered,

    - The date and time the event or condition occurred,

    - The affected structures, systems, and components (SSCs), equipment, or procedures,

    - The environmental conditions at the time of the event or occurrence, if relevant,

    - The root cause of the event or condition,

    Note: Additional guidance on discussing the root cause or causes in written follow-up reports may be found in Staff Regulatory Guidance position 17 of this RG.

    - Whether any human performance errors caused or contributed to the event or condition (e.g., personnel errors, inadequate procedures, or inadequate training),

    - Whether any previous events or conditions are relevant to the current event or condition and whether corrective actions were ineffective or insufficient to prevent recurrence,

- Whether this event or condition is a recurring failure of an SSC or a procedure important to security,

Note: The phrase "procedure important to security" often relates to a licensee's procedures that provide detailed directions implementing a security regulatory function or requirement in a licensee's physical security plan.

- What compensatory measures, if any, were implemented in response to the event or condition, and

- When corrective actions to prevent recurrence, if any, were or will be taken.

Licensees are also required to comply with the transmission criteria requirements of 10 CFR 73.1205(d) for written follow-up reports. These include the following:

- The licensee must provide written follow-up reports to 1) an addressee specified in 10 CFR 73.4 and 2) the NRC's Director, Office of Nuclear Security and Incident Response.

- The licensee must transmit written follow-up reports containing classified information to the NRC's Headquarters through a transmission system authorized for the use of classified information under 10 CFR Part 95. This involves secure transmission either to the NRC Headquarters' classified mailing address, or to the NRC Headquarters' secure email address, given in Table 2 and Table 1, respectively, of Appendix A to 10 CFR Part 73. Additionally, reports containing classified information must be created, used, destroyed, stored, marked, labeled, handled, and transmitted in accordance with the licensee's NRC-approved Standard Practices Procedures Plan under 10 CFR Part 95.

- The licensee must transmit written follow-up reports containing SGI to the NRC Headquarters' mailing address given in 10 CFR 73.4, in accordance with the requirements of 10 CFR 73.21 and 10 CFR 73.22. Reports containing SGI must be created, used, destroyed, stored, marked, labeled, handled, and transmitted in accordance with the requirements of 10 CFR 73.21 and 10 CFR 73.22 and the licensee's NRC-approved physical security plan.

Licensees are required to comply with the records retention requirements of 10 CFR 73.1205(e). Licensees must maintain a copy of each written follow-up report as a record for a period of 3 years from the date of the report or until termination of the license, whichever is later (see also the Records Destruction Considerations below).

Recording of Physical Security Events and Conditions Adverse to Security

Licensees are required to record physical security events and conditions adverse to security in accordance with the recordkeeping requirements of 10 CFR 73.1210. Such events and conditions do not require a notification to the NRC. However, the licensee must record such events and conditions with sufficient details to facilitate the licensee's monitoring of the effectiveness of their quality assurance programs, as well as, effective tracking, trending, and performance monitoring of physical security events, conditions adverse to security, and implementation of corrective actions to prevent recurrence.

Under 10 CFR 73.1210(a)(1), licensees must record the physical security events and conditions adverse to security specified in 10 CFR 73.1210(c)-(f). Under 10 CFR 73.1210(a)(3), these events and conditions include, but are not limited to, the following broad categories:

- Human performance errors,
- Failures of licensee or contractor personnel to comply with security procedures,
- Insufficient or inadequate security procedures,
- Security equipment failures and malfunctions,
- Design deficiencies in security SSCs,
- Inadequate or insufficient security SSCs, and
- Events or conditions in which the licensee has implemented compensatory security measures within the required timeframe specified in its physical security plan.

For events or conditions in which a licensee has not implemented compensatory security measures within the required timeframe specified in its physical security plan, the licensee must make an event notification under 10 CFR 73.1200. Accordingly, the licensee should refer to the applicable provisions for physical security event notifications under 10 CFR 73.1200(g) and 10 CFR 73.1200(h).

Licensees must comply with the general requirements of 10 CFR 73.1210(b) when recording physical security events and conditions adverse to security. These requirements include the following:

- Under 10 CFR 73.1210(b)(1), licensees must record these events or conditions within 24 hours of the time of discovery.
- Under 10 CFR 73.1210(b)(3), licensees must record such events and conditions in either a stand-alone safeguards event log, in a corrective action program which is part of the licensee's overall quality assurance program, or both. Licensees must ensure that any SGI or classified information in such reports is created, stored, and handled in accordance with the requirements of 10 CFR 73.21 and 10 CFR 73.22 or 10 CFR Part 95, as applicable.
- Under 10 CFR 73.1210(b)(4), these records must include, but are not limited to, the following data elements, as applicable.
    - The date and time the event or condition was discovered,
    - The date and time the event or condition occurred,
    - The affected SSCs, or procedures,
    - A description of the event or condition,
    - Any relevant environmental conditions at the time of the event or occurrence;
    - The root cause of the event or condition,

    Note: Additional guidance on discussing root cause or causes in security event record keeping may be found in Staff Regulatory Guidance position 18 of this RG.

- Whether any human performance errors caused or contributed to the event or condition, including personnel errors, inadequate procedures, or inadequate training,
- Whether any previous events or conditions are relevant to the current event or condition and whether corrective actions were ineffective or insufficient,
- Whether this event or condition is a recurring failure of an SSC or procedure,
- What compensatory measures, if any, were implemented in response to the event or condition,
- What corrective actions, if any, were or will be taken in response to the event or condition, and
- When corrective actions, if any, were taken.

- Under 10 CFR 73.1210(b)(5) and 10 CFR 73.1210(b)(7), licensees are not required to record physical security events or conditions adverse to security for which a licensee made a physical security event notification under 10 CFR 73.1200.
- Under 10 CFR 73.1210(b)(6) licensees are not required to record physical security events or conditions adverse to security for which a licensee made a suspicious activity report under 10 CFR 73.1215.

Records Retention and Destruction

Under 10 CFR 73.1205(e), licensees must retain a copy of a written follow-up report submitted to the NRC for 3 years or until the license is terminated, whichever is later.

Under 10 CFR 73.1210(b)(2), licensees must retain records of physical security events and conditions adverse to security that were recorded in a safeguards event log or in a corrective action program log for 3 years or until the license is terminated, whichever is later.

Licensees must destroy reports or records that are no longer required to be retained and contain SGI or classified information in accordance with the appropriate destruction procedures for the applicable class of information, as specified in 10 CFR 73.21, 10 CFR 73.22, and 10 CFR Part 95.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA develops Safety Requirements and Safety Guides for protecting people and the environment from harmful effects of ionizing radiation. This system of safety fundamentals, safety requirements, safety guides, and other relevant reports, reflects an international perspective on what constitutes a high level of safety. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission's International Policy Statement (Ref. 25) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. 26). The NRC staff did not identify any IAEA Safety Requirements or Guides with information related to the topic of this RG.

C. STAFF REGULATORY GUIDANCE

This section provides detailed descriptions and examples of the methods and procedures that the NRC staff considers acceptable for use by a licensee or its designated MCC in meeting the physical security event notification, written follow-up reporting, and recordkeeping requirements in 10 CFR 73.1200, 10 CFR 73.1205, and 10 CFR 73.1210.

1. Time of Discovery

In 10 CFR 73.2, "Definitions," the NRC has defined the term "Time of discovery" as follows:

> *Time of discovery* means the time at which a cognizant individual observes, identifies, or is notified of a security-significant event or condition. A cognizant individual is considered anyone who, by position, experience, and/or training, is expected to understand that a particular condition or event adversely impacts security.

The time of discovery is determined by a cognizant individual. Consequently, the licensee's formal determination of the time of discovery of a potential security event or condition by a cognizant individual may differ from the time of initial identification of the event or condition. The concept of time of discovery also applies to the reporting requirements for suspicious activity, as discussed in RG 5.87. These suspicious activity reporting guidance in RG 5.87 are outside the scope of RG 5.62.

The NRC expects that licensees will typically designate a supervisor or manager to function as the cognizant individual. However, the definition is intended to provide licensees with broad flexibility in determining the personnel to be identified and trained as cognizant individuals authorized to make a time of discovery determination. The NRC recommends that, as a good practice, licensees specify in their implementing procedures the personnel who are considered to be "cognizant individuals" responsible for making a time of discovery determination under 10 CFR 73.1200 or 10 CFR 73.1210.

With respect to physical security event notification and recordkeeping, the time of discovery is the starting point for the timeliness requirement for assessing whether an event or condition requires an event notification under 10 CFR 73.1200 or recording under 10 CFR 73.1210, and then submitting the notification or recording it. The NRC prioritizes the prompt submission (e.g., within the timeliness requirements) of such physical security event notifications within the various timeliness specified under 10 CFR 73.1200.

Licensees may take sufficient time and use their best judgment to assess or confirm whether a physical security event or condition requires an event notification to the NRC under 10 CFR 73.1200. For some events or conditions, the licensee may need to perform an analysis and evaluation to determine the need for a notification. However, in such cases, the licensee must reach a reportability conclusion within the timeliness requirement applicable to the event or condition under 10 CFR 73.1200. If a licensee is uncertain whether an event or condition requires a notification, a licensee should notify the NRC within the applicable timeliness requirement. If the licensee subsequently concludes that an event notification was unnecessary, it may retract the notification under 10 CFR 73.1200(q).

For physical security event recordkeeping under 10 CFR 73.1210, the time of discovery serves as the starting point for the 24-hour timeliness requirement for recording an event or condition in the licensee's safeguards event log and/or corrective action program.

2. Malevolent Intent and Credible Bomb Threat Considerations

2.1 Malevolent Intent Considerations

For certain events, a licensee may need to determine whether an individual acted with malevolent intent. Examples of when a licensee may need to make such a determination include, but are not limited to, the following:

- Under 10 CFR 73.1200(c)(1)(i)(C), 10 CFR 73.1200(c)(1)(i)(D), 10 CFR 73.1200(e)(1)(vi), 10 CFR 73.1200(g)(1)(ii), or 10 CFR 73.1200(g)(1)(iii), whether the potential unauthorized operation, manipulation, or tampering event that involved an error that could be due to either human performance or malevolent intent.

- Under 10 CFR 73.1200(e)(1)(iii) or 10 CFR 73.1200(e)(1)(iv), whether the actual or attempted introduction of contraband could have been unintentional or involved malevolent intent.

A licensee may use existing processes, procedures, and/or practices to determine if an event involved malevolent intent. If a licensee concludes that malevolent intent was not present for such events, then the licensee should not submit an event notification under 10 CFR 10 CFR 73.1200. Instead, the licensee should record the event in accordance with the applicable provisions in 10 CFR 73.1210 (see Staff Regulatory Guidance position 18.2).

