UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

June 9, 2015

SECRETARY

COMMISSION VOTING RECORD

DECISION ITEM: SECY-14-0129

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

The Commission acted on the subject paper as recorded in the Staff Requirements Memorandum (SRM) of June 9, 2015.

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Commission.

Annette L. Vietti-Cook
Secretary of the Commission

Enclosures:
1. Voting Summary
2. Commissioner Vote Sheets

cc: Chairman Burns
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
OGC
EDO
PDR

VOTING SUMMARY - SECY-14-0129

RECORDED VOTES

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIP	COMMENTS	DATE
CHRM. BURNS	X				X	3/31/15
COMR. SVINICKI		X			X	5/11/15
COMR. OSTENDORFF	X				X	12/16/14
COMR. BARAN	X				X	2/20/15

AFFIRMATION ITEM

RESPONSE SHEET

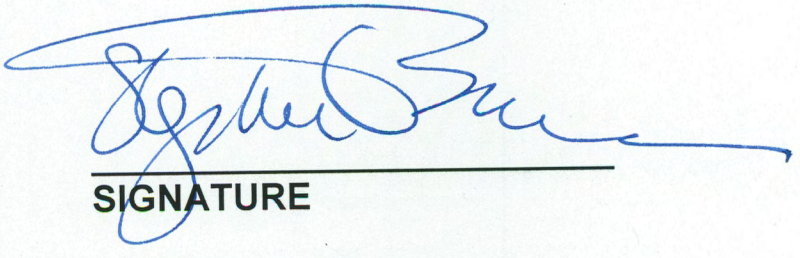
TO: Annette Vietti-Cook, Secretary

FROM: Chairman Burns

SUBJECT: SECY-14-0129 FINAL RULE: CYBER SECURITY EVENT NOTIFICATIONS (10 CFR PART 73) (RIN-3150-AJ37)

Approved XX Disapproved ____ Abstain ____ Not Participating ____

COMMENTS: Below ____ Attached XX None ____



SIGNATURE

31 March 2015

DATE

Entered in STARS: Yes x No ____

Chairman Burns' Comments on SECY-14-0129
"Final Rule: Cyber Security Event Notifications (10 CFR Part 73) (RIN-3150-AJ37)

I approve the final Cyber Security Event Notifications rule for publication in the *Federal Register*, subject to the attached edits. I also 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)).

I agree with Commissioner Baran that the draft *Federal Register* notice demonstrates that the staff has seriously considered and taken into account the various stakeholder comments received during the rulemaking process. Additionally, I recognize that the staff has continued to engage with stakeholders to understand and address their concerns and to provide clarification of the rule language in the accompanying guidance document. The staff's efforts to find an appropriate balance between ensuring that the NRC receives prompt notification of cyber attacks while reducing the potential for nuisance reports is commendable.

Stephen Burns
31 March 2015

5019, Revision 1, and RG 5.83 reflect public comment. This approach (i.e., publish draft guidance with proposed rules and final guidance with final rules) is consistent with the agency's efforts to incorporate enhancements in the rulemaking process to address Cumulative Effects of Regulation, as approved by SRM-SECY-11-0032 (ADMAS Accession No. ML112840466).

II. Discussion.

The NRC is adding cyber security event notification requirements for nuclear power reactor facilities. These additions are necessary because cyber security event notification requirements were not included in the NRC's final rule that added 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" to the NRC's regulations (74 FR 13926; March 27, 2009). Section 73.54 requires power reactor licensees to establish and maintain a cyber security program that provides high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Cyber security event notification requirements will contribute to the NRC's analysis of the reliability and effectiveness of licensees' cyber security programs and plays an important role in the continuing effort to protect digital computer and communication systems and networks associated with: safety-related and important-to-safety functions; security functions; emergency preparedness functions, to include offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, and emergency preparedness (SSEP) functions. Notifications conducted and written reports generated by licensees will be used by the NRC to respond to emergencies, monitor ongoing events, assess trends and patterns, identify precursors of more significant events, and inform other NRC licensees of cyber security-related events, enabling them to take preemptive actions, if necessary (e.g., increase security posture). In addition, timely notifications assist the NRC in achievinge its strategic

notifications, one that is based on whether the cyber attack caused an adverse impact (or not) to SSEP functions. The final rule and RG 5.83 have been revised to reflect this new approach.

