[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Part 73

[NRC-2014-0036]

RIN 3150-AJ37

Cyber Security Event Notifications

AGENCY: Nuclear Regulatory Commission.

ACTION: Final rule.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is adopting new cyber security regulations that govern nuclear power reactor licensees. This final rule codifies certain reporting activities associated with cyber security events contained in security advisories issued by the NRC. This rule establishes new cyber security event notification requirements that 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 provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat.

DATES: *Effective Date*: This final rule is effective **[INSERT DATE 30 DAYS AFTER THE DATE OF PUBLICATION]**. *Compliance Date*: Compliance with this final rule is required by **[INSERT DATE 180 DAYS AFTER THE DATE OF PUBLICATION]**, for those licensed to operate under parts 50 and 52 of Title 10 of the *Code of Federal Regulations* (10 CFR) and subject to § 73.54.

ADDRESSES: Please refer to Docket ID NRC-2014-0036 when contacting the NRC about the availability of information for this action. You may obtain publicly-available information related to this action by any of the following methods:

- **Federal Rulemaking Web Site:** Go to http://www.regulations.gov and search for Docket ID NRC-2014-0036. Address questions about NRC dockets to Carol Gallagher; telephone: 301-415-3463; e-mail: Carol.Gallagher@nrc.gov. For technical questions, contact the individuals listed in the FOR FURTHER INFORMATION CONTACT section of this document.

- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly-available documents online in the ADAMS Public Documents collection at http://www.nrc.gov/reading-rm/adams.html. To begin the search, select "ADAMS Public Documents" and then select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to pdr.resource@nrc.gov. The ADAMS accession number for each document referenced (if it is available in ADAMS) is provided the first time that it is mentioned in the SUPPLEMENTARY INFORMATION section.

- **NRC's PDR:** You may examine and purchase copies of public documents at the NRC's PDR, Room O1-F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852.

FOR FURTHER INFORMATION CONTACT: Robert H. Beall, Office of Nuclear Reactor Regulation, telephone: 301-415-3874, e-mail: Robert.Beall@nrc.gov, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

SUPPLEMENTARY INFORMATION:

TABLE OF CONTENTS:

I. Background.

On July 9, 2008, in SECY-08-0099, "Final Rulemaking – Power Reactor Security Requirements" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML081650474), the NRC staff recommended the Commission approve a final rule

amending the NRC's Power Reactor Security Requirements. The NRC staff also recommended removing sections in the Power Reactor Security Requirements rule on new and revised security notification requirements in § 73.71 and appendix G of part 73 of title 10 of the *Code of Federal Regulations* (10 CFR), "Reportable Safeguards Events," and placing them in a new proposed enhanced weapons rulemaking. In SRM-SECY-08-099, dated December 17, 2008 (ADAMS Accession No. ML083520252), the Commission approved the Power Reactor Security final rule and the bifurcation of the security notification requirements in § 73.71 and appendix G to 10 CFR part 73 to the new proposed enhanced weapons rule.

On June 27, 2010, in SECY-10-0085, "Proposed Rule: Enhanced Weapons, Firearms Background Checks and Security Event Notifications" (ADAMS Accession No. ML101110121), the NRC staff recommended delegating to the Office of the Executive Director for Operations the authority to issue new cyber security notification changes in the proposed enhanced weapons rule for publication in the *Federal Register,* as well as issue draft implementing guidance on the proposed rule. On October 19, 2010, in SRM-SECY-10-0085, "Proposed Rule: Enhanced Weapons, Firearms Background Checks and Security Event Notifications" (ADAMS Accession No. ML102920342), the Commission directed the NRC staff to publish a proposed rule implementing requirements for enhanced weapons, revised physical security event notifications, and adding new cyber security event notifications. This proposed rule was published in the *Federal Register* for comment on February 3, 2011 (76 FR 6199). The public was provided a total of 180 days to review and comment on the proposed rule and associated guidance.

In SECY-12-0125, "Interim Actions to Execute Commission Preemption Authority Under Section 161A of the Atomic Energy Act of 1954, as Amended," dated September 20, 2012 (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, therefore avoiding any further delay associated with the aforementioned Firearms Guidelines revision. In addition, this action would supplement the existing cyber security requirements (i.e., § 73.54, "Protection of Digital Computer and Communication Systems and Networks") included in the 2009 power reactor security rule (76 FR 6199; 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 those public comments. Additionally, Draft Regulatory Guide (DG)-5019, Revision 1, "Reporting and Recording Safeguards Events" (ADAMS Accession No. ML100830413), 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 (RG) (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 (CER), as approved by