If a licensee determines that malevolent intent was present, then a notification to the NRC is required under 10 CFR 73.1200. Any licensee analysis and evaluation of whether malevolent intent was present must lead to a reportability conclusion within the timeliness requirement applicable to the event or condition under 10 CFR 73.1200. A licensee should also refer to Staff Regulatory Guidance position 1 on defaulting to notification if no conclusion can be reached within the timeliness limit, and on subsequent retraction of a notification.

Note: The NRC staff considers a licensee's discovery of potential contraband during a search before entrance into the protected area as evidence of positive performance of the licensee's security staff.

2.2 Credible Bomb Threat Considerations

The NRC staff's view is that a licensee may not possess the resources necessary to assess whether a bomb threat is credible within the 15-minute or 1-hour timeliness requirements applicable to a bomb threat. Therefore, a licensee is not required to assess whether the bomb threat is credible before it notifies the NRC. A licensee must notify the NRC of the bomb threat within the applicable timeliness requirement of 10 CFR 73.1200. Under 10 CFR 73.1200(q), a licensee may retract a previous bomb threat event notification if the licensee subsequently receives information from law enforcement or the intelligence community that the threat is not credible. The results of a bomb threat search are considered significant supplemental information (see Staff Regulatory Guidance position 16.3).

3. Exception for Event Notifications Containing Safeguards Information

Under 10 CFR 73.1200(o)(3), notifications that contain SGI may be made to the NRC HOC without using secure communications systems under the exception in 10 CFR 73.22(f)(3), as such notifications are considered emergency or extraordinary conditions. If a licensee has ready access to secure communications equipment, the NRC recommends using that equipment to communicate the

notification containing SGI to the NRC. Secure communications equipment that is appropriate for transmitting classified information is also considered appropriate for transmitting SGI. However, the licensee should not exceed the timeliness requirement for the event notification in an effort to obtain access to secure communications equipment to communicate the notification. The licensee should follow the procedure in Section III of Appendix A to 10 CFR Part 73 to make a notification using secure communications equipment.

The exception in 10 CFR 73.22(f)(3) applies only to notifications associated with actual events. A simulated notification to the NRC related to a security drill, response exercise, or security evaluation is not an emergency or extraordinary condition justifying the use of this exception. Therefore, any such notification should not contain SGI. If SGI must be conveyed in a notification related to a simulated security drill, response exercise, or security evaluation, then the licensee should convey it using secure communications equipment. If an actual emergency or extraordinary condition occurs during a licensee's simulated security drill, response exercise, or security evaluation, the licensee may make use of the exception in 10 CFR 73.22(f)(3), as necessary.

4. Consideration of Other Notifications or Recordings

Licensees should evaluate an event using all of the applicable notification requirements under 10 CFR 73.1200 and the regulatory positions in this RG. A licensee's evaluation should proceed from the applicable guidance in order of priority—that is, from the most urgent notification (shortest timeliness requirement) to the least urgent notification (longest timeliness requirement). If an event requires a notification under multiple requirements with varying time limits, the licensee should make the notification within the shortest applicable timeliness requirement. Finally, if a licensee concludes that a security event does not require a notification to the NRC under 10 CFR 73.1200, the licensee should also evaluate whether the event is instead recordable under 10 CFR 73.1210 or reportable under 10 CFR 73.1215. Staff Regulatory Guidance position 18.2 in this RG provides guidance on recordable events and RG 5.87 provides guidance on reporting suspicious activities.

5. Movement Control Center

For transportation-related activities discussed in this guide, a licensee may use a designated MCC to meet the requirements of 10 CFR 73.1200 and 10 CFR 73.1205. Accordingly, an MCC, acting on behalf of the licensee, may monitor a shipment's position and status, request assistance from LLEA, receive threat information from government agencies, make any required notifications to the NRC, and staff a continuous communications channel (if the NRC requests such a channel under 10 CFR 73.1200(o)). An MCC, acting on behalf of the licensee, may prepare the written follow-up reports required under 10 CFR 73.1205 following an event notification made under 10 CFR 73.1200. The NRC recommends as a good practice that the licensee review and approve these written follow-up reports and any corrective actions before the reports are submitted to the NRC.

6. Considerations for Contraband and Prohibited Items

In 10 CFR 73.2, the term "contraband" is defined, in part, to mean unauthorized firearms, explosives, incendiaries, or other dangerous materials (e.g., disease-causing agents) that can cause acts of sabotage against a licensee's facility. NRC regulations prohibit the introduction of contraband items into a licensee's protected area (PA), vital area (VA), or material access area (MAA). The mention of "other dangerous materials (e.g., disease causing agents)" in the definition was not meant to imply that licensees must have the capability to detect such materials. The NRC staff is evaluating the need for rulemaking to address this issue and has issued Enforcement Guidance Memorandum (EGM)-23-001, "Interim

Guidance for Dispositioning Violations Associated with the Enhanced Weapons, Firearms Background Checks, and Security Event Notification Rule" (Ref. 27), to provide further guidance to NRC staff.

The NRC notes that the physical security program for some classes of licensees do not require the licensee to search for contraband. However, if a licensee discovers contraband – e.g., in the course of other normal security activities – then as a good practice the licensee should submit an event notification under 10 CFR 73.1200(e)(1)(iii).

The definition of contraband in 10 CFR 73.2 is broader for licensees who possess or conduct activities involving classified information or RD. For those licensees, contraband also includes unauthorized electronic devices or unauthorized electronic media that could be used in the act of espionage involving NSI, or the unauthorized communication, transmission, receipt, tampering or disclosure of RD. However, for licensees subject to 10 CFR Part 95, the reporting and recordkeeping requirements of 10 CFR 95.57(a) and (b), respectively, have primacy over the event notification and recordkeeping requirements of 10 CFR 73.1200 and 10 CFR 73.1210, e.g., unauthorized electronic devices or media, and do not need to be duplicated under the requirements of 10 CFR Part 73. An exception to this general guidance would involve an event in which the loss or theft of a classified object (e.g., a classified shape) also involved the loss or theft of SNM contained within the classified object (see Staff Regulatory Guidance position 19).

The NRC does not consider the following items to be contraband, if the items are authorized by facility management and if they are possessed by authorized personnel for legitimate purposes or are stored in authorized secure locations: explosives, explosive devices, incendiary devices, and weapons. Examples include, but are not limited to, weapons possessed by the facility's security personnel as part of their official duties; weapons possessed by local, State, or Federal law enforcement personnel visiting the facility for official purposes; explosive squib valves used in certain types of reactors; and explosive or incendiary devices intended for authorized and legitimate purposes at the facility. The NRC staff recommends as a good practice that any such authorizations by facility management be documented in writing.

Items possessed by authorized persons for authorized purposes associated with a transportation activity outside the facility should not be considered contraband. For example, licensees should not consider the following to be contraband: weapons possessed by local, State, or Federal law enforcement personnel performing escort duties; explosives possessed by law enforcement personnel performing escort duties; weapons possessed by authorized licensee escort personnel; or weapons possessed by vehicle operators under applicable State law. Specifically with respect to a weapon possessed by a vehicle operator who has a valid concealed carry permit, the weapon should not be considered contraband if the operator declares the weapon before entering the PA. Instances in which an armed vehicle operator does not declare the weapon do require an event notification under 10 CFR 73.1200(e), even if the operator has a valid permit.

Under 10 CFR 73.67, licensees possessing Category II and III quantities of SSNM, or Category II and III quantities of SNM, are not required to conduct searches of personnel, packages, or vehicles before they enter the controlled access area (CAA). However, the NRC staff recommends as good practice that licensees voluntarily notify the NRC of the discovery of items inside the CAA that would normally be considered contraband. These voluntary notifications should be made consistent with the timeliness requirements of the applicable contraband event notification provisions in 10 CFR 73.1200(e).

NRC regulations do not define the term "prohibited items." Consequently, licensees may determine what they consider to be prohibited items and where on their site these items are prohibited. The NRC staff recommends as a good practice that licensees clearly specify what items are prohibited and

where on the site they are prohibited, and that they communicate this information to licensee personnel, contactor personnel, and visitors.

7. 15-Minute Notifications

The NRC recognizes that the 15-minute event notification requirement imposes a burden upon a licensee and MCC staff personnel. Accordingly, the NRC has adopted a graded approach that limits the requirements in 10 CFR 73.1200(a) and 10 CFR 73.1200(b) to a narrowly specified group of licensees and to events involving imminent or actual hostile actions or potential hostile actions or acts of sabotage against the licensee's facility, material, or shipment activities.

Such actions or acts of sabotage against an individual licensee may be a precursor to a more general (widespread) attack upon the other NRC-licensed facilities or the Nation's other critical infrastructure sectors. By promptly notifying the NRC of such actions or acts, licensees enable the NRC's HOC to promptly communicate the information to the U.S. Department of Homeland Security's National Operations Center, other Federal agencies, and other potentially affected NRC licensees. Such communications are a vital component of the U.S. Government's overall response to threats against critical infrastructure. The NRC's rapid dissemination of these notifications permits other NRC licensees, Federal facilities, military installations, and critical infrastructure facilities to immediately increase their defensive posture in advance of potential coordinated multiple-target, or multiple-sector, terrorist attacks.

7.1 15-Minute Facility Notifications

The 15-minute event notification requirement applies to imminent or actual hostile actions or attempted acts of sabotage against a licensee's facility or material. Under 10 CFR 73.1200(a)(3), a licensee must provide certain specified information when making a 15-minute notification. Given the urgency of 15-minute notifications, the information they require is a subset of the information required under 10 CFR 73.1200(o).

Examples of imminent or actual hostile actions or attempted acts of sabotage against a licensee's facility or material that warrant notification under 10 CFR 73.1200(a) include, but are not limited to, the following:

(1) The licensee initiates a security response in accordance with its safeguards contingency plan or protective strategy based on an imminent or actual hostile action, act of sabotage, or security condition affecting the licensee's facility or material.

(2) The licensee receives a notification from law enforcement, the intelligence community, or other government officials of a credible threat of a potential hostile action or an act of sabotage against the licensee's facility and the action is expected to occur within the next 12 hours. If the timing of the threat is indeterminate, then the licensee should notify the NRC under the 1-hour notification provisions (see Staff Regulatory Guidance position 8.1). Notification is not required if the NRC itself is the government agency that has informed the licensee of the threat.

