RULEMAKING ISSUE
(Affirmation)

November 20, 2014 SECY-14-0129

FOR: The Commissioners

FROM: Mark A. Satorius
Executive Director for Operations

SUBJECT: FINAL RULE: CYBER SECURITY EVENT NOTIFICATIONS (10 CFR PART 73) (RIN-3150-AJ37)

PURPOSE:

To obtain Commission approval to publish a final rule to amend certain cyber security event notification requirements in the regulations that governs the licensing of nuclear power plants.

DISCUSSION:

The amendments to the cyber security event notification requirements will result in changes and additions to the following sections in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials":

- 10 CFR 73.22, "Protection of safeguards information: Specific requirements",
- 10 CFR 73.54, "Protection of digital computer and communication systems and networks."

Also, the following section will be added to Part 73:

- 10 CFR 73.77, "Cyber security event notifications."

The final rule will require 10 CFR Parts 50 and 52 licensees that are subject to the requirements of § 73.54 to ensure that their cyber security program meets the cyber security event notification requirements in the final rule.

CONTACTS: Robert H. Beall, NRR/DPR
(301) 415-3874

Brad L. Bergemann, NSIR/CSD
(301) 287-3797

Significant Changes from the Proposed Rule to the Final Rule

The U.S. Nuclear Regulatory Commission (NRC) made some significant changes to the proposed rule as a result of public comments and other staff considerations. The final rule reflects the following changes:

- *Adverse impact to safety, security and emergency preparedness (SSEP) functions*. Under the proposed rule, cyber security event notifications were included in the same section as the physical security event notifications but have been moved to § 73.77 in the final rule. One-hour notifications addressed uncompensated cyber security events, as well as acts or threats committed or caused to modify, destroy, or compromise systems, networks, and equipment that falls within the scope of § 73.54. The staff revised the requirements for one-hour notifications to align more closely with § 73.54 requirements and now addresses cyber attacks that adversely impacted SSEP functions.

- *Suspicious or threatening cyber security activities*. Under the proposed rule, suspicious cyber security events were captured under four-hour notifications and included tampering and malicious or unauthorized access, use, operation, manipulation, modification, and potential compromise (i.e., unauthorized activities) of systems, networks, and equipment within the scope of § 73.54. Under the final rule, the term "suspicious cyber security events" was clarified and the requirement to report such events was moved to eight-hour notifications. The final rule maintains a new requirement to report cyber tampering and unauthorized cyber activities under four-hour notifications.

- *Site Corrective Action Program (CAP)*. Under the proposed rule certain cyber security events were to be recorded in a Safeguards Event Log (SEL). The staff revised the language to require the recording of certain cyber security events in the site CAP instead of the SEL. Licensees will use the site CAP to record vulnerabilities, weaknesses, failures and deficiencies in their cyber security program within twenty-four hours of their discovery as well as notifications made to the NRC. This revision eliminates redundancy in recording of cyber security events in two separate places (SEL and site CAP) as well as closely aligns with existing provisions utilized under the physical protection program (10 CFR 73.55(b)(10)).

Cumulative Effects of Regulation

The NRC issued draft guidance for comment concurrent with the proposed rule and conducted a public meeting at the NRC Headquarters on June 1, 2011, to discuss the proposed rule, draft guidance, and the draft implementation plan. In addition, a public meeting on the final draft implementation date was conducted on July 31, 2014, during the final rulemaking stage. These efforts are consistent with the intent of the formal Cumulative Effects of Regulation (CER) in spite of the proposed rule having been issued prior to the CER requirements promulgated by staff requirements memorandum (SRM)-SECY-0032, "Consideration of the Cumulative Effects of Regulation in the Rulemaking Process", dated October 11, 2011 (Agencywide Document Access and Management System (ADAMS) Accession No. ML112840466).

The feedback from these meetings informed the staff's recommended schedule for the implementation of the new cyber security event notification requirements in the enclosed *Federal Register* notice (Enclosure 2).

A fundamental CER process discussed in SRM-SECY-11-0032 is to publish the final guidance with the final rule to support effective implementation. In the spirit of CER, this final rulemaking accomplished that by ensuring the draft final guidance was complete and available when the final rule was provided to the Commission for deliberation.

Public Input to the Proposed Rule

In an effort to conduct a rulemaking that is transparent and open to stakeholder participation, the NRC engaged the public through various means during the development of this rule. The staff posted draft rule language and the draft supporting guidance on the e-rulemaking Web site at http://www.regulations.gov on February 3, 2011. In addition, the staff met with stakeholders on June 1, 2011, to answer questions the public had on the proposed rule language and supporting guidance documents. At this meeting, the NRC discussed the proposed cyber security event notification requirements and the associated draft guidance documents, and answered clarifying questions from participants.

