(1) Production or utilization facilities;

(2) High-level waste storage or disposal facilities and independent spent fuel storage installations;

(3) Uranium enrichment, uranium conversion, or nuclear fuel fabrication facilities.

(b)(1) Licensees or certificate holders operating facilities described in paragraph (a) of this section that have a protected area shall conspicuously post notices at every vehicle and pedestrian entrance to the protected area.

(2) Licensees or certificate holders operating facilities described in paragraph (a) of this section that include buildings not within a protected area that nonetheless contain special nuclear material, byproduct material, or source material shall conspicuously post notices at the personnel and vehicle entrances to each such building, except with respect to buildings for which no security plan is required under this part.

(3) The required notices must state: ''The willful unauthorized introduction of any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property into or upon these premises is a Federal crime. (42 U.S.C. 2278a.)''

(4) Every notice posted under this section must be easily readable day and night by both pedestrian and vehicular traffic entering the facility or installation.

(5) These notices may be combined with other notices.

(c) This section does not apply to facilities that, in addition to being regulated by the NRC under a license or certificate of compliance issued by the Commission, are also covered by U.S. Department of Energy regulations imposing criminal penalties, and associated posting requirements, under section 229 of the Atomic Energy Act with respect to unauthorized introduction of dangerous weapons, explosives, or other dangerous instruments or materials likely to produce substantial injury or damage to persons or property.

[74 FR 52674, Oct. 14, 2009]

§ 73.77 Cyber security event notifications.

(a) Each licensee subject to the provisions of § 73.54 shall notify the NRC Headquarters Operations Center via the Emergency Notification System (ENS), in accordance with paragraph (c) of this section:

(1) Within one hour after discovery of a cyber attack that adversely impacted safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions within the scope of § 73.54.

(2) Within four hours:

(i) After discovery of a cyber attack that could have caused an adverse impact to safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that could have compromised support systems and equipment, which if compromised, could have adversely impacted safety, security, or emergency preparedness functions within the scope of § 73.54.

(ii) After discovery of a suspected or actual cyber attack initiated by personnel with physical or electronic access to digital computer and communication systems and networks within the scope of § 73.54.

(iii) After notification of a local, State, or other Federal agency (e.g., law enforcement, FBI, etc.) of an event related to the licensee's implementation of their cyber security program for digital computer and communication systems and networks within the scope of § 73.54 that does not otherwise require a notification under paragraph (a) of this section.

(3) Within eight hours after receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer and communication systems and networks within the scope of § 73.54.

(b) *Twenty-four hour recordable events.* (1) The licensee shall use the site corrective action program to record vulnerabilities, weaknesses, failures and deficiencies in their § 73.54 cyber security program within twenty-four hours of their discovery.

(2) The licensee shall use the site corrective action program to record notifications made under paragraph (a) of this section within twenty-four hours of their discovery.

(c) *Notification process.* (1) Each licensee shall make telephonic notifications required by paragraph (a) of this section to the NRC Headquarters Operations Center via the ENS. If the ENS is inoperative or unavailable, the licensee shall make the notification via a commercial telephone service or other dedicated telephonic system or any other methods that will ensure a report is received by the NRC Headquarters Operations Center within the timeframe. Commercial telephone numbers for the NRC Headquarters Operations Center are specified in appendix A to this part.

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

(3) Notifications required by this section that contain Safeguards Information and/or classified national security information and/or restricted data must be made to the NRC Headquarters Operations Center using secure communications systems appropriate to the sensitivity/classification level of the message. Licensees making these types of telephonic notifications must contact the NRC Headquarters Operations Center at the commercial numbers specified in appendix A to this part and request a transfer to a secure telephone.

(i) If the licensee's secure communications capability is unavailable (e.g., due to the nature of the security event), the licensee must provide as much information to the NRC as is required by this section, without revealing or discussing any Safeguards Information and/or Classified Information, in order to meet the timeliness requirements of this section. The licensee must also indicate to the NRC that its secure communications capability is unavailable.

