DRAFT FINAL 10 CFR PART 73 RULE LANGUAGE

Cyber Security Notifications Events

The NRC staff is providing this draft final rule language to the public in preparation for the public meeting on July 31, 2014, to discuss the proposed implementation dates of the draft cyber security event notification final rule.

NOTE: The NRC is making this draft final rule language available for public viewing only. The release of the draft final requirements is intended to inform stakeholders of the current status of the NRC's activities on the rulemaking. The draft final rule language has not been reviewed by the Commission and may be subject to significant revisions during the final rulemaking process. The NRC is not soliciting formal public comments on these draft final rule language provisions. No stakeholder requests for a comment period will be granted at this stage in the rulemaking process. This draft final rule language reflects the NRC's consideration of stakeholder comments throughout this rulemaking process.

Any questions on this rule language may be addressed to the NRC rulemaking project manager, Robert Beall (301-415-3874; Robert.Beall@nrc.gov).

For the reasons set out in the preamble and under the authority of the Atomic Energy Act of 1954, as amended; the Energy Reorganization Act of 1974, as amended; and 5 U.S.C. 552 and 553, the NRC is adopting the following amendments to 10 CFR Part 73.

PART 73 – PHYSICAL PROTECTION OF PLANTS AND MATERIALS

1. The authority citation for Part 73 continues to read as follows:

Authority: Atomic Energy Act secs. 53, 147, 161, 223, 234, 1701 (42 U.S.C. 2073, 2167, 2169, 2201, 2273, 2282, 2297(f), 2210(e)); Energy Reorganization Act sec. 201, 204 (42 U.S.C. 5841, 5844); Government Paperwork Elimination Act sec. 1704, (44 U.S.C. 3504 note); Energy Policy Act of 2005, Pub. L. 109-58, 119 Stat. 594 (2005).

Section 73.1 also issued under Nuclear Waste Policy Act secs. 135, 141 (42 U.S.C, 10155, 10161). Section 73.37(f) also issued under sec. 301, Pub. L. 96-295, 94 Stat. 789 (42 U.S.C. 5841 note).

FEDERAL REGISTER CITATION: July 6, 2012; 77 FR 39899, 39909.

2. In section 73.8, revise paragraphs (b) and (c)(1) to read as follows:

§ 73.8 Information collection requirements: OMB approval.

* * * * *

(b) The approved information collection requirements contained in this part appear in §§ 73.5, 73.20, 73.21, 73.23, 73.24, 73.25, 73.26, 73.27, 73.37, 73.40, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 73.70, 73.71, 73.71a, 73.72, 73.73, 73.74, and appendices B, C.

* * * * *

(c) * * *

(1) In § 73.71 and § 73.71a, NRC Form 366 is approved under control number 3150-0104.

* * * * *

3. In section 73.22, revise the last sentence in paragraph (f)(3) to read as follows:

§ 73.22 Protection of Safeguards Information: Specific requirements.

* * * * *

(f) * * *

(3) * * * Cyber security event notifications required to be reported pursuant to § 73.71a are considered to be extraordinary conditions.

* * * * *

4. In section 73.54, add paragraph (d)(4) to read as follows:

§ 73.54 Protection of digital computer and communication systems and networks.

* * * * *

(d) * * *

(4) Conduct cyber security event notifications in accordance with the provisions of § 73.71a.

5. Add section 73.71a to read as follows:

DRAFT FINAL 10 CFR PART 73 RULE LANGUAGE

Cyber Security Notifications Events

§ 73.71a Cyber security event notifications.

Each licensee or applicant subject to the provisions of § 73.54 shall notify the NRC Headquarters Operations Center via the Emergency Notification System of the following cyber security events within the timeliness requirements of paragraphs (a), (b) and (c) of this section, as applicable.

(a) *One-hour notifications.*

(1) Upon 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 compromises support systems and equipment that results in adverse impacts to safety, security, or emergency preparedness functions within the scope of § 73.54.

(2) Notifications must be made according to paragraph (e) of this section.

(b) *Four-hour notifications*.

(1) Upon 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 support systems and equipment, which if compromised, could have adversely impacted safety, security, or emergency preparedness functions within the scope of § 73.54.

(2) Upon 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.

(3) Upon notification of a local, State, or other Federal agency (e.g., law enforcement, Federal Bureau Of Investigation, etc.) of an event related to the licensee's or applicant'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 or other provision of paragraph (b) of this section.

(4) Notifications must be made to the NRC according to paragraph (e) of this section.

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

(c) *Eight-hour notifications*.

(1) Upon 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.

(2) Notifications must be made according to paragraph (e) of this section.

(3) Notifications made under paragraphs (a) and (b) of this section are not required to be duplicated under this paragraph.

(d) *Twenty-four hour recordable events.*

(1) The licensee or applicant shall use the site corrective action program to document, track, trend, correct, and prevent recurrence of failures and deficiencies in their § 73.54 cyber security program.

(2) The licensee or applicant shall use the site corrective action program to document, track, and trend notifications made under paragraphs (a), (b) and (c) of this section.

(e) *Notification process.*

(1) Each licensee or applicant shall make telephonic notifications required by paragraphs (a), (b), and (c) of this section to the NRC Headquarters Operations Center via the Emergency Notification System. If the Emergency Notification System is inoperative or unavailable, the licensee or applicant 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 of 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 of § 73.22(f)(3) for emergency or extraordinary conditions.

(3) Notifications required by this section that contain classified national security information and/or restricted data must be made to the NRC Headquarters Operations Center using secure communications systems appropriate to the classification level of the message. Licensees and applicants making classified 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 or applicant's secure communications capability is unavailable (e.g., due to the nature of the security event), the licensee or applicant must provide as much information to the NRC as is required by this section, without revealing or discussing any classified information, in order to meet the timeliness requirements of this section. The licensee or applicant must also indicate to the NRC that its secure communications capability is unavailable.

(ii) Licensees or applicants using a non-secure communications capability may be directed by the NRC Emergency Response management to provide classified information to the NRC over the non-secure system, due to the significance of the ongoing security event. In such circumstances, the licensee or applicant 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 (h) of this section.

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

(5) Licensees or applicants 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, 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. However, these notifications should also indicate the applicable § 73.71a reporting criteria.

(f) *Written security follow-up reports.* Each licensee or applicant making an initial telephonic notification of security events to the NRC according to the provisions of paragraphs (a)(1), (b)(1) and (b)(2) 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 and applicants are not required to submit a written security follow-up report following a telephonic notification made under § 73.71a(b)(3), a notification to a local, State, or other Federal agency and § 73.71a(c)(1) a notification regarding activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack.

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

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

(4) In addition to the addressees specified in § 73.4, the licensee or applicant shall also provide one copy of the written security follow-up report addressed to the Director, Cyber Security Directorate, Office of Nuclear Security and Incident Response. 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 (e) 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 or applicant 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 or applicant 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 or applicant 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 or applicant 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.