Guidance Documents

The NRC staff will publish the following final guidance document in conjunction with the final rule:

- Regulatory Guide 5.83, "Cyber Security Event Notifications"

COMMITMENT:

The staff plans to publish this final rule in the *Federal Register* pending Commission approval and subsequent review from the Office of Management and Budget (OMB).

RESOURCES:

The cyber security event notifications final rule requires resources in fiscal years 2014, 2015, and 2016 in the Operating Reactors Business Line. Detailed resource estimates can be found in Enclosure 3.

RECOMMENDATIONS:

The staff recommends that the Commission take the following actions:

(1) Approve the final rule (Enclosure 2) for publication in the *Federal Register*.

(2) Certify that this rule, if issued, will not have a significant economic impact on a substantial number of small entities in order to satisfy requirements of the Regulatory Flexibility Act of 1980, as amended (5 U.S.C. 605(b)).

(3) Note the following:

– The staff has prepared a final regulatory analysis (Section VII of Enclosure 2).

– The staff has determined that this action is not a “major rule” as defined in the Congressional Review Act of 1996 (5 U.S.C. 804(2)) and has confirmed this determination with OMB. The staff will inform the appropriate Congressional and Government Accountability Office contacts.

– The staff has performed a final environmental assessment and reached a finding of no significant impact (Section VII of Enclosure 2).

– This final rule creates new information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). The staff will submit this rule to OMB for review and approval of the information collection requirements (Section XII of Enclosure 2).

– The staff will inform the appropriate Congressional committees.

– The Office of Public Affairs will issue a press release.

COORDINATION:

The Office of the General Counsel has reviewed the final rule and has no legal objections. The Office of the Chief Financial Officer has reviewed the final rule for resource implications and has no objections. The Office of Information Services has reviewed the final rule and has no objections to the changes in information collection requirements.

The Advisory Committee on Reactor Safeguards (ACRS) did not review the final rule because the Commission determined in SRM-M031002, dated October 31, 2003 (ADAMS Accession No. ML033040278), that issues associated with threat assessment, physical security, or force-on-force assessments are outside the ACRS's area of expertise, and involve intelligence information not available to the ACRS.

/RA Michael R. Johnson for/

Mark A. Satorius
Executive Director
for Operations

Enclosures:
1. History of the Cyber Security Event Notification Rulemaking Activities
2. *Federal Register* notice
3. Resources for Cyber Security Event Notification Rulemaking Activities
4. Regulatory Analysis

The Advisory Committee on Reactor Safeguards (ACRS) did not review the final rule because the Commission determined in SRM-M031002, dated October 31, 2003 (ADAMS Accession No. ML033040278), that issues associated with threat assessment, physical security, or force-on-force assessments are outside the ACRS's area of expertise, and involve intelligence information not available to the ACRS.

/RA Michael R. Johnson for/

Mark A. Satorius
Executive Director
for Operations

Enclosures:
1. History of the Cyber Security Event Notification Rulemaking Activities
2. *Federal Register* notice
3. Resources for Cyber Security Event Notification Rulemaking Activities
4. Regulatory Analysis

ADAMS ACCESSION Nos.: PKG: ML14136A209/ Memo: ML14136A212
WITS: CMSY13-0031-1-NRR *Via E-Mail

OFFICE	NRR/DPR/PRMB	NRR/DPR/PRMB	NRR/DPR/PRMB	NRR/DPR	NRR/DPR
NAME	RBeall	GLappert*	TInverso*	AMohseni	LKokajko
DATE	07/28/14	09/03/14	07/28/14	07/29/14	08/01/2014
OFFICE	NSIR/CSD	OIS/IRSD*	ADM/DAS/RDB*	OE*	NRO*
NAME	BWestreich	FMajeed	CBladey	RZimmerman (TMarenchin for)	GTracy (MMayfield for)
DATE	07/29/14	08/29/14	08/14/14	08/11/14	08/12/14
OFFICE	CFO*	NSIR	OGC*	NRR	EDO
NAME	MWylie (ARossi for)	JWiggins	NStAmour(SClark for)	DDorman (JUhle for)	MSatorius(MRJohnson for)
DATE	08/05/14	10/16/14	10/07/14	09/09/14	11/20/14

OFFICIAL RECORD COPY

ENCLOSURE 1