(3) A detonation of bulk explosives or of an explosive device occurs at or near the licensee's facility. This includes the use of explosives by ground assault force personnel or the use of a vehicle-borne improvised explosive device (VBIED), either land-based or waterborne. The detonation of bulk explosives or an explosive device authorized by the licensee for legitimate purposes is not an imminent or actual hostile action and does not warrant notification under 10 CFR 73.1200(a).

(4) Unauthorized explosive or incendiary materials are discovered within, or in direct contact with, a building or structure located within the licensee's PA that contains equipment that is safety-related, important to safety, or security-related; hazardous materials; spent nuclear fuel; or HLW.

(5) Unauthorized weapons are fired within the licensee's PA, VA, MAA, or CAA.

(6) Unauthorized weapons are fired from outside of the licensee's facility and the projectiles hit the facility, causing an immediate threat to the facility, to security personnel, or to other personnel.

(7) Unauthorized personnel or vehicles succeed in violently or forcibly penetrating a PA, VA, MAA, or CAA.

(8) Hostages are taken inside the licensee's facility.

(9) Offsite hostage-taking is reasonably determined to be related to facility operations or security functions (e.g., family members of facility personnel have been kidnapped to coerce employees into violating laws, NRC regulations, or the facility's license).

(10) Explosives, explosive devices, or incendiary devices are used to cause, or attempt to cause, radiological sabotage or the theft or diversion of SSNM, SNM, SNF, or HLW.

(11) A vehicle is used to cause an actual or attempted breach or disablement of the licensee's required vehicle barrier system (VBS), for example by attempting to circumvent the VBS or by striking it violently at a high speed. See also Staff Regulatory Guidance position 12.

7.2 15-Minute Shipment Notifications

The 15-minute event notification requirement applies to imminent or actual hostile actions or attempted acts of sabotage against an applicable licensee's shipment activities. Under 10 CFR 73.1200(b)(3), the licensee or its MCC must provide certain specified information when making a 15-minute notification. Given the urgency of 15-minute notifications, the information they require is a subset of the information required under 10 CFR 73.1200(o).

Examples of imminent or actual hostile actions or attempted acts of sabotage against a licensee's shipment activities that warrant notification under 10 CFR 73.1200(b) include, but are not limited to, the following:

(1) The licensee initiates a security response in accordance with its safeguards contingency plan or protective strategy based on an imminent or actual hostile action or act of sabotage against a shipment conducted by the licensee.

(2) The licensee receives a notification from law enforcement, the intelligence community, or other government officials of a credible threat of a potential hostile action or an act of sabotage against a shipment conducted by the licensee and the action is expected to occur within the next 12 hours. If the timing of the threat is indeterminate, then the licensee should notify the NRC under the 1-hour notification provisions (see Staff Regulatory Guidance position 8.2). Notification is not required if the NRC itself is the government agency that has informed the licensee of the threat.

(3) A detonation of bulk explosives or an explosive device occurs at or near a transport vehicle. This includes the use of explosives by ground assault force personnel or the use of VBIEDs.

(4) An incendiary device is ignited against the transport vehicle or the transport package.

(5) There is actual or believed theft or sabotage of a shipment.

(6) Adversaries fire weapons at the transport vehicle(s), and projectiles hit the transport vehicle(s), which causes an immediate threat to the shipment.

(7) Adversaries fire weapons at the transport vehicle(s), and projectiles hit the transport vehicle(s) or escort vehicles, which causes an immediate threat or injury to the shipment's security escorts or the vehicle operators.

(8) Unauthorized personnel succeed in forcibly penetrating a transport vehicle.

(9) Unauthorized personnel succeed in forcibly penetrating a transport package.

(10) Hostages are taken on site (e.g., at the shipping facility, receiving facility, or MCC) or off site, and the hostage-taking is related to the shipment's operations or security.

(11) Offsite hostage-taking is reasonably determined to be related to shipment operations or security functions (e.g., family members have been kidnapped to coerce employees into violating laws, NRC regulations, U.S. Department of Transportation regulations, or the shipping or receiving facility's license or certificate of compliance).

7.3 Precedence of 15-Minute Notifications

Under 10 CFR 73.1200(a) and 10 CFR 73.1200(b), a licensee or its designated MCC must complete a 15-minute notification to the NRC as soon as possible, but within 15 minutes of the time of discovery of an event triggering these notification requirements. However, when a 15-minute notification is required, a licensee's or MCC's request for immediate LLEA assistance, initiation of a contingency response, or notification of State officials as required under the licensee's Emergency Response Plan should take precedence over its physical security event notification to the NRC. Under 10 CFR 73.1200(a)(6) or (b)(6), the notification to the NRC HOC must occur as soon as possible after the LLEA and State notifications are completed, and the contingency response is initiated, even if this exceeds the 15-minute timeliness requirement.

Under 10 CFR 73.1200(o)(5), the NRC has clarified the requirement for a licensee to staff a continuous communications channel following an initial 15-minute notification for facilities and materials. If the NRC HOC requests such a channel, the licensee should establish a continuous communications channel as soon as possible after the NRC's request. The continuous communications channel must be staffed by an individual who is knowledgeable about the licensee's security, operations, or emergency response organizations.

Under 10 CFR 73.1200(o)(6), the NRC has clarified the requirement for a licensee or its designated MCC to staff a continuous communications channel following an initial 15-minute notification for shipping activities. If the NRC HOC requests such a channel, the licensee or its MCC should establish a continuous communications channel as soon as possible after the NRC's request. The continuous communications channel must be staffed by an individual who is knowledgeable about the licensee's security, operations, or emergency response organizations, or by a knowledgeable individual from the

MCC that is monitoring a licensee's shipment. Staff Regulatory Guidance position 16 provides further guidance on communicating event notifications to the NRC HOC.

8. 1-Hour Notifications

Under 10 CFR 73.1200(c) and 10 CFR 73.1200(d), a licensee or its designated MCC must notify the NRC HOC as soon as possible but not later than 1-hour after the time of discovery of certain significant physical security events affecting licensee facilities and shipping activities. The 1-hour event notification requirement applies to those events that pose the greatest risk to the physical security of the facility or shipping activity. The NRC has taken risk into account when determining what constitutes a significant physical security event. This approach reduces the number of notifications that must be made to the NRC within 1-hour. Many of the events that previously required 1-hour notifications now require either 4-hour or 8-hour notifications.

8.1 1-Hour Facility Notifications

The significant physical security events affecting facilities for which notifications must be submitted within 1-hour are identified in 10 CFR 73.1200(c)(1)(i)-(iii). Examples of significant physical security events and related clarifications include, but are not limited to, the following:

(1) The licensee receives notification from law enforcement, the intelligence community, or other government officials of a credible threat of a potential hostile action or act of sabotage, and either action is not expected to occur within the next 12 hours, or the time of occurrence is indeterminate. A licensee is not required to notify the NRC HOC if the NRC itself was the government agency that informed the licensee of the threat.

(2) The licensee directly receives an unsubstantiated bomb threat or threat of sabotage (e.g., a threat lacking corroboration from the NRC, law enforcement, or the intelligence community).

(3) The licensee implements its contingency response plan after learning of the threat of a potential hostile action or act of sabotage, and either the action is not expected to occur within the next 12 hours, or the time of occurrence is indeterminate.

(4) The licensee discovers unauthorized explosive materials, incendiary materials, or an improvised explosive device within the site boundary. (Licensees subject to 10 CFR 73.50, 10 CFR 73.60, and 10 CFR 73.67 must meet the 1-hour notification requirement in 10 CFR 73.1200(c) but are not subject to the 15-minute notification requirement in 10 CFR 73.1200(a)).

(5) A vehicle strikes a component of a required VBS in a manner that is more than a minor accident (i.e., the impact degrades the ability of the VBS to perform its intended functions). See also Staff Regulatory Guidance position 12.

(6) All offsite communications capabilities are lost, and these capabilities are necessary to meet regulatory requirements (e.g., they are specified in the licensee's physical security plan).

(7) All normal and alternate security radio-communications necessary to implement the facility's protective strategy are inoperable.

(8) The licensee loses all alternating current and direct current power to security systems (e.g., powering detection and assessment systems, alarm sensors, electronic locks and keypads, or

security communications systems) that affects the licensee's ability to successfully implement its protective strategy.

Under 10 CFR 73.1200(c)(1)(i)(A), licensees must notify the NRC of the theft or diversion of a Category I, II, or III quantity of SSNM or a Category II or III quantity of SNM. A licensee possessing a Category I quantity of SSNM automatically possesses a lesser included Category II and III quantity of SSNM. Similarly, a licensee possessing a Category II quantity of SNM automatically possesses a lesser included Category III quantity of SNM. The regulatory language in 10 CFR 73.1200(c)(1)(i)(A) requires an event notification for the theft or diversion of any such lesser included quantity of SSNM or SNM. For example, the theft or diversion of a Category III quantity of SSNM from a Category I licensee's facility would require an event notification under 10 CFR 73.1200(c)(1)(i)(A).

Because the quantity limits depend upon the enrichment or nuclide, the NRC staff has provided the following non-inclusive examples of events requiring a 1-hr notification:

(1) For a licensee possessing a Category I quantity of SSNM (e.g., 2.0 kilograms (kg) or more of plutonium), any theft or diversion of a Category III quantity of this SSNM (e.g., more than 15 g of this plutonium).

(2) For a licensee possessing a Category II quantity of SSNM (e.g., 1.0 kg or more of uranium enriched to 92.5 weight percent U-235), any theft or diversion of a Category III quantity of this SSNM (e.g., more than 15 g of this uranium).

(3) For a licensee possessing a Category II quantity of SNM (e.g., 10 kg or greater of uranium enriched to 19.0 weight percent U-235), any theft or diversion of a Category III quantity of this SNM (e.g., more than 1 kg of this uranium).

(4) For a licensee possessing a Category III quantity of SNM (e.g., more than 10 kg of uranium enriched to 5.0 weight percent U-235), any theft or diversion of a Category III quantity of this SNM (e.g., more than 10 kg of this uranium).

Under 10 CFR 73.1200(c)(1)(i)(C), licensees must notify the NRC of unauthorized operation, manipulation, or tampering events involving safety-related SSCs at reactors. Similarly, under 10 CFR 73.1200(c)(1)(i)(D), licensees must notify the NRC of unauthorized operation, manipulation, and tampering events involving items relied upon for safety at Category I SSNM facilities. A licensee is not required to notify the NRC of such an event if the licensee assesses that the event was due to human performance errors and no malevolent intent was present. Any such notification must be completed within 1-hour of discovery, even if the licensee is unable to complete a malevolent intent determination within that timeframe. However, a licensee may retract such a notification under 10 CFR 73.1200(q) if it subsequently determines that there was no malevolent intent.