SRM-SECY-0032, “Consideration of the Cumulative Effects of Regulation in the Rulemaking Process,” dated October 11, 2011 (ADAMS 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 § 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 § 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 play 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 the NRC in achieving its strategic communications mission by informing the U.S. 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. 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 (§ 73.54). The addition of cyber security event notification requirements supplements § 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 § 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 62664), 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 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 than 50 people. Additional individuals remotely participated in the meeting through audio teleconferencing and webinar. Presenters at the meeting included NRC staff, the Bureau of

Alcohol, Tobacco, Firearms and Explosives, and the Federal Bureau of Investigations (FBI). Since the NRC was not accepting public comments, the meeting was not transcribed; however, a meeting summary and the handouts from the meeting are available in ADAMS under Accession No. ML111720007.

The NRC staff also met with internal and external stakeholders on July 31, 2014. This public meeting was to discuss the draft final rule implementation date for the cyber security event notification requirements. The public meeting was held at the NRC Headquarters in Rockville, Maryland, and it was attended by six individuals in person and eight individuals remotely through audio teleconferencing and webinar. The NRC staff presented the current status of the draft final cyber security event notifications rule and the draft final implementation date. The NRC transcribed the meeting in order to capture public input on the draft final implementation date. The feedback from this meeting, as well as all the previous interactions, informed the NRC's schedule for the implementation of the new cyber security event notification requirements. The meeting summary, handouts, and a transcript of the meeting are available in ADAMS under Accession No. ML14240A404.

B. Opportunity for Public Comment

The proposed rule was published in the *Federal Register* on February 3, 2011 (76 FR 6199), and the public comment period closed on August 4, 2011. On the same day the NRC also published a separate notice requesting comment on DG-5019, Revision 1, "Reporting and Recording Safeguards Events." The NRC received a total of 14 submittals on the proposed rule and draft guidance relating to enhanced weapons, firearms background checks and security event notifications (which included cyber security event notifications). The majority of comments came from the Nuclear Energy Institute (NEI) on behalf of the nuclear power reactor licensees.

IV. Public Comment Analysis.

The proposed enhanced weapons rule was published February 03, 2011 (76 FR 6199), and the public comment period closed on August 04, 2011. On the same day the NRC also published a separate notice requesting comment on DG-5019, Revision 1, "Reporting and Recording Safeguards Events."

The NRC received 14 submittals on the proposed rule and draft guidance. The NRC also received one comment on the proposed implementation date during the July 31, 2014, public meeting. Comments specific to cyber security event notifications in the proposed enhanced weapons rule and DG-5019, Revision 1, were identified and are addressed in this final rule. The comments specific to the proposed rule on Enhanced Weapons, Firearms Background Checks, and Security Event Notifications (76 FR 6200) are not addressed in this final rule and will be addressed in a subsequent rulemaking. In addition, certain event notification comments in the proposed rule that were generic (e.g., comments referring to four-hour notifications in general) are addressed for cyber security events in this final rule. The submittals containing comments specific to cyber security event notifications were consolidated into a single document (ADAMS Accession No. ML14226A596) that assigns the comment designators (e.g., NEI-155) used in this final rule. In the proposed rule and draft guidance, the cyber security event notifications aligned with physical security event notifications with a focus on compensated and uncompensated events. However, based on public comments, the final rule and regulatory guidance now aligns more closely with § 73.54 with a focus on adverse impacts to SSEP functions.

A. Public Comments on Proposed Rule

Comment 1: One commenter stated that neither § 73.71 nor appendix G to 10 CFR part 73 contains an effective date for cyber security reporting requirements, and recommended that the reporting requirements align with the date the cyber security plan becomes effective. [NEI-155]

Response: The NRC disagrees with this comment. Notification of a cyber security event is necessary to assist the NRC in assessing and evaluating issues with potential cyber security-related implications in a timely manner, determining the significance and credibility of the identified issue(s), and providing recommendations and/or courses of action to NRC management. Currently, licensees are reporting certain cyber security events voluntarily to the NRC. However, because this is done voluntarily there could be certain cyber security events that may not be reported to the NRC in a timely manner or reported at all. The cyber security event notifications final rule removes the voluntary aspects of reporting certain cyber security events, provides regulatory stability, and ensures the NRC is notified in a timely manner.

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. Like the attacks of September 2001, a cyber attack has the capability to be launched against multiple targets simultaneously or spread quickly throughout multiple sectors of critical infrastructure. In light of these potential consequences, the NRC does not want to delay the implementation of the cyber security event notification final rule to match the effective date of each licensee's cyber security plan (i.e., Milestone 8) because those cyber security plans may not be fully effective for several years.