Comment 7: The NRC received one comment pertaining to use of the term "uncompensated" in the context of cyber security, stating that the term is unclear, and is not defined within the CSP. In addition, one of the commenters also stated that the term "failure" in the context of cyber security required clarification. [NEI-164, 207]

Response: The NRC agrees with this comment. The terms "uncompensated" and "failure" have been removed from the final rule language. Based on public comments, the NRC has developed a different approach for determining cyber security event notifications, one that is based on whether the cyber attack or event caused an adverse impact (or not) to SSEP functions. RG 5.83 has been revised to reflect this new approach.

Comment 8: One commenter proposed changes to the rule language, appendix G I.(h)(1), adding the terms "credible", "malicious" and "radiological sabotage" to add clarity. The commenter recommended rewriting the event to add in part, "a credible threat to commit or cause a malicious act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of 10 CFR 73.54 of this part where a compromise of these systems has resulted or could result in radiological sabotage." [NEI-157, 206]

Response: The NRC disagrees with this comment. Based on public comments, the NRC developed a different approach for determining cyber security event notifications, one that is based on whether a cyber attack caused an adverse impact (or not) to SSEP functions. This approach aligns more closely with § 73.54 and the terms credible, malicious, and radiological

Comment 13: One commenter proposed changes to appendix G IV.(a)(2) to add the words "that would". [NEI-163]

Comment [SGB1]: Staff should provide the appendix G IV.(a)(2) sentence or statement that was identified in this comment in order to allow readers of this notice to understand the full context of the comment.

Response: The NRC disagrees with this comment. Adding the words, "that would" to the rule text changes the context of the type of events that are required to be recorded. However, based on public comments, the NRC revaluated the 24-hour recordable events for cyber security event notifications and developed an approach that aligns more closely with the CSP requirements. Under this approach, licensees are required to use their corrective action program to record vulnerabilities, weaknesses, failures, and deficiencies in their cyber security program. RG 5.83 has been updated to reflect this change.

Comment 14: One commenter recommended revising the proposed rule language to align exactly with the rule language in 10 CFR 73.54(a)(2), which discusses protecting digital assets from cyber attacks that would adversely impact the operations of SSEP functions. Specifically, the commenter notes that the reporting rule text uses the word "could" instead of "would." [NEI-168]

Response: The NRC agrees in part, with this comment. The NRC agrees that the reporting rule text should align more closely with 10 CFR 73.54. However, the NRC disagrees with changing the word "could" to "would," because these words are correctly used in their respective rules. 10 CFR 73.54 addresses hypothetical future cyber attacks that must be protected against, while this rule describes notifications that licenses are required to issue after an event has already occurred. Further, there are different types of cyber attacks that licensees are required to report. One type of attack required to be reported is a cyber attack that adversely impacted SSEP functions. This type of attack is to be reported within one-hour after discovery. Another type required to be reported is a cyber attack that could have caused an adverse

systems or equipment from this requirement and they are now captured under 10 CFR 73.77(a)(1), (a)(2)(i) and (a)(2)(ii) of this final rule.

Comment 11: One commenter indicated that appendix G I.(c)(2) in the proposed rule text should be completely removed because it duplicates other proposed rule text. [NEI-160]

Response: The NRC agrees in part, with this comment. The commenter's reference to appendix G I.(c)(2) appears to be misquoted. The changes proposed by the commenter would amend Appendix G II.(c)(2). The final rule text has been revised to remove all duplicative language and is aligned more closely with the requirements in 10 CFR 73.54 (i.e., adverse impacts to SSEP functions). This revised requirement is designated as § 73.77(a)(2)(i). RG 5.83 has been revised to reflect this change.