Note: If a licensee concludes that an event was due to a human performance error and reporting is not required under 10 CFR 73.1200(c)(1)(i)(C) or (D), the licensee should still evaluate whether the event is reportable under 10 CFR 50.72; 10 CFR 70.52, "Reports of accidental criticality"; or 10 CFR 72.74, "Reports of accidental criticality or loss of special nuclear material."

For notifications required under 10 CFR 73.1200(c)(1)(ii), licensees should refer to RG 5.69 or RG 5.70, as applicable, for guidance on whether the quantity of unauthorized explosives meets or exceeds the limits for the facility's adversary characteristics.'

The NRC staff recommends, as good practice, that production facility licensees should notify the NRC of any events involving unauthorized operation, manipulation, or tampering that interrupt normal operations of the facility. Such events may include, but are not limited to, interruptions of the production of SSNM, electricity, and/or process steam.

8.2 1-Hour Shipment Notifications

The significant physical security events affecting shipment activities for which notifications must be submitted within 1-hour are identified in 10 CFR 73.1200(d)(1)(i)-(iv). Examples of significant physical security events and related clarifications include, but are not limited to, the following:

(1) The licensee receives a notification from law enforcement, the intelligence community, or other government officials of a credible threat of a potential hostile action or act of sabotage (including bomb threats) where the threat is not expected to occur within the next 12 hours, or the time of occurrence is indeterminate. A licensee is not required to notify the NRC HOC if the NRC was the government agency that informed the licensee of the threat of a potential hostile action or act of sabotage.

(2) The licensee implements its contingency response plan after learning of the threat of a potential hostile action or act of sabotage, and either the action is not expected to occur within the next 12 hours, or the time of occurrence is indeterminate.

(3) The licensee discovers an actual or suspected explosive or incendiary device, or the detonation or ignition of such a device, in relation to a shipment activity. (Licensees subject to 10 CFR 73.67 must meet the 1-hour event notification requirement in 10 CFR 73.1200(d), but are not subject to the 15-minute notification requirement in 10 CFR 73.1200(b)).

9. 4-Hour Notifications

Under 10 CFR 73.1200(e) and 10 CFR 73.1200(f), for certain physical security events affecting a licensee's facilities or shipping activities, the licensee must submit an event notification to the NRC HOC within 4 hours of the time of discovery of the event. These 4-hour notifications are required for events that are less significant than those subject to the 1-hour notification requirement.

9.1 4-Hour Facility Notifications

The physical security events affecting facilities for which notifications must be submitted to the NRC within 4 hours are identified in 10 CFR 73.1200(e)(1)-(4). Examples of such physical security events and related clarifications include, but are not limited to, the following:

(1) The licensee discovers falsified identification badges, key cards, or other access-control devices that could allow unauthorized personnel entry into a PA, VA, MAA, or CAA.

(2) The security force stages a strike or work slowdown.

(3) The licensee provides information to law enforcement that a licensee employee or contractor may be involved in terrorist or criminal activities, or may be affiliated with a terrorist organization, even if the information is unsubstantiated.

For event notifications under 10 CFR 73.1200(e)(1)(v), authorized weapons are those that are specified in the licensee's physical security plan. Consistent with Staff Regulatory Guidance position 1,

the time of discovery of an event is defined as the time when a cognizant individual determines that an authorized weapon is not in the possession of authorized personnel or in an authorized weapons storage location.

Notes: An authorized weapon that is recovered within the 4-hour timeliness requirement for this event notification should be recorded as an uncontrolled weapon, constituting a decrease in effectiveness events under 10 CFR 73.1210(f) (see Staff Regulatory Guidance position 18.2, example (8)).

Weapons in the possession of on-duty law enforcement, shipment escort personnel, or government personnel while they are present at the licensee's facility are not considered to be uncontrolled authorized weapons.

For event notifications under 10 CFR 73.1200(e)(1)(vi), licensees should notify the NRC of unauthorized operation, manipulation, or tampering events involving security-related SSCs at reactors or security-related systems at Category I SSNM facilities that could prevent the licensee's implementation of its protective strategy for any target set.

For event notifications under 10 CFR 73.1200(e)(3)(i), licensees need not notify the NRC of law enforcement responses for minor incidents at the licensee's facility, such as traffic accidents, or for events for which notifications would otherwise have been submitted under 10 CFR 73.1200(a)-(h) or reported under other NRC regulations, such as 10 CFR 50.72(b)(2)(xi) or 10 CFR 72.75(b)(2).

The NRC staff does not view the presence of law enforcement personnel at the licensee's facility for the purposes of training, security exercises, site familiarization, or coordination activities as an example of LLEA response that requires an event notification under 10 CFR 73.1200(e)(3).

The NRC staff does not view a licensee's reporting of suspicious activities to local, State, or Federal law enforcement or government agencies in accordance with 10 CFR 73.1215 as requiring an event notification under 10 CFR 73.1200(e)(2).

9.2 4-Hour Shipment Notifications

The physical security events affecting shipments for which notifications must be submitted to the NRC within 4 hours are identified in 10 CFR 73.1200(f)(1)-(2). Such physical security events include, but are not limited to, the following:

- Law enforcement receives information that a licensee employee or contractor may be involved in terrorist or criminal activities, or may be affiliated with a terrorist organization, even if the information is unsubstantiated.

Under 10 CFR 73.1200(f)(2), licensees must notify the NRC of an event involving "implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials." The NRC staff does not view routine shipment-related notifications made to local, State, or Tribal officials in accordance with 10 CFR Part 71, "Packaging and Transportation of Radioactive Material" (Ref. 28), 10 CFR Part 73, or NRC Orders as requiring event notification under 10 CFR 73.1200(f)(2). Examples of such communications include, but are not limited to, coordination of escort coverage, advance notification of shipments, notifications of shipment delay, and notification of departure or arrival.

The NRC staff also does not view a licensee's reporting of suspicious activities to local, State, or Federal law enforcement agencies in accordance with 10 CFR 73.1215 as requiring an event notification under 10 CFR 73.1200(f)(2).

10. 8-Hour Notifications

Under 10 CFR 73.1200(g) and 10 CFR 73.1200(h), applicable licensees must submit an event notification to the NRC HOC within 8 hours after the time of discovery of certain security program failures affecting licensee's facilities or shipment activities, respectively. The NRC staff has determined that these security events are not likely to have a significant effect or potential effect on the physical security of a facility or shipment activity.

10.1 8-Hour Facility Notifications

The physical security events affecting facilities that must be reported within 8 hours are set forth in 10 CFR 73.1200(g)(1)(i)-(iii). Examples of such physical security events and related clarifications include, but are not limited to, the following:

(1) The licensee discovers a design flaw in a security system; for example, the failure of a required VBS to reposition to its secure configuration on a loss of power.

(2) The loss of an alarm capability or locking mechanism occurs at a SNM access control point or transfer portal that is not compensated for in accordance with the facility's NRC-approved security plan.

(3) An uncompensated event occurs involving the failure of all PA lighting, or the PA perimeter intrusion detection, assessment, or delay system.

(4) A strike or work stoppage by the security force is anticipated within the next 48 hours.

(5) The licensee discovers improper or inadequate supervision of access-control equipment (e.g., badge fabrication, access-control computers, keys, key card stock, passwords, or cipher codes) that could have allowed an unauthorized individual access into a PA, VA, MAA, or CAA. However, the event did not result in actual or attempted access into such areas by an unauthorized individual (see Staff Regulatory Guidance position 9.1).

Note: This does not include improper or inadequate supervision of access control equipment (e.g., fabricated badges) that are deactivated when an individual exits the facility and must be reactivated to gain entry. For example, an instance of a deactivated access badge being lost outside of the facility would not be reportable.

For notifications required under 10 CFR 73.1200(g)(1)(ii) or (iii), licensees should notify the NRC of unauthorized operation, manipulation, or tampering events involving safety-related SSCs that do not interrupt the normal operations of a power reactor or events involving items relied upon for safety at Category I SSNM facilities that do not result in the interruption of normal operation of the facility or an accidental criticality, respectively.

The NRC staff recommends as a good practice that a licensee for a production reactor facility notify the NRC under 10 CFR 73.1200(g)(1)(ii) of unauthorized operation, manipulation, or tampering events that do not interrupt the normal operations of the facility (i.e., events that affects the normal production of SSNM, electricity, or process steam).

Licensees should not notify the NRC of events under 10 CFR 73.1200(g)(1)(ii) or (iii) in which an otherwise previously trained and qualified individual conducts authorized operations or maintenance activities, and the licensee subsequently determines that the individual's qualifications permitting the activity had lapsed before they conducted the activity. The NRC staff recommends as good practice that such a security-related operations or maintenance event should be recorded under 10 CFR 73.1210(f) as a decrease in effectiveness.

10.2 8-Hour Shipment Notifications

The physical security events affecting shipments for which notifications must be submitted to the NRC within 8 hours are identified in 10 CFR 73.1200(h)(1)(i)-(ii).

11. Notifications for Enhanced Weapons

Under 10 CFR 73.1200(m), applicable licensees who have obtained enhanced weapons under 10 CFR 73.15 must notify the ATF, the NRC HOC, and the applicable LLEA if any of these enhanced weapons are stolen or lost.

Under 10 CFR 73.1200(n), applicable licensees who have obtained enhanced weapons under 10 CFR 73.15 must notify the NRC HOC as soon as possible, and not later than 24 hours after receipt of an adverse action by the ATF regarding the licensee's possession, receipt, transfer, transportation, or storage of enhanced weapons.

11.1 Immediate Notifications for Enhanced Weapons

Under 10 CFR 73.1200(m)(1)(i), licensees possessing enhanced weapons under 10 CFR 73.15 must immediately notify the ATF of the theft or loss of enhanced weapons. At the time of this RGs issuance, the ATF requirement for immediate notification was located in the ATF's regulations under 27 CFR 479.141, "Stolen or Lost Firearms" (Ref. 29). It is a licensee's responsibility to understand and comply with all applicable ATF regulations associated with the possession of enhanced weapons. Consequently, NRC licensees are encouraged to discuss any questions on these notification requirements with the ATF's National Firearms Act (NFA) Division staff. Contact information for the NFA Division appears on the ATF web site: https://www.atf.gov/contact/licensing-and-other-services.