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

(4) For events reported under paragraph (a)(1) of this section, the NRC may request that the licensee maintain an open and continuous communication channel with the NRC Headquarters Operations Center.

(5) Licensees desiring to retract a previous security event report that has been determined to not meet the threshold of a reportable event must telephonically notify the NRC Headquarters Operations Center and indicate the report being retracted and basis for the retraction.

(6) *Declaration of emergencies.* Notifications made to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter, as applicable.

(7) *Elimination of duplication.* Separate notifications and reports are not required for events that are also reportable in accordance with §§ 50.72 and 50.73 of this chapter. However, these notifications should also indicate the applicable § 73.77 reporting criteria.

(d) *Written security follow-up reports.* Each licensee making an initial telephonic notification of security events to the NRC according to the provisions of paragraphs (a)(1), (a)(2)(i), and (a)(2)(ii) of this section must also submit a written security follow-up report to the NRC within 60 days of the telephonic notification in accordance with § 73.4.

(1) Licensees are not required to submit a written security follow-up report following a telephonic notification made under § 73.77(a)(2)(iii) or (a)(3).

(2) Each licensee shall submit to the NRC written security follow-up reports that are of a quality that will permit legible reproduction and processing.

(3) Licensees shall prepare the written security follow-up report on NRC Form 366.

(4) In addition to the addressees specified in § 73.4, the licensee shall also provide one copy of the written security follow-up report addressed to the Director, Office of Nuclear Security and Incident Response, or the Director's designee. Any written security follow-up reports containing classified information shall be transmitted to the NRC Headquarters' classified mailing address as specified in appendix A to this part.

(5) The written security follow-up report must include sufficient information for NRC analysis and evaluation.

(6) Significant supplemental information which becomes available after the initial telephonic notification to the NRC Headquarters Operations Center or after the submission of the written security follow-up report must be telephonically reported to the NRC Headquarters Operations Center under paragraph (c) of this section and also submitted in a revised written security follow-up report (with the revisions indicated) as required under this section.

(7) Errors discovered in a written security follow-up report must be corrected in a revised written security follow-up report with the revision(s) indicated.

(8) The revised written security follow-up report must replace the previous written security follow-up report; the update must be complete and not be limited to only supplementary or revised information.

(9) If the licensee subsequently retracts a telephonic notification made under this section as not meeting the threshold of a reportable event, and has not yet submitted a written security follow-up report then submission of a written security follow-up report is not required.

(10) If the licensee subsequently retracts a telephonic notification made under this section as not meeting the threshold of a reportable event after it has submitted a written security follow-up report required by this paragraph, then the licensee shall submit a revised written security follow-up report in accordance with this paragraph.

(11) Each written security follow-up report submitted containing Safeguards Information or Classified Information must be created, stored, marked, labeled, handled, and transmitted to the NRC according to the requirements of §§ 73.21 and 73.22 or with part 95 of this chapter, as applicable.

(12) Each licensee shall maintain a copy of the written security follow-up report of an event submitted under this section as a record for a period of three years from the date of the report or until the Commission terminates the license for which the records were developed, whichever comes first.

[80 FR 67275, Nov. 2, 2015]

ENFORCEMENT

§ 73.80 Violations.

(a) The Commission may obtain an injunction or other court order to prevent a violation of the provisions of—

(1) The Atomic Energy Act of 1954, as amended;

(2) Title II of the Energy Reorganization Act of 1974, as amended; or

(3) A regulation or order issued pursuant to those Acts.

(b) The Commission may obtain a court order for the payment of a civil penalty imposed under section 234 of the Atomic Energy Act:

(1) For violations of—

(i) Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended:

(ii) Section 206 of the Energy Reorganization Act;

(iii) Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;

(iv) Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

(2) For any violation for which a license may be revoked under Section 186 of the Atomic Energy Act of 1954, as amended.

[57 FR 55078, Nov. 24, 1992]