Comment 12: One commenter proposed changes to appendix G III to clarify the language under eight-hour reportable events to be consistent with 10 CFR 73.54(c)(1), which implements security controls to protect CDAs and critical systems from cyber attacks. [NEI-162]

Response: The NRC agrees in part, with this comment. Based on public comments, the NRC developed an approach that aligns more closely with 10 CFR 73.54. The implementation of security controls to protect CDAs from cyber attacks as described in 10 CFR 73.54(c)(1) is designed to prevent adverse impacts to SSEP functions. Therefore, in the final rule, a cyber attack that adversely impacted SSEP functions requires notification within one hour after discovery, and cyber attacks that could have caused an adverse impact to SSEP functions requires notification within four hours after discovery due to the potential consequences of these events. RG 5.83 has been revised to reflect this new approach.

Response: The NRC disagrees with this comment. The final rule language reflects a different approach, one based on whether the cyber attack or event caused an adverse impact (or not) to SSEP functions, instead of whether the cyber attack or event was compensated or uncompensated. RG 5.83 has been revised to reflect this new approach.

Comment 30: Several commenters recommended changes to definitions provided in the glossary of DG-5019. One commenter proposed the term "cyber attack" be revised to be consistent with the definition provided in NEI 08-09. Another commenter proposed the term "CDA" be revised to only include digital computer, communication systems, and networks that fall within level 3 or 4 boundaries. Another commenter recommended synchronization with code requirements and regulatory guides. [NEI-138, 204, 205]

Comment [SGB2]: The comment summary indicates that it reflects input from several commenters but only one commenter is shown here. Staff should ensure that the comment summary and the list of comment numbers are consistent.

Response: The NRC agrees in part. The definitions of cyber attack and CDA in RG 5.83 have been revised to synchronize with the definitions in RG 5.71, not NEI 08-09.

Comment 31: Two commenters proposed a definition of the term "discovery time of" in DG-5019. The commenters suggested discovery occurs after initial notifications are made and a determination made that the event meets applicable reporting requirements. [NEI-19, B&W-29]

Response: The NRC disagrees with this comment. Internal notifications and gathering information to make a determination as to whether it meets applicable reporting requirements could take several hours, or even days, depending on the amount of information needed to reach a conclusion. The time to report an event is upon recognition; the licensee can withdraw a report (based on subsequent analysis of the circumstances) without prejudice to its security performance indicators. No changes have been made to the guidance.

and the feedback from the public meetings informed the staff's recommended schedule for the final implementation date in the CSEN final rule.

A fundamental CER process improvement is to publish the final guidance with the final rule so as to support effective implementation. This final rulemaking accomplishes this by ensuring that final guidance is complete and available concurrent with this final rule publication in the *Federal Register*.

X. Plain Writing.

The Plain Writing Act of 2010 (Pub. L. 111-274) requires Federal agencies to write documents in a clear, concise, and well-organized manner. The NRC has written this document to be consistent with the Plain Writing Act as well as the Presidential Memorandum, "Plain Language in Government Writing," published June 10, 1998 (63 FR 31883).

XI. National Environmental Policy Act

The NRC has determined that this final rule is the type of action described in 10 CFR 51.22(c)(3)(iii). Therefore, neither an environmental impact statement nor environmental assessment has been prepared for this final rule.

Comment [SGB3]: The SECY-14-0129 cover letter includes the following statement, which contradicts the information provided in this FRN (Enclosure 2):

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

Staff should ensure that the FRN provides accurate information regarding the staff's NEPA review.

XII. Paperwork Reduction Act.

This final rule contains new or amended information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These requirements were approved by the Office of Management and Budget (OMB), approval number 3150-0002 and 3150-0104.

(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, ~~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 (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.

(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.

Dated at Rockville, Maryland, this ___th day of , ~~2014~~2015.

For the Nuclear Regulatory Commission.

Annette L. Vietti-Cook,
Secretary of the Commission.