11.2 1-Hour Notifications for Enhanced Weapons

Under 10 CFR 73.1200(m)(1)(ii), licensees possessing enhanced weapons under 10 CFR 73.15 must notify the NRC HOC as soon as possible, and not later than 1-hour after notifying the ATF of the discovery of the theft or loss of any enhanced weapons they possess.

11.3 24-Hour Notifications for Enhanced Weapons

Under 10 CFR 73.1200(n)(1), licensees possessing enhanced weapons under 10 CFR 73.15 must notify the NRC HOC, as soon as possible, and not later than 24 hours after receiving an adverse action by the ATF regarding their possession, receipt, transfer, transportation, or storage of enhanced weapons.

Under 10 CFR 73.1200(n)(1), licensees must notify the NRC of adverse ATF actions that include, but are not limited to, the following:

(1) Adverse inspection findings (e.g., notices of violation, nonconformance, or deficiency);

(2) Enforcement actions (e.g., escalated enforcement, civil penalties, or orders); or

(3) Other adverse notices (specific to the licensee) that would affect the licensee's ability to possess or receive enhanced weapons.

Licensees who have voluntarily obtained a Federal firearms license (FFL) from the ATF (in conjunction with obtaining enhanced weapons under Section 161A of the AEA) must also notify the NRC HOC as soon as possible, but within 24 hours of the receipt of an adverse ATF action regarding the licensee's FFL.

11.4 48-Hour Notifications for Enhanced Weapons

Under 10 CFR 73.1200(m)(1)(iii), licensees possessing enhanced weapons under 10 CFR 73.15 must notify the applicable LLEA as soon as possible, and not later than 48 hours after the time of discovery that any enhanced weapons have been stolen or lost. Licensees must notify LLEA officials by telephone or in person. This approach enables LLEA officials to ask follow-up questions that could mitigate the public safety implications of the theft or loss of enhanced weapons.

When deciding which LLEA to notify, the licensee should consider where the weapons were stolen or lost. The following two examples provide clarification:

(1) If the enhanced weapons are stolen or lost from the storage facility of a training range located away from the licensee's facility, then the licensee should notify the LLEA with jurisdiction over the training facility.

(2) If the enhanced weapons are stolen or lost during the escorting of a shipment a significant distance from the facility (e.g., 1,600 kilometers (994 miles) away) or during the security team's return to its home base by commercial aircraft, then the licensee should notify the LLEA with jurisdiction over the location where the theft or loss occurred or is believed to have occurred.

Since a 48-hr notification to LLEA of stolen or lost enhanced weapons is occurring after the licensee has completed a 1-hr notification to the NRC HOC of the same event, a separate 4-hr notification to the NRC HOC under 10 CFR 73.1200(e)(2) (regarding a notification to LLEA) is not required.

12. Required Vehicle Barrier System

The event notifications requirements under 10 CFR 73.1200(c)(1)(ii) and (e)(1)(viii) refer to a required (VBS). A VBS is considered required if its use at the licensee's facility is necessary to implement the licensee's protective strategy, including the licensee's physical protection program or physical security plan in accordance with the regulatory requirements in 10 CFR Part 73 or NRC orders. Some licensees may establish a VBS in the owner-controlled area (OCA) as part of an early warning system (EWS). If the licensee relies on and takes credit for the OCA EWS VBS in its physical security plan, then this VBS is considered a required barrier.

13. Unauthorized Persons

Under 10 CFR 73.1200(e)(1)(i)-(ii), a licensee must submit an event notification to the NRC HOC for any actual or attempted access to a facility's PA, VA, MAA, or CAA by unauthorized persons. Licensees must also notify the NRC of any actual entry of unauthorized persons into the PA, VA, MAA,

or CAA due to the failure of the facility's security barrier or control systems to prevent an unauthorized person from accessing the licensee's PA, VA, MAA, or CAA. A licensee does not need to submit a notification in those cases in which an individual was improperly granted unescorted access to a facility's PA, VA, MAA, or CAA, because they provided inaccurate or false background information or omitted derogatory information.

An individual who has been improperly approved for unescorted access is not considered an unauthorized person. Instead, the NRC staff recommends that the licensee should record the event under 10 CFR 73.1210(f) as a decrease in effectiveness of the security access control program (see Staff Regulatory Guidance position 18.2, example (1)). The NRC staff also recommends that any events involving an authorized person tailgating into a facility's PA, VA, MAA, or CAA (in noncompliance with a licensee's access control procedures) be recorded under 10 CFR 73.1210(f) as a decrease in effectiveness of the security access control program.

Under 10 CFR 73.1200(e), a licensee is not required to notify the NRC of an actual or attempted entry of unauthorized persons into the licensee's OCA. However, if a licensee determines that the unauthorized person's actual or attempted entry into the OCA constitutes a suspicious activity then, under 10 CFR 73.1215, the licensee must report this suspicious activity. Under 10 CFR 73.1200(e)(2), licensees must notify the NRC of events involving the "implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials." Since suspicious activity reports under 10 CFR 73.1215(c) must report suspicious activities to the applicable LLEA, the FBI, and the NRC HOC, the NRC staff views a separate notification to the NRC under 10 CFR 73.1200(e)(2) (which concerns notifications to law enforcement officials) as duplicative; and therefore, unnecessary.

Under 10 CFR 73.1200(f)(1)(i)-(iv), a licensee must notify the NRC HOC of any unauthorized persons actually gaining or attempting to gain access to a transport vehicle or to the material being transported. The licensee does not need to submit a notification in cases in which an individual was improperly granted unescorted access to a transport vehicle or to the material being transported because they provided inaccurate or false background information or omitted derogatory information. An individual who has been improperly approved for unescorted access is not considered an unauthorized person. Instead, the NRC staff recommends that the licensee should record such instances of improper granting of access under 10 CFR 73.1210(f) as a decrease in effectiveness of the security access control program (see Staff Regulatory Guidance position 18.2, example (1)).

14. Retraction of Event Notifications

Under 10 CFR 73.1200(q), a licensee may retract a physical security event notification made under 10 CFR 73.1200(a)-(h), (m), or (n) that it has determined to be invalid. The licensee may discuss the applicability of a particular notification or recording requirement in 10 CFR 73.1200 or 10 CFR 73.1210 to a specific security event with the NRC staff, if time permits, before making the corresponding notification or record. Contacting the applicable NRC regional office is preferred.

Under 10 CFR 73.1200(q), an MCC that is monitoring a shipment for a licensee may retract a physical security event notification it has made under 10 CFR 73.1200(b), (d), (f), or (h) that it has determined to be invalid.

A licensee or its MCC may base such a determination upon new information or relevant information received from an external entity subsequent to its initial notification. Examples of such a determination include, but are not limited to the following:

(1) An event in which the initial information is subsequently determined to be incorrect, and

(2) An event in which the licensee has used existing processes, procedures, and/or practices to conclude that malevolent intent was not present, but such a conclusion was reached after a notification was submitted to the NRC (see Staff Regulatory Guidance position 2.1).

15. Items Relied Upon for Safety

Several of the notification requirements in 10 CFR 73.1200 refer to events involving unauthorized operation of, manipulation of, or tampering with SSCs. These requirements apply to facilities licensed under 10 CFR Part 70 that use the term "items relied upon for safety" (IROFS). Notification requirements referring to "any SSC" would include IROFS, but these notifications are not limited to IROFS.

The NRC staff did not intend to give the term SSC any new meaning in the final rule or this RG. Its intent was to require notification of unauthorized operation, manipulation, or tampering events affecting any SSCs, not just "safety-related SSCs" as that term is defined in 10 CFR Part 50 or "items relied on for safety" as that term is defined in 10 CFR 70.4, "Definitions."

16. Security Event Notification Process

Under 10 CFR 73.1200(o), licensees must make the event notifications required under 10 CFR 73.1200(a)-(h), (m), and (n) by telephone, within the specified timeliness limits. The timeliness requirement begins at the time of discovery of the event, as this term is defined in 10 CFR 73.2. Staff Regulatory Guidance position 1 contains additional guidance on the term "time of discovery."

Under 10 CFR 73.1200(o)(1) and (2), licensees may use any available communication system to make the telephonic notifications to the NRC HOC as required by 10 CFR 73.1200 within the applicable timeliness requirement. Additionally, under 10 CFR 73.1200(p) and (q), licensees may use any available communication system to notify the NRC of significant supplemental information and retraction of previous notifications.

16.1 Continuous Communications Channel

In response to a licensee's event notification under 10 CFR 73.1200(a)-(h) and (m), the NRC may request that the licensee or its MCC establish a continuous communications channel. The NRC's objective is to rapidly obtain accurate and current information on the security status of an event, especially in the cases of deteriorating facility or security conditions, high-significance events, or high-consequence events.

Under 10 CFR 73.1200(o), a licensee or its MCC may establish a requested communications channel through any available communications system. The licensee or its MCC may place the individual staffing the communications channel at a location it deems appropriate (e.g., an alarm station, technical support center, or emergency operations facility) and may move the individual to another appropriate location, if necessary.

Under 10 CFR 73.1200(o), a licensee must staff the communications channel with an individual knowledgeable about the licensee's operations, security, or emergency response organizations. The individual should be knowledgeable about the facility or shipment, and about the licensee's facility or transportation security procedures, as applicable. An MCC must staff the communications channel with an individual from the MCC, who is knowledgeable about the shipment and the transportation security procedures.

The individual monitoring the communications channel may perform other assigned duties, provided they are able to respond to NRC requests for information on the channel.

16.2 Information Security Considerations During Event Notifications

Consistent with 10 CFR 73.22(f)(3), when making event notifications under 10 CFR 73.1200 concerning actual events that contain SGI, licensees are exempted from the requirement to use secure communications equipment to convey SGI. However, if secure communications equipment is readily available, then the licensee should consider using this secure capability when notifying the NRC on a not to delay basis. Further guidance appears in Section B, under "Event Notification Process," and in Staff Regulatory Guidance position 3. The exemption in 10 CFR 73.22(f)(3) applies only to notifications associated with actual events, not to simulated notifications made by a licensee during a security drill, response exercise, or security evaluation.

Separately, as also discussed under "Event Notification Process" in Section B of this RG, a licensee making an event notification under 10 CFR 73.1200 that contains classified information must transmit the notification to the NRC HOC using secure communications equipment appropriate to the classification level of the information. This requirement applies to both classified NSI and classified RD. Such secure communications equipment must meet the requirements of 10 CFR 95.39. The regulations in 10 CFR Part 95 do not provide exceptions for emergencies or exigent circumstances as 10 CFR 73.22(f)(3) does for SGI. Therefore, even in emergencies, licensees must use secure communications equipment to submit to the NRC any physical security event notifications containing classified information.