The final rule will become effective 30 days after publication in the *Federal Register*. The compliance date will be 180 days after publication (consistent with the implementation schedule described in the proposed rule) to allow licensees time to revise their event notification

procedures and train personnel on event notifications specific to cyber security (i.e., identification, reporting). The cyber security event notification final rule is consistent with existing notification processes (i.e., §§ 50.72 and 73.71) and aligns closely with § 73.54 (e.g., adverse impacts to SSEP functions) as well as current voluntary reporting activities associated with cyber security requiring less time for implementation. In addition, the cyber security event notification final rule complements the implementation of Milestones 1 through 7. For example, the identification of critical systems and critical digital assets (Milestone 2), the implementation of a deterministic one-way device (Milestone 3), and access controls for portable media devices (Milestone 4) are all programs that when properly implemented and maintained, should identify and mitigate adverse impacts to SSEP functions. The cyber security event notification final rule requires licenses to notify the NRC when a cyber attack caused or could have caused an adverse impact to SSEP functions. These factors, along with the importance of the NRC strategic communications mission of informing the 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, support the need for the 180-day implementation schedule.

Comment 2: One commenter indicated that critical digital assets (CDAs) that are not part of a target set should not have the same sensitivity as those CDAs that are contained within a target set. [NEI-156]

Response: The NRC disagrees with this comment. The NRC staff has recognized that a graded approach to controls required for CDAs is warranted based on the ability to detect and mitigate the consequences of a cyber attack. However, the cyber security event notification requirements focus on events that have or could have an adverse impact to SSEP functions,

and thereby incorporates consideration of protections that prevent successful cyber attacks. Therefore, the notification requirements cover all CDAs and critical systems within the scope of § 73.54, which includes: safety-related and important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; and support 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, therefore 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 § 50.72(b)(2)(xi). In addition, unsuccessful cyber attacks has been clarified to align more closely with § 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 have been clarified to address suspected or actual cyber attacks initiated by personnel with physical or electronic access and were 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 § 73.54.

Comment 4: One commenter suggested adding the word “significant” in front of cyber security events. [NEI-167]

Response: The NRC disagrees with this comment. Prefacing the phrase “cyber security events” with “significant” does not add clarity to the rule. The NRC is requiring only those cyber security events associated with actual or potential adverse impacts to be reported. The NRC has changed the rule text and associated guidance to align more closely with § 73.54 and distinguishes cyber security events by whether an adverse impact has occurred (or not) to SSEP functions as a result of a cyber attack.

Comment 5: One commenter suggested removing the requirement in appendix G of 10 CFR part 73 regarding the recording of events in a safeguards event log. The commenter suggested licensees use the corrective action program instead of using a separate log. [NEI-18, 194, 202]

Response: The NRC agrees with this comment. The cyber security plan for each licensee describes the use of the corrective action program to track, trend, correct, and prevent recurrence of cyber security failures and deficiencies. Therefore, the cyber security event notification rule text (§ 73.77) has been revised to require licensees to use their corrective action program to record vulnerabilities, weaknesses, failures and deficiencies in their cyber security program. Regulatory Guide 5.83 has also been revised to reflect this change.

Comment 6: The NRC received a comment regarding the use of the term “compensatory” in the context of cyber security, stating that the term is unclear, and is not defined in the two cyber

security plan (CSP) templates, Appendix A of RG 5.71, and Appendix A of NEI 08-09. [NEI-153, 165]

Response: The NRC agrees with this comment. The term "compensatory" is not defined in either CSP template or in other NRC guidance related to cyber security. 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 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. Regulatory Guide 5.83 has been revised to reflect this new approach.

Comment 8: One commenter proposed changes to the rule language, paragraph I.(h)(1) in appendix G of 10 CFR part 73, 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 sabotage" are not needed to provide clarity under this approach. Regulatory Guide 5.83 has been revised to reflect this new approach.

Comment 9: One commenter proposed revising the proposed rule language in paragraph I.(h)(2) in appendix G of 10 CFR part 73 to include language regarding the defense-in-depth protective strategies required by § 73.54(c)(2). [NEI-158]

Response: The NRC agrees with this comment. The NRC evaluated the proposed rule language and determined that items to be reported under this section are duplicative. Based on public comments, the NRC developed a different approach for determining cyber security event notifications, one based on whether the cyber attack caused an adverse impact (or not) to SSEP functions. Regulatory Guide 5.83 has been revised to reflect this approach.