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER SVINICKI

SUBJECT: SECY-14-0129 – FINAL RULE: CYBER SECURITY EVENT NOTIFICATIONS (10 CFR PART 73) (RIN-3150-AJ37)

Approved ____ Disapproved XX Abstain ____ Not Participating ____

COMMENTS: Below _____ Attached XX None _____

SIGNATURE

05/ 11 /15

DATE

Entered in STARS: Yes ✓ No _____

Commissioner Svinicki's Comments on SECY-14-0129
Final Rule: Cyber Security Event Notifications (10 CFR Part 73) (RIN-3150-AJ37)

I disapprove the draft final rule (Enclosure 2 to SECY-14-0129). The Commission should return this rule to the staff with instructions to remedy its defects. Additionally, I am unable to approve this draft final rule as I remain unconvinced, based on a review of the record, that the staff has fulfilled, in a searching and genuine way, the NRC's obligations under the Administrative Procedure Act (APA) with respect to both form and process. Because some provisions contained in the draft final rule cannot be traced clearly to the proposed rule nor do they appear to grow out of the public comment received, the draft final rule should be re-noticed for public comment.

The public comment received on the proposed rule was considerable in both quantity and substance. In contrast, the proposed public comment responses as reflected in the draft *Federal Register* notice are, for the most part, superficial and lack the level of scrutability that I expect at the NRC. We can do better, even on an issue of this complexity.

Of note, the U.S. Court of Appeals for the District of Columbia Circuit, in a decision issued just this month, struck down an agency rule as "arbitrary and capricious" in light of agency obligations under the APA and noted that the agency offered "wan responses" to public comments received. "[The agency] cannot get away so easily from its obligations under the APA to respond to 'relevant and significant' comments. Naturally, an agency need not 'discuss every item of fact or opinion included in the submissions made to it.' But an agency must respond sufficiently to 'enable us to see what major issues of policy were ventilated . . . and why the agency reacted to them as it did.' . . . During oral argument, [the agency's] attorney told the court that [the agency] 'heard' the commenters' concerns . . . [b]ut merely hearing is not good enough[. The agency] must respond to serious objections. By failing to do so here, its rulemaking was arbitrary and capricious."[1]

As an example, one commenter requested that the proposed notification requirements should take a graded approach, i.e., critical digital assets that are not part of a target set should not have the same sensitivity as those critical digital assets that are contained within a target set. In its response, the staff states that it disagrees with the comment and that cyber security event notification requirements in the draft final rule "focus on events that have or could have had" an adverse impact. In addition to being extremely difficult to interpret in practice, this approach is a significant policy departure from the NRC's risk-informed approach to regulation. Moreover, it risks repeating the unfortunate learning curve that the agency experienced in its approach to the overarching cyber security rule (currently under implementation).

A similar disconnect appears in Comment 16 and its response. The commenter proposed changing the wording of a requirement from events that "could" allow unauthorized or undetected access to events that "would" allow such access. The proposed response has NRC disagreeing, stating that the objective of event reporting is not to have licensees report that an event has occurred but rather that it could occur. This is challenging to understand on paper and, in practice, will be exceedingly murky to implement. In a similar vein, the draft final rule text would institute requirements to notify the NRC within a time certain after discovery of a "cyber attack" but does not define "cyber attack" in the rule itself. In other words, the rule sets

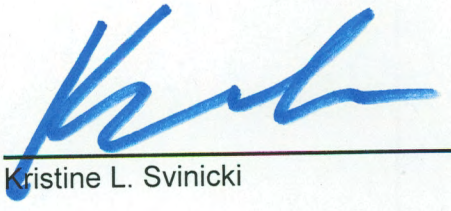
---

[1] *Delaware Dept. of Natural Resources and Environmental Control v. E.P.A.*, Nos. 13-1093, 13-1102, 13-1104, 2015 WL 1947436, at 15-16 (D.C. Cir. May 1, 2015) (citations omitted, first ellipsis in original).

out with great particularity the requirement to make notifications to NRC but fails to provide clarity on when these requirements are invoked. Some level of basic definition regarding this is needed in the rule itself; it cannot all be left to the guidance documents.