However, under 10 CFR 73.1200(o)(4)(ii) and 10 CFR 73.1200(o)(4)(iii), if the licensee's secure communications equipment is unavailable or inoperable (e.g., because of the nature of the security event), then the licensee must provide the NRC HOC with as much information as possible about the event without disclosing classified information in order to meet the timeliness requirements under 10 CFR 73.1200. In addition, the licensee must indicate to the NRC that its secure communications capability is unavailable or inoperable. In such circumstances, if the significance of the ongoing security event necessitates it, the NRC's emergency response manager may direct the licensee, in accordance with 32 CFR 2001.52(a), to provide classified NSI to the NRC over a nonsecure system. However, licensees must only use secure communications capabilities to communicate classified RD (i.e., no exceptions exist for non-secure communication of classified RD).

Under 10 CFR 73.1200(o)(4)(iii), a licensee's follow-up report for an event involving non-secure communication of classified NSI must document this NRC direction and the specific classified NSI that was communicated non-securely. Under 10 CFR 73.1205(d)(2)-(3), the licensee must prepare and submit such a report as a classified document.

16.3 Significant Supplemental Information

Under 10 CFR 73.1200(p), a licensee or its MCC must notify the NRC of significant supplemental information. The length of time required to identify any supplemental information, assess its significance, and conclude that it is significant enough to warrant notification may vary greatly from event to event. Consequently, the NRC staff recommends as a good practice that once a licensee or an MCC has determined that supplemental information is significant, the licensee or MCC should notify the NRC HOC of the supplemental information within a timeframe consistent with the timeliness requirement for the original event notification.

The NRC expects licensees to consider the results of any bomb searches conducted by the licensee or by LLEA search teams as significant supplemental information and to notify the NRC HOC accordingly. The results of bomb searches are only one example of significant supplemental information that should be reported to the NRC.

17. Written Follow-Up Reports

Under 10 CFR 73.1205(a)(1), licensees must submit a written follow-up report within 60 calendar days after making an event notification under 10 CFR 73.1200(a)-(h). However, the regulations in 10 CFR 73.1205(a)(2) identify several exceptions to this requirement. The discussion topic under "Exceptions and Exemptions to Reporting and Recordkeeping Requirements" in Section B of this RG contains details about these exceptions.

Additionally, 10 CFR 73.1205(a)(3) states that a licensee need not submit a written follow-up report for a notification made under 10 CFR 73.1200 if it has subsequently retracted the notification in accordance with 10 CFR 73.1200(q). However, if the licensee has already submitted a written follow-up report, then before retracting the notification, the licensee is required to submit a revised written follow-up report documenting the retraction and the basis for the retraction. Licensees should refer to Staff Regulatory Guidance position 14 for further direction. The revised report is necessary to ensure the completeness of the agency's docketed history of the licensee's communications with the NRC.

The following two examples further clarify the timing considerations associated with this distinction:

(1) On day 0, Licensee A makes an event notification to the NRC under 10 CFR 73.1200(c). If on day 35 the licensee notifies the NRC under 10 CFR 73.1200(q) that it is retracting the event notification, then under 10 CFR 73.1205(a)(3)(i), Licensee A is not required to submit a written follow-up report for this event.

(2) On day 0, Licensee B makes the same event notification to the NRC under 10 CFR 73.1200(c). On day 59 the licensee submits a written follow-up report to the NRC. If on day 85, the licensee notifies the NRC under 10 CFR 73.1200(q) that it is retracting this event notification, then under 10 CFR 73.1205(a)(3)(ii), Licensee B is required to submit a supplemental written follow-up report to the NRC to indicate that the original event notification was retracted and to document the basis for the retraction.

Under 10 CFR 73.1205(b)(2), licensees subject to 10 CFR 50.73 must submit written follow-up reports using NRC Form 366. Licensees not subject to 10 CFR 50.73 (e.g., those specific licensees subject to 10 CFR Part 70 or 10 CFR Part 72) must submit written follow-up reports using a letter format instead of NRC Form 366.

Consistent with the principle of avoiding duplicate communications in 10 CFR 73.1200(s), a licensee may submit a single written follow-up report on notifications required by 10 CFR 73.1200 and by 10 CFR 50.72, 10 CFR 63.73, 10 CFR 70.50, or 10 CFR 72.75. There is no need to provide duplicate written follow-up reports. For example, a licensee that has made a notification under 10 CFR 50.72 and 10 CFR 73.1200 in a single communication may submit a single written follow-up report to comply with the requirements of 10 CFR 50.73 and 10 CFR 73.1205.

A security event requiring a notification under 10 CFR 73.1200 may affect both a reactor facility and a co-located ISFSI facility. Rather than submitting a separate written follow-up report for both types

of facilities, the licensees may submit a single written follow-up report using NRC Form 366. In such circumstances, the licensee should include all applicable docket numbers for the affected facilities.

The NRC staff does not view the regulatory language in 10 CFR 73.1205(c)(3)(v) as requiring a licensee to perform a formal root cause analysis for an event or condition being reported to the NRC. It is sufficient for the licensee to make a good faith effort to identify the proximate cause or causes of the event or condition. The licensee has the discretion to decide whether to complete a formal root cause analysis for an event or condition. An event or condition may have one root cause or multiple root causes. The licensee's report should indicate all of the applicable root causes for the event or condition. For example, for event involving both an incorrect or incomplete procedure and a human performance error, the report should specify that there were two root causes.

In instances where a licensee is not able to identify the root cause or causes of the event or condition within the 60-day timeliness requirement, the licensee should submit the written follow-up report within 60-days but indicate that they are still determining the root cause of the event or condition. The report should provide as much information as available about the cause or causes of the event or condition, as well as all other required information, and should state that a supplemental report will be provided once the final root cause or causes have been determined.

18. Recordable Security Events and Conditions

Under 10 CFR 73.1210, applicable licensees must record physical security events or conditions adverse to security within 24 hours of the time of discovery of such events and conditions. Licensees should refer to Staff Regulatory Guidance position 1 for further guidance on the time of discovery. The specific classes of licensees subject to this recordkeeping requirement are set forth in 10 CFR 73.1210(a)(1). However, certain licensees subject to 10 CFR 73.67 are exempted under 10 CFR 73.1210(h) from the recordkeeping requirements of 10 CFR 73.1210. Additionally, 10 CFR 73.1210(b)(5)-(7) provides several exceptions to the recordkeeping requirements of 10 CFR 73.1210 for certain events or activities.

The NRC staff does not view the regulatory language in 10 CFR 73.1210(b)(4)(i) as requiring a licensee to perform a formal root cause analysis for an event or condition being recorded in either a safeguards event log or a corrective action program. It is sufficient for the licensee to make a good faith effort to identify the proximate cause or causes of the event or condition. The licensee has the discretion to decide whether to complete a formal root cause analysis for an event or condition. An event or condition may have one root cause or multiple root causes. The licensee's record should indicate all of the applicable root causes for the event or condition. For example, for an event involving both an incorrect or incomplete procedure and a human performance error, the record should specify that there were two root causes.

In instances where a licensee is not able to identify the root cause of the event or condition within the 24-hour timeliness requirement, the licensee should record the event or condition within the 24-hour timeliness requirement, but indicate that they are still determining the root cause or causes of the event or condition. The record should provide as much information available about the cause or causes of the event or condition, as well as all other required information, and should state that the record will be supplemented once a final root cause or causes have been determined.

18.1 Facility and Shipment Recordable Events and Conditions

Under 10 CFR 73.1210(c)(1)-(3) and 10 CFR 73.1210(d)(1)-(2), a licensee must record within 24 hours certain physical security events or conditions adverse to security at facilities. Under

10 CFR 73.1210(c)(4)-(7), a licensee must record within 24 hours certain physical security events or conditions during shipment activities. The following clarifications apply to these events and conditions:

(1) For authorized live ammunition events under 10 CFR 73.1210(d)(1), the NRC staff recommends as good practice that licensees should consider a small quantity of ammunition to be 5 rounds or less.

(2) For unauthorized live ammunition events under 10 CFR 73.1210(d)(2)(i), the regulations in 10 CFR 73.1210(d)(2)(ii)-(iv) provide direction on what is meant by the terms "a small quantity of live ammunition" (i.e., 5 rounds or less), "uncontrolled authorized ammunition," and "unauthorized ammunition."

Additionally, the regulations at 10 CFR 73.1210(d)(3)(i)-(ii) provide exemptions to the ammunition recordkeeping requirements in 10 CFR 73.1210(d) for ammunition that is in the authorized possession of law enforcement personnel performing official duties, and for blank ammunition used by the licensee for the purposes of training; or security exercises, drills, or evaluations.

18.2 Recordable Events and Conditions Related to Decreases in Effectiveness

Under 10 CFR 73.1210(f), a licensee must record within 24 hours certain physical security events and conditions, either at facilities or during shipment activities, that are related to decreases in effectiveness of the physical security program described in the licensee's NRC-approved physical security plans. Examples of such events and conditions include, but are not limited to, the following:

(1) An event in which an individual was improperly granted unescorted access because they provided inaccurate or false background information or omitted derogatory information. An individual who has been improperly approved for unescorted access is not considered an unauthorized person. This example encompasses individuals gaining entry into a PA, VA, MAA, or CAA; gaining access to a vehicle transporting a Category I or Category II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW; gaining access to SSNM or SNM; or gaining access to SGI. If indications of tampering, attempted sabotage, or theft or diversion are evident, the licensee should evaluate reportability under the 1-hour or 4-hour event notification requirements (see Staff Regulatory Guidance positions 8 and 9).

Note: For this example, consistent with the guidance in RG 5.66, "Access Authorization Program for Nuclear Power Plants" (Ref. 30), the time of discovery is considered to be the time when the licensee completes an assessment of the individual's intent in providing inaccurate or false background information. In cases of this type, licensees should follow the latter guidance rather than the time of discovery guidance contained in RG 5.62, Staff Regulatory Guidance position 1.

(2) An event in which an individual approved for unescorted access tailgates through a security barrier for a PA, VA, MAA, or CAA in noncompliance with a licensee's access control procedures.

(3) A programmatic breakdown of the licensee's processes or procedures for reviewing criminal history records checks and background information, involving multiple failures to seek or review relevant information that would have yielded an adverse decision on access to a facility, to a transport vehicle, to SSNM or SNM, or to SGI.

(4) An event involving unplanned missed security patrols or checks which resulted in a failure to meet the licensee's NRC-approved physical security plans. This includes patrols or checks that were not accomplished within the require timeframes specified in these physical security plans.