Comment 10: One commenter proposed language to paragraph I.(c)(1) in appendix G of 10 CFR part 73 to report only instances of suspicious or surveillance activity or attempts to access systems, networks, or equipment that is within the scope of § 73.54. Additionally, the commenter recommended deleting proposed language that would include reporting of additional types of events like potential tampering or potential destruction of networks, systems, or equipment. [NEI-159]

Response: The NRC disagrees with this comment. The commenter's reference to paragraph I.(c)(1) in appendix G of 10 CFR part 73 appears to be misquoted. The changes proposed by the commenter would amend paragraph II.(c)(1) in appendix G. The NRC believes that surveillance activities are captured within activities that indicate intelligence gathering or pre-operational planning and should be reported, and has made appropriate changes to this final rule. The NRC has clarified and relocated this requirement to the eight-hour notifications, now designated as § 73.77(a)(3). Additionally, the NRC moved the reporting of potential tampering, or potential destruction of networks, systems or equipment from this requirement and they are now captured under § 73.77(a)(1), (a)(2)(i), and (a)(2)(ii) of this final rule.

Comment 11: One commenter indicated that paragraph I.(c)(2) in appendix G of 10 CFR part 73 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 paragraph I.(c)(2) in appendix G of 10 CFR part 73 appears to be misquoted. The changes proposed by the commenter would amend paragraph II.(c)(2) in appendix G. The final rule text has been revised to remove all duplicative language and is aligned more closely with the requirements in § 73.54 (i.e., adverse impacts to SSEP functions). This revised requirement is designated as § 73.77(a)(2)(i). Regulatory Guide 5.83 has been revised to reflect this change.

Comment 12: One commenter proposed changes to paragraph III in appendix G of 10 CFR part 73 to clarify the language under eight-hour reportable events to be consistent with § 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 § 73.54. The implementation of security controls to protect CDAs from cyber attacks as described in § 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. Regulatory Guide 5.83 has been revised to reflect this new approach.

Comment 13: One commenter recommended adding "that would" to a proposed 24-hour recordable event provision in paragraph IV.(a)(2) in appendix G of 10 CFR part 73. Specifically, the commenter recommended that the proposed appendix G provision regarding compensated security events state in part as follows:

> (a) Any failure, degradation, or discovered vulnerability in a safeguards system, had compensatory measures not been established, that could … (2) Degrade the effectiveness of the licensee's or certificate holder's cyber security program that would allow unauthorized or undetected access to any systems, networks, or equipment that fall within the scope of § 73.54 of this part.

The commenter stated that this re-worded provision would better align with another proposed provision in paragraph I.(h)(2) in appendix G of 10 CFR part 73. [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 other public comments, the NRC re-evaluated 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, as reflected in the new § 73.77(b)(1) provision being added

as part of this final rule, licensees will be required to use their corrective action program to record vulnerabilities, weaknesses, failures, and deficiencies in their cyber security program within twenty-four hours of their discovery. Regulatory Guide 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 § 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 § 73.54. However, the NRC disagrees with changing the word "could" to "would," because these words are correctly used in their respective rules. Section 73.54 addresses hypothetical future cyber attacks that must be protected against, while this rule describes notifications that licensees 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 impact to SSEP functions; this type of attack is to be reported within four-hours after discovery. The NRC has revised RG 5.83 to reflect this new approach that aligns more closely with § 73.54 regarding adverse impacts to SSEP functions.

Comment 15: One commenter proposed deleting the requirement in paragraph II.(c)(2) in appendix G of 10 CFR part 73 because the commenter believes it is duplicated in paragraph I.(h)(2) in appendix G. [NEI-169]

Response: The NRC agrees that the proposed paragraph II.(c)(2) in appendix G of 10 CFR part 73 is similar to paragraph I.(h)(2) in appendix G; therefore, the NRC has revised the final rule to make it clear exactly what types of cyber attacks are reported to the NRC. Specifically, the final rule language reflects a different approach for determining cyber security event notifications, eliminates duplicative requirements, and provides clarity based on whether the attack caused an adverse impact (or not) to SSEP functions. Regulatory Guide 5.83 has been revised to reflect this new approach.

Comment 16: One commenter proposed rule language in paragraph I.(h)(2) in appendix G of 10 CFR part 73 that would change events that "could" allow unauthorized or undetected access into systems, networks, or equipment to events that "would" allow unauthorized or undetected access into systems, networks, or equipment. [NEI-170]

Response: The NRC disagrees with this comment, but has, for other reasons, revised the requirement in the final rule. The objective of this reporting requirement is not to have licensees confirm with the NRC that a cyber attack has occurred. Rather, the objective is to report conditions in which such an attack could have occurred. The NRC continues to believe that licensees should report events or circumstances that could have resulted in undetected or compromised conditions at the facility. However, the NRC staff evaluated the language in the proposed rule and determined that items reported under this section were duplicative and therefore removed this requirement from the final rule text. Regulatory Guide 5.83 was revised to reflect this change.