The draft *Federal Register* notice explains that a backfit analysis was not prepared for the draft final rule because it affects solely information collection and reporting requirements. The associated regulatory analysis (Enclosure 4), however, elaborates that the rule "requires power reactor licensees to establish and maintain a cyber security program at their facilities" and that the compliance date of the final rule "will be 180 days after publication . . . to allow licensees time to revise their event notification procedures and train personnel." These measures extend beyond the scope of information collection activities appropriate for invoking exceptions to backfit analysis (those administrative in nature) and impact more broadly the operational structure of licensed facilities. The staff is reminded that, under 10 CFR 50.109, a backfit is "modification of or addition to . . . procedures or organization required to . . . operate a facility." In light of this, a backfit analysis should also be prepared for this rule.

The procedural history of this rulemaking is rather tortured, I acknowledge, as it was severed from a larger rulemaking (with the Commission's approval). I cannot discern if this was a contributor to the odd result that a number of the provisions in the draft final rule do not appear to exist clearly anywhere in the proposed rule. I realize that draft final rules are shaped by the process of responding to public comment and will not read exactly the same in final form but, in any event, the agency must meet its legal obligation that the provisions of a final rule have their origins in or be a logical outgrowth of the proposed rule. I cannot confirm that this test is met here.



Kristine L. Svinicki 05/11/15

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER OSTENDORFF

SUBJECT: SECY-14-0129 - FINAL RULE: CYBER SECURITY EVENT NOTIFICATIONS (10 CFR PART 73) (RIN-3150-AJ37)

Approved XX Disapproved ____ Abstain ____ Not Participating ____

COMMENTS: Below ____ Attached XX None ____

Vicki Ostendorff
SIGNATURE

12/16/14
DATE

Entered in STARS: Yes ____ No ____

Commissioner Ostendorff's Comments on SECY-14-0129,
"Final Rule: Cyber Security Event Notifications (10 CFR PART 73) (RIN-3150-AJ37)"

I approve the final Cyber Security Event Notifications rule for publication in the *Federal Register*. I also 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)). I commend the staff for a well-written rule that provides clarity and removes all voluntary aspects of reporting certain cyber security events.

In a public comment submission, NEI recommended that the implementation date of this rule align with the date that cyber security plans become effective. I have considered this recommendation in light of the cumulative effect of regulation; however, the schedule for full implementation of cyber security plans (i.e. milestone 8) has been extended for several licensees and may not be completed for several years. In the interim, compliance with the cyber security event notifications rulemaking is necessary so that the NRC will receive prompt notification of cyber security attacks or attempted attacks. As stated in the staff's response to NEI's comment, "Prompt notification of a cyber attack could be vital to the NRC's ability to take immediate action in response to a cyber attack and, if necessary, to notify other NRC licensees, Government agencies, and critical infrastructure facilities, to defend against a multiple sector (e.g., energy, financial, etc.) cyber attack." Therefore, I support the staff's proposed implementation schedule of 180 days after publication of the final rule.

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: Commissioner Baran

SUBJECT: SECY-14-0129: FINAL RULE: CYBER SECURITY EVENT NOTIFICATIONS (10 CFR PART 73) (RIN-3150-AJ37)

Approved X **Disapproved** ____ **Abstain** ____ **Not Participating** ____

COMMENTS: **Below** ____ **Attached** X **None** ____

SIGNATURE

2/20/15

DATE

Entered in STARS: **Yes** √ **No** ____

Commissioner Baran's Comments on SECY-14-0129,
"Final Rule: Cyber Security Event Notifications (10 CFR Part 73) (RIN-3150-AJ37)"

I commend the NRC staff for the years of work that went into completing this final rule on cyber security event notification for nuclear power plants. It is clear from reading the draft *Federal Register* notice that the staff took seriously the public comments from a variety of external stakeholders during the rulemaking process, refined its approach, and made significant improvements reflected in the final rule.