(5) An event involving a loss of control or protection over SGI where there appears to be no evidence of theft or compromise.

(6) An event involving a failure or degradation of PA, VA, MAA, or CAA lighting or illumination, such that the lighting or illumination does not meet regulatory requirements or is inconsistent with the licensee's security plan.

(7) An event involving the full loss of one alarm station's capabilities (for a facility with two alarm stations).

(8) An event involving an uncontrolled authorized weapon within a PA, VA, MAA, or CAA.

(9) An event involving the actual or attempted introduction of contraband at or into a PA, VA, or MAA, and the licensee has assessed that malevolent intent was not present.

(10) Any other threatened, attempted, or committed act, not otherwise defined in 10 CFR 73.1210, that has decreased or could decrease the effectiveness of the facility's or transport system's physical security program below the level committed to in the licensee's NRC-approved physical security plans.

(11) An event involving unauthorized or undetected access to the OCA surrounding the facility (e.g., by a hunter during hunting season) is not required to be recorded under 10 CFR 73.1210. However, licensees should assess under RG 5.87 if such access constitutes suspicious activity that is required to be reported under 10 CFR 73.1215.

(12) An event involving unauthorized manipulation of security equipment, in which the licensee has assessed that malevolent intent was not present.

Note: A licensee must implement compensatory measures to mitigate the effect of physical security events or conditions that decrease the effectiveness of the licensee's security program within certain required timeframes. Under 10 CFR 73.1200(g)(1)(i), if a licensee does not implement timely compensatory measures for certain events or conditions, the licensee must notify the NRC of the event or condition. Under 10 CFR 73.1210(c)(1)-(7), if the licensee does implement timely compensatory measures, then the licensee is not required to notify the NRC under 10 CFR 73.1200 of the event or condition; however, the licensee must instead record the events or conditions identified in 10 CFR 73.1210(c) in a safeguards event log or corrective action program consistent with 10 CFR 73.1210(b)(1).

18.3 Information Security Considerations for Recordkeeping

Under 10 CFR 73.1210(b)(3), a licensee may record physical security events or conditions adverse to security in either a standalone safeguards event log or the corrective action program. Some records on physical security events or conditions may contain SGI or classified information. Under 10 CFR 73.1210(b)(iii), a licensee must ensure that any SGI or classified information contained in such records is created, stored, and handled in accordance with the requirements of 10 CFR 73.21 and 10 CFR 73.22 or 10 CFR Part 95, as applicable. Furthermore, the licensee must ensure that only

individuals with a valid need to know are permitted access to any SGI. Individuals seeking access to classified information contained in such records must have a valid need to know and appropriate security clearance.

Consistent with 10 CFR 73.1210(b)(3)(ii), a licensee choosing to maintain records of physical security events and conditions adverse to security in an uncontrolled corrective action program database must ensure that the records contain sufficient detail and information to permit the licensee to effectively track, trend, and monitor these events or conditions and implement corrective actions to prevent recurrence without revealing SGI or classified information. Under 10 CFR 73.1210(b)(3)(iv), a licensee may choose to bifurcate the information in such records systems so as to maximize the usefulness of their corrective action program while simultaneously compartmentalizing sensitive security information and security vulnerabilities to prevent unauthorized access to SGI or classified information. Thus, for example, a licensee may maintain an uncontrolled corrective action database together with controlled safeguards event log.

19. Events Involving Classified Information

Under 10 CFR 73.1200(t), a licensee must notify the NRC HOC, in accordance with 10 CFR 95.57, of events associated with the deliberate disclosure, theft, loss, compromise, or possible compromise of classified documents, information, or material. A single event may require both a physical security event notification and a classified information event report. For example, some types of SSNM may have physical characteristics or shapes that are considered to be classified information. The loss or theft of such SSNM would be considered both a physical security event requiring notification under 10 CFR 73.1200 and a loss of classified information requiring reporting under 10 CFR 95.57. The NRC staff considers such events to be rare. If the report on such an event contains classified information, then the licensee should report the event to the NRC HOC in accordance with the communication procedure specified in Section III of Appendix A to 10 CFR Part 73.

As a good practice, and consistent with the provisions in 10 CFR 73.1200(s) on eliminating duplication of event notifications, a licensee may make a single communication to the NRC HOC of an event that requires both notification under 10 CFR 73.1200 and reporting under 10 CFR 95.57. When communicating with the NRC HOC, the licensee must identify each regulation under which the licensee is making the communication.

20. Superseded Guidance

The guidance in this RG supersedes the following previous NRC guidance documents on physical security event notifications, in particular, with respect to emergency response notifications for security-based events and hostile actions.

(1) Bulletin 2005-02, “Emergency Preparedness and Response Actions for Security-Based Events” dated July 18, 2005 (Ref. 31),

(2) Regulatory Issue Summary 2006-12, “Endorsement of Nuclear Energy Institute Guidance ‘Enhancements to Emergency Preparedness Program for Hostile Action,’” dated July 19, 2006 (Ref. 32), and

(3) Generic Letter 1991-03, “Reporting of Safeguards Events,” dated March 6, 1991 (Ref. 33).

D. IMPLEMENTATION

The NRC staff may use this RG as a reference in its regulatory processes, such as licensing, inspection, or enforcement. The NRC staff does not expect or plan to require the use of this RG. However, should the NRC determine to require the use of this RG, such an imposition would not constitute backfitting, as that term is defined in 10 CFR 50.109, "Backfitting," 10 CFR 70.76, "Backfitting," or 10 CFR 72.62, "Backfitting"; affect the issue finality of an approval issued under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"; or constitute forward fitting, as that term is defined in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. 34), because reporting requirements are not included within the scope of the NRC's backfitting or issue finality rules or forward fitting policy.

GLOSSARY

authorized weapon	A weapon specified under the licensee's physical security plan that is in the possession of licensee security personnel or is stored in an armory or ready-service locker, alternatively, A service weapon in the possession of Federal, State, or local law enforcement personnel.
classified National Security Information (NSI)	Has the same meaning as given in 10 CFR 95.5, "Classified National Security Information means information that has been determined under E.O. 13526, as amended, or any predecessor or successor order to require protection against unauthorized disclosure and that is so designated."
classified Restricted Data (RD)	Has the same meaning as given in 10 CFR 95.5, "Restricted data means all data concerning design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Act."
cognizant individual	An individual designated by a licensee who has the requisite experience, and/or training, and who is expected to understand that a particular condition or event requires a physical security event notification or recordkeeping under 10 CFR 73.1200 or 10 CFR 73.1210.
condition adverse to security	Any failure or deficiency affecting the licensee's physical protection program that is recorded under 10 CFR 73.1210 in the licensee's corrective action program and/or safeguards event log. The term "condition adverse to security" and the term "security-related conditions adverse to quality" are considered equivalent for the purposes of implementing the requirements of 10 CFR Part 73, Subpart T.
controlled access area (CAA)	Has the same meaning given in 10 CFR 73.2, "Definitions." This type of area is specified under the security provisions of 10 CFR 73.67 or NRC orders for licensees possessing a Category II or Category III quantity of SNM. The term "controlled access area" (as used in 10 CFR Part 73) is different from the term "controlled area," which is defined in 10 CFR 72.3, as an area in which "ISFSI or MRS operations are performed" (see 10 CFR 72.106).
contraband	Unauthorized firearms, explosives, incendiaries, or other dangerous materials (e.g., disease-causing agents), that can be used to commit acts of sabotage against a licensed facility or licensed radioactive material, as specified under 42 U.S.C. 2284. Contraband items are banned from a licensee's PA, VA, and MAA. For licensees that possess or conduct activities involving classified NSI or classified RD, as defined in 10 CFR 95.5, contraband also means unauthorized electronic devices or unauthorized electronic media that are capable of facilitating acts of espionage; unauthorized communication, transmission, disclosure, or receipt of RD; or tampering with RD, pursuant to 18 U.S.C. 793 or 42 U.S.C. 2274-2276.
enhanced weapon	Any short-barreled shotgun, short-barreled rifle, or machine gun authorized under 10 CFR 73.15. Enhanced weapons do not include destructive devices as defined in 18 U.S.C. 921(a) (Ref. 35).

geologic repository operations areas (GROAs)	Has the same meaning as given in 10 CFR 63.2, "Geologic repository operations area means a high-level radioactive waste facility that is part of a geologic repository, including both surface and subsurface areas, where waste handling activities are conducted."
greater than Class C waste (GTCC)	Has the same meaning as given in 10 CFR 72.3, "Greater than Class C waste or GTCC waste means low-level radioactive waste that exceeds the concentration limits of radionuclides established for Class C waste in § 61.55 of this chapter."
high-level radioactive waste (HLW)	Has the same meaning as given in 10 CFR 72.3, "High-level radioactive waste or HLW means (1) the highly radioactive material resulting from the reprocessing of spent nuclear fuel, including liquid waste produced directly in reprocessing and any solid material derived from such liquid waste that contains fission products in sufficient concentrations; and (2) other highly radioactive material that the Commission, consistent with existing law, determines by rule requires permanent isolation."
hostile action	An act directed at a licensee's facility, shipment, or personnel that includes the use of force to damage or destroy the facility or shipment, divert or steal SNM or radioactive material, take hostages, or intimidate the licensee into violating its NRC license or NRC regulations. This includes attacks using guns, explosives, projectiles, vehicles, or other devices to deliver destructive force. A hostile action should not be construed to include protests or other acts of civil disobedience.
hostile force	One or more individuals who are engaged in an assault directed at a licensee's facility, shipment, or personnel.
imminent	An event or condition that is likely to occur within the time periods specified in 10 CFR 73.1200(a), (b), (c), and (d).
independent spent fuel storage installation (ISFSI)	Has the same meaning as given in 10 CFR 72.3, "Independent spent fuel storage installation or ISFSI means a complex designed and constructed for the interim storage of spent nuclear fuel, solid reactor-related GTCC waste, and other radioactive materials associated with spent fuel and reactor-related GTCC waste storage. An ISFSI which is located on the site of another facility licensed under this part or a facility licensed under part 50 of this chapter and which shares common utilities and services with that facility or is physically connected with that other facility may still be considered independent."
material access area (MAA)	Has the same meaning as given in 10 CFR 73.2, "This type of area is specified under the security provisions of 10 CFR 73.46 or NRC orders for licensees possessing a Category I quantity of SSNM."
movement control center (MCC)	Has the same meaning as given in 10 CFR 73.2, "Movement control center means an operations center which is remote from the transport activity and which maintains position information on the movement of special nuclear material or radioactive material; receives reports of actual or attempted attacks, thefts, or sabotage; provides a means for notifying these and other problems to the NRC and appropriate agencies; and can request and coordinate appropriate aid."