I agree with the staff that, although voluntary reporting initiatives implemented through security advisories have served an important purpose, it is appropriate to establish mandatory cyber security event notification requirements for nuclear power plants. As the staff points out, the current voluntary reporting is not enforceable or subject to any timeliness requirements. Yet prompt and complete reporting is vital to NRC's ability to respond quickly to actual or imminent cyber-attacks, notify other NRC licensees and government agencies when necessary, evaluate suspicious cyber activities for threat implications, and accomplish the agency's strategic communications mission. The regulatory analysis for the draft final rule shows that the implementation costs to NRC and licensees would be modest. Therefore, I approve the final rule for publication in the *Federal Register*, subject to the attached edits. I also 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)).

In SECY-12-0125, "Interim Actions to Execute Commission Preemption Authority Under Section 161A of the Atomic Energy Act of 1954, as Amended" (ADAMS Accession No. ML12171A089), the NRC staff reported their discussions with the U.S. Department of Justice on the need to revise the Firearms Guidelines to limit the firearms background check requirement to only licensees that apply for preemption authority. Subsequently in SRM-SECY-12-0125, dated November 12, 2012, (ADAMS Accession No. ML12326A653), the Commission directed the NRC staff to revise the Firearms Guidelines accordingly, and publish a supplemental proposed enhanced weapons rule for public comment as soon as possible.

On December 20, 2013, in COMSECY-13-0031, "Bifurcation of the Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule," (ADAMS Accession No. ML13280A366), the NRC staff informed the Commission of its plan to bifurcate the cyber security event notifications from the Enhanced Weapons rule due to delays resulting from the Firearms Guidelines revision. The bifurcation would allow the NRC staff to prepare a separate final rule for cyber security event notifications, thus avoiding any further delay associated with the aforementioned Firearms Guidelines revision. In addition, this action would supplement the existing cyber security requirements (i.e., 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks") included in the 2009 power reactor security rule (76 FR 6200; February 3, 2011).

As part of the 2011 proposed enhanced weapons rule, the NRC received comments on the proposed cyber security event notification requirements. Changes between the proposed rule and this final cyber security event notifications rule reflect these public comments. Additionally, Draft Guide (DG)-5019, Revision 1, "Reporting and Recording Safeguards Events" (ADAMS Accession No. ML 100830413) was published for public comment on February 3, 2011 (76 FR 6085). The portions of the DG related to cyber security event notifications were also separated out from the original draft guide, and are now included in a new final regulatory guide (Regulatory Guide (RG) 5.83, "Cyber Security Event Notifications," ADAMS Accession No.

ML14269A388). Changes between DG-5019, Revision 1, and RG 5.83 reflect public comment. This approach (i.e., publish draft guidance with proposed rules and final guidance with final rules) is consistent with the agency's efforts to incorporate enhancements in the rulemaking process to address Cumulative Effects of Regulation, as approved by SRM-SECY-11-0032 (ADMAS Accession No. ML112840466).

II. Discussion.

The NRC is adding cyber security event notification requirements for nuclear power reactor facilities. These additions are necessary because cyber security event notification requirements were not included in the NRC's final rule that added 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" to the NRC's regulations (74 FR 13926; March 27, 2009). Section 73.54 requires power reactor licensees to establish and maintain a cyber security program that provides high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Cyber security event notification requirements will contribute to the NRC's analysis of the reliability and effectiveness of licensees' cyber security programs and plays an important role in the continuing effort to protect digital computer and communication systems and networks associated with: safety-related and important-to-safety functions; security functions; emergency preparedness functions, to include offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, and emergency preparedness (SSEP) functions. Notifications conducted and written reports generated by licensees will be used by the NRC to respond to emergencies, monitor ongoing events, assess trends and patterns, identify precursors of more significant events, and inform other NRC licensees of cyber security-related events, enabling them to take preemptive actions, if necessary (e.g., increase their

security posture). In addition, timely notifications ~~assist~~ help the NRC achieve its strategic communications mission by informing the Department of Homeland Security (DHS) and Federal intelligence and law enforcement agencies of cyber security-related events that could: (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries.

The terrorist attacks of September, 11, 2001, demonstrated that adversaries were capable of simultaneously attacking multiple sectors of critical infrastructure ~~(financial, military)~~. After those attacks, the NRC issued several Security Orders, as well as the Design Basis Threat (DBT) final rule (72 FR 12705; March 19, 2007) and the Power Reactor Security final rule (74 FR 13926; March 27, 2009). These Orders and final rules were steps taken by the NRC to ensure adequate protection of the public health and safety and common defense and security. The DBT final rule, in § 73.1, "Purpose and Scope," describes in general terms the types of attacks licensees must protect against in order to prevent radiological sabotage and to prevent theft or diversion of strategic special nuclear material. An adversary attribute included under the DBT for radiological sabotage is a cyber attack, which is a type of attack that adversaries could remotely launch against multiple targets (i.e., nuclear power reactors) simultaneously. The Power Reactor Security final rule included specific requirements to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks (10 CFR 73.54). The addition of cyber security event notification requirements supplements 10 CFR 73.54 by enabling the timely notifications of potential and/or imminent cyber attacks directed against licensees. This allows for more timely assessment and dissemination of threat information, and improves the NRC's ability to respond and take the actions necessary to mitigate the adverse impacts of cyber attacks directed against licensees.

Separating the cyber security event notification requirements from the Power Reactor Security proposed rule narrowed the applicability to licensees subject to the requirements of 10 CFR 73.54, which applies to operating nuclear power plants after the effective date of the final

cyber security rule. Under the original proposed rule published on October 26, 2006 (71 FR 62663), cyber security event notifications were included with other event notifications (physical security, enhanced weapons, etc.) requiring a broader range of applicability (e.g., Fuel Cycle Facilities).

The NRC considered other options for licensees to report cyber attacks to the NRC. The NRC considered taking no additional regulatory actions and relying upon the continuation of voluntary reporting initiatives currently in place through security advisories. These voluntary reporting initiatives have allowed the NRC to identify certain cyber security-related events that might have had a negative impact upon licensees (e.g., vendor software updates containing malware) as well as provided licensees with threat information that assist them ~~to~~ in protecting against cyber security-related threats. However, the security advisories are not mandatory requirements and do not provide timeliness requirements (one-hour, four-hour, eight-hour), which can be instrumental in the NRC's ability to respond to cyber security-related events, to evaluate cyber security-related activities for threat implications, and to accomplish the Agency's strategic communications mission.

III. Opportunities for Public Participation.

A. Public and Stakeholder Meetings

As part of its comprehensive assessment of the NRC's cyber security event notification regulations and guidance development for this rule, the NRC staff held two meetings with internal and external stakeholders.

On June 1, 2011, staff held a public meeting to discuss the proposed Enhanced Weapons, Firearms Background Checks, and Security Event Notifications rulemaking, which included the cyber security event notification requirements. The meeting was in workshop format, and was held at the NRC Headquarters in Rockville, Maryland; it was attended by more

systems and equipment which, if compromised, would adversely impact safety, security or emergency preparedness functions.

Comment 3: Two commenters recommended that the four-hour notification events should be incorporated into the eight-hour notification events, thus eliminating the four-hour notification events. One commenter specifically recommended that suspicious events be moved from four-hour to eight-hour notifications. [NEI-17, 161, Hardin-2]