monitored retrievable storage installations (MRSs)

Has the same meaning as given in 10 CFR 72.3, as derived from the Nuclear Waste Policy Act of 1982, as amended. "Monitored Retrievable Storage Installation or MRS means a complex designed, constructed, and operated by DOE for the receipt, transfer, handling, packaging, possession, safeguarding, and storage of spent nuclear fuel aged for at least one year, solidified high-level radioactive waste resulting from civilian nuclear activities, and solid reactor-related GTCC waste, pending shipment to a HLW repository or other disposal."

production facility

Has the same meaning as given in 10 CFR 50.2, "Production facility means:

(1) Any nuclear reactor designed or used primarily for the formation of plutonium or uranium-233; or

(2) Any facility designed or used for the separation of the isotopes of plutonium, except laboratory scale facilities designed or used for experimental or analytical purposes only; or

(3) Any facility designed or used for the processing of irradiated materials containing special nuclear material, except (i) laboratory scale facilities designed or used for experimental or analytical purposes, (ii) facilities in which the only special nuclear materials contained in the irradiated material to be processed are uranium enriched in the isotope U-235 and plutonium produced by the irradiation, if the material processed contains not more than 10^{-6} grams of plutonium per gram of U-235 and has fission product activity not in excess of 0.25 millicuries of fission products per gram of U-235, and (iii) facilities in which processing is conducted pursuant to a license issued under parts 30 and 70 of this chapter, or equivalent regulations of an Agreement State, for the receipt, possession, use, and transfer of irradiated special nuclear material, which authorizes the processing of the irradiated material on a batch basis for the separation of selected fission products and limits the process batch to not more than 100 grams of uranium enriched in the isotope 235 and not more than 15 grams of any other special nuclear material."

prohibited items

Devices, items, and materials that the licensee has determined are not permitted in the PA, VA, or MAA. Prohibited items do not include contraband. The licensee may specify any prohibited items in its physical security plan or implementing procedures.

protected area (PA)

Has the same meaning as given in 10 CFR 73.2, "Protected area means an area encompassed by physical barriers and to which access is controlled."

security condition

Any security event listed in the approved security contingency plan that constitutes a threat to or compromise of facility or transportation security, a threat to facility or transportation personnel, or a potential degradation of the level of safety of the facility or transportation system.

security event

Any occurrence that represents an attempted, threatened, or actual breach of the security system, or a reduction in the physical protection program for the facility or transportation system. Security events may be security incidents, security conditions or hostile actions.

security incident

Any security event listed in the approved security contingency plan that may result in communication with an LLEA or draw media attention.

spent nuclear fuel (SNF) or spent fuel	Has the same meaning as given in 10 CFR 73.2, "Spent nuclear fuel (SNF) or spent fuel means the fuel that has been withdrawn from a nuclear reactor following irradiation and has not been chemically separated into its constituent elements by reprocessing. Spent nuclear fuel includes the special nuclear material, byproduct material, source material, and other radioactive materials associated with a fuel assembly."
Time of discovery	Has the same meaning as given in 10 CFR 73.2, "The time of discovery begins the timeliness requirement for assessing whether an event or condition requires an event notification under 10 CFR 73.1200 or recording under 10 CFR 73.1210, and then accomplishing those actions. The time of discovery is only made by a cognizant individual. Consequently, the time of initial identification of a potential security event or condition may be different than the formal time of discovery determination made by a cognizant individual."
uncompensated	A situation that exists when compensatory measures specified in applicable security plans or procedures have not been implemented, were implemented incorrectly, or were ineffective.
uncontrolled authorized weapon	An authorized weapon in accordance with the licensee's security plan that is neither in the possession of authorized personnel nor in an authorized weapons storage location.
unsubstantiated threat	A threat for which no specific organization or individual claims responsibility and that is not supported by any evidence other than the threat message itself.
vehicle barrier system	A continuous barrier, which may include buildings, natural barriers, commercially available barriers, and any combination of these items, utilized to stop a land vehicle used as transportation to gain proximity to vital areas or used to transport a bomb (i.e., a VBIED).
vital area (VA)	Has the same meaning as given in 10 CFR 73.2, "Vital area means any area which contains vital equipment."

Notes:

1) For additional security terms, users may consult NUREG-2203, "Glossary of Security Terms for Nuclear Power Reactors," issued February 2017 (Ref. 36).

2) The terms "ammunition," "handgun," "rifle," "machine gun," "large-capacity ammunition feeding device," "semiautomatic assault weapon," "short-barreled shotgun," "short-barreled rifle," and "shotgun" have the same meaning as provided in the ATF's regulations under 27 CFR 478.11, "Meaning of terms" (Ref. 37).

REFERENCES [3]

1 *U.S. Code of Federal Regulations* (CFR), "Physical Protection of Plants and Materials," Part 73, Chapter I, Title 10, "Energy."

2 CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

3 CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter I, Title 10, "Energy."

4 CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Chapter I, Title 10, "Energy."

5 CFR, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste," Part 72, Chapter I, Title 10, "Energy."

6 *Atomic Energy Act of 1954* (AEA), as amended, Section 161A, "Use of firearms by security personnel," Title 42, *United States Code* (42 U.S.C.), Chapter 23, Division A, Subchapter XIII, 2201a.

7 CFR, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," Part 95, Chapter I, Title 10, "Energy."

8 AEA, Section 224, "Communication of Restricted Data;" Section 225, "Receipt of Restricted Data;" and Section 226, "Tampering with Restricted Data;" 42 U.S.C., Chapter 23, Division A, Subchapter XVII, "Enforcement of Chapter," 2274-2276.

9 18 U.S.C. Section 793, "Gathering, transmitting or losing defense information," Part I, Chapter 37, "Espionage and Censorship."

10 CFR, "Exemptions and Continued Regulatory Authority in Agreement States and In Offshore Waters Under Section 274," Part 150, Chapter I, Title 10, "Energy."

11 CFR, "Classified National Security Information," Part 2001, Chapter XX, Subtitle B, Title 32, "National Defense."

[3] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. For problems with ADAMS, contact the Public Document Room staff at 301-415-4737 or (800) 397-4209, or email pdr.resource@nrc.gov. The NRC Public Document Room (PDR), where you may also examine and order copies of publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

The NRC withdrew NUREG-1304, Revision 0, upon the publication of the agency's final rule on "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications." Revision 1 of NUREG-1304 will be issued after a public question-and-answer workshop, which will take place after the extended compliance (implementation) period and any exemptions for the final rule.

Licensees with a need to know may request non-publicly available documents listed herein through their cognizant NRC licensing project manager.'

12 Executive Order (E.O.) 13526, "Classified National Security Information," issued December 29, 2009, *Federal Register*, Vol. 75, No. 2: pp. 707-731 (75 FR 707), Washington, DC, January 5, 2010.

13 U.S. Nuclear Regulatory Commission (NRC), NUREG-1304, "Physical Security Event Notifications, Reports, and Recordkeeping," Washington, DC, February 1988 (ML16012A188). (See footnote on previous page)

14 NRC, Regulatory Guide (RG) 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements (U)," Washington, DC. *(Not publicly available)* (See footnote on previous page)

15 NRC, RG 5.70, "Guidance for the Application of the Theft and Diversion Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.45 and 73.46 Requirements (U)," Washington, DC. *(Not publicly available)* (See footnote on previous page)

16 NRC, RG 5.86, "Preemption Authority, Enhanced Weapons Authority, and Firearms Background Checks," Washington, DC.

17 NRC, RG 5.87, "Suspicious Activity Reports Under 10 CFR Part 73," Washington, DC.

18 NRC, "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule," [final rule] *Federal Register*, Vol. 88, No. 49: pp. 15864-15899 (88 FR 15864), Washington, DC, March 14, 2023.

19 NRC, RG 5.62, Revision 2, "Physical Security Event Notifications, Reports, and Records," Washington, DC, March 2023 (ML17131A285).

20 NRC, RG 5.62, Revision 0, "Reporting of Physical Security Events," Washington, DC, February 1981 (ML12187A729).

21 NRC, RG 5.62, Revision 1 "Reporting of Safeguards Events," Washington, DC, November 1987 (ML003739271).

22 CFR, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," Part 37, Chapter I, Title 10, "Energy."

23 CFR, "Domestic Licensing of Source Material," Part 40, Chapter I, Title 10, "Energy."

24 NRC, Form 366, "Licensee Event Reports (LER)," Washington, DC.

25 NRC, "Nuclear Regulatory Commission International Policy Statement," *Federal Register*, Vol. 79, No. 132: pp. 39415-39418 (79 FR 39415), Washington, DC, July 10, 2014.

26 NRC, Management Directive (MD) 6.6, "Regulatory Guides," Washington, DC, May 2, 2016.

27 NRC, Enforcement Guidance Memorandum (EGM-23-001), "Interim Guidance for Dispositioning Violations Associated with the Enhanced Weapons, Firearms Background Checks, and Security Event Notification Rule," Washington, DC, December 5, 2023 (ML23312A221).

28 CFR, "Packaging and Transportation of Radioactive Material," Part 71, Chapter 1, Title 10, "Energy."

29 CFR, "Machine Guns, Destructive Devices, and Certain Other Firearms," Part 479, Subpart J, Subchapter B, Chapter II, Title 27, "Alcohol, Tobacco Products and Firearms." (27 CFR 479.141, "Stolen or lost firearms")

30 RG 5.66, "Access Authorization Program for Nuclear Power Plants," Washington, DC.

31 NRC, Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," Washington, DC, July 18, 2005 (ML051740058).

32 NRC, Regulatory Issue Summary 2006-12, "Endorsement of Nuclear Energy Institute Guidance 'Enhancements to Emergency Preparedness Program for Hostile Action,'" Washington, DC, July 19, 2006 (ML061530290).

33 NRC, Generic Letter 1991-03, "Reporting of Safeguards Events," Washington, DC, March 6, 1991.

34 NRC, MD 8.4, "Management of Backfitting, Forward Fitting, Issue Finality and Information Requests," Washington, DC, September 20, 2019.

35 18 U.S.C. Section 921, "Definitions," Part I, Chapter 44, "Firearms."

36 NRC, NUREG-2203, "Glossary of Security Terms for Nuclear Power Reactors," Washington, DC, February 2017 (ML17047A669).

37 CFR, "Commerce in Firearms and Ammunition," Part 478, Chapter II, Subchapter B, Title 27, "Alcohol, Tobacco Products and Firearms."