Response: The NRC agrees in part, with this comment. The NRC agrees that suspicious cyber security events (i.e., activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack) should be moved from four-hour notifications to eight-hour notifications. However, notifications with a local, State, or other Federal agency is consistent with existing NRC regulations at 10 CFR 50.72(b)(2)(xi). In addition, unsuccessful cyber attacks has been clarified to align more closely with 10 CFR 73.54 and addresses cyber attacks that could have caused an adverse impact to SSEP functions and remains a four-hour notification so the NRC can conduct additional notifications as appropriate (e.g., other NRC licensees, federal law enforcement agencies, the intelligence community) to mitigate the effects of a widespread cyber attack, or use as part of the National threat assessment process. Furthermore, unauthorized operation and tampering events haves been clarified to address suspected or actual cyber attacks initiated by personnel with physical or electronic access and whereas moved in the final rule to four-hour notifications due to the implications of an internal threat. Accordingly, the NRC has revised the rule language and associated guidance consistent with this approach to address the broader recommendation of aligning more closely with 10 CFR 73.54.

requires notification within four hours after discovery due to the potential consequences of these events. RG 5.83 has been revised to reflect this new approach.

Comment 13: One commenter proposed changes to appendix G IV.(a)(2) to add the words "that would". [NEI-163]

Response: The NRC disagrees with this comment. Adding the words, "that would" to the rule text changes the context of the type of events that are required to be recorded. However, based on public comments, the NRC revaluated the 24-hour recordable events for cyber security event notifications and developed an approach that aligns more closely with the CSP requirements. Under this approach, licensees are required to use their corrective action program to record vulnerabilities, weaknesses, failures, and deficiencies in their cyber security program. RG 5.83 has been updated to reflect this change.

Comment 14: One commenter recommended revising the proposed rule language to align exactly with the rule language in 10 CFR 73.54(a)(2), which discusses protecting digital assets from cyber attacks that would adversely impact the operations of SSEP functions. Specifically, the commenter notes that the reporting rule text uses the word "could" instead of "would." [NEI-168]

Response: The NRC agrees in part, with this comment. The NRC agrees that the reporting rule text should align more closely with 10 CFR 73.54. However, the NRC disagrees with changing the word "could" to "would," because these words are correctly used in their respective rules. 10 CFR 73.54 addresses hypothetical future cyber attacks that must be protected against, while this rule describes notifications that licenses are required to issue after an event has already occurred. Further, there are different types of cyber attacks that licensees are

Response: The NRC agrees in part with this comment. The staff recognizes that this rule will have an impact on licensee resources (similar skillsets required for CSEN and cyber security program implementation). The staff acknowledges this and is conducting Cumulative Effects of Regulation related activities in an effort to minimize the impact (e.g., conducting a public meeting on the implementation date during final rulemaking, issuing final guidance with the final rule). In addition, the CSEN final rule is consistent with existing notification processes (i.e., 10 CFR 50.72, 73.71) and aligns closely with 10 CFR 73.54 and the current voluntary reporting initiatives ~~there by~~thereby reducing the level of impact on implementation. However, the CSEN final rule removes the voluntary aspect of reporting certain cyber security events and provides regulatory stability and ensures the NRC is notified in a timely manner while maintaining its strategic communications mission outlined in the framework of the National Infrastructure Protection Plan developed by the DHS. Prompt notification of a cyber attack could be vital to the NRC's ability to take immediate action in response to a cyber attack and, if necessary, to notify other NRC licensees, Government agencies, and critical infrastructure facilities, to defend against a multiple sector cyber attack. A cyber attack has the capability to be launched against multiple targets simultaneously or spread quickly throughout multiple sectors of critical infrastructure; therefore, the NRC has not changed the 180-day implementation schedule.

V. Section-by-Section Analysis.

The following section-by-section analysis discusses the final revisions to the NRC's regulations regarding cyber security, and explains how the final rule differs from the language in the proposed rule. This final rule adds a new section (§ 73.77) to 10 CFR part 73 and revises three existing sections (§§ 73.8; 73.22 and 73.54) to make conforming changes.

(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, ~~Cyber Security Directorate,~~ 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.

(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.

Dated at Rockville, Maryland, this ___th day of , ~~2014~~2015.

For the Nuclear Regulatory Commission.

Annette L. Vietti-Cook,
Secretary of the Commission.