Comment 17: One commenter recommended four and eight-hour notifications be consolidated into "within 24-hours" to mitigate event reporting violations. [B&W-30]

Response: The NRC disagrees with this comment. The four and eight-hour notifications include cyber attacks and activities (i.e., precursors to an attack) where the timeliness of information allows the NRC to conduct additional notifications (to DHS, other NRC licensees), assists the Federal Government and/or other NRC licensees to take mitigative measures to prevent a widespread cyber attack, and allows the NRC to respond to public and/or media inquiries. In addition, notifications to a local, State or other Federal agency is consistent with existing NRC regulations at § 50.72(b)(2)(xi).

Comment 18: One commenter recommended clarification on cyber security event notification requirements regarding exclusion of licensees not subject to § 73.54. [NFS-11, 12]

Response: The NRC agrees with this comment. The final rule text was revised and clarified to only apply to licensees subject to the provisions of § 73.54.

Comment 19: One commenter recommended that “one-hour notifications” should be related to a specific threat or attempted threat to the facility, and events that do not pose an actual threat should be “eight-hour notifications.” [NEI-22, 33]

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. Cyber attacks that adversely impacted SSEP functions are now one-hour notifications. Cyber attacks that could have caused an adverse impact to SSEP functions are now four-hour notifications, and activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack are now eight-hour notifications.

Comment 20: One commenter recommended adding the word “malevolent” to proposed requirements describing an unauthorized operation or tampering event to rule out human error events. [NEI-31, 48]

Response: The NRC disagrees with this comment. The word “malevolent” is unnecessary because, under the new approach, notification of such events is not based on the intent of the act, but based on the potential consequences of the event (i.e., adverse impact (or not) to SSEP functions). No change has been made to the final rule based on this comment.

Comment 21: One commenter recommended clarifying requirements regarding law enforcement interactions. The commenter recommended that notifications that could result in public or media inquiries should not duplicate notifications made under other NRC regulations such as § 50.72(b)(2)(xi). [NEI-35]

Response: The NRC agrees with this comment. The final rule has been revised to eliminate duplication of notifications made under other NRC regulations. Regulatory Guide 5.83 has been revised to reflect this change.

Comment 22: One commenter recommended clarification regarding retraction of reports determined later to be invalid. The commenter stated that the notification may not be invalid, but later be determined it does not meet the threshold of a one-, four-, or eight-hour notification (i.e., recordable event). [NEI-40]

Response: The NRC agrees with this comment. The final rule and RG 5.83 have been revised to clarify that retraction of reports can include valid reports which later do not meet the threshold of a one-, four-, or eight-hour notification.

Comment 23: One commenter recommended adding the term “malicious intent” to each of the eight-hour reportable events regarding unauthorized operation or tampering events. [NEI-53, 112]

Response: The NRC disagrees with this comment. The term “malicious intent” is unnecessary because, under the new approach, notification of such events is not based on the intent of the act, but based on the potential consequences of the event (i.e., adverse impact (or not) to SSEP functions).

Comment 24: One commenter recommended that cyber attack reporting needs to be synchronized with NEI 08-09 and RG 5.71 to ensure reporting criteria are well-defined. [NEI-69]

Response: The NRC agrees with this comment. The final rule reflects an approach that aligns more closely with § 73.54 and RG 5.71 and provides additional clarity on cyber security event notification criteria (i.e., adverse impact to SSEP functions). Regulatory Guide 5.83 has also been revised to reflect this new approach.

Comment 25: One commenter recommended deleting the requirements and guidance for written follow-up reports on several reporting events (four and eight-hour notifications). [NEI-117]

Response: The NRC disagrees with this comment. Submission of written follow-up reports is consistent with existing NRC regulations and provides the NRC with information that may not have been available at the time of the notification.

Comment 26: One commenter recommended that the final rule require licensees to notify their local FBI Joint Terrorism Task Force (JTTF) of suspicious events as contained in voluntary guidance documents and eliminate or reduce the timeliness of reporting such events to the NRC. [Hardin-3]

Response: The NRC disagrees with this comment. The reporting of events to the FBI JTTF is voluntary and as such, does not have a timeliness requirement. This final rule requires notification to the NRC within a stated time for activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack. Notifications of activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack will be evaluated and forwarded as appropriate by the NRC to federal law enforcement agencies and the intelligence community as part of the National threat assessment process.

B. Public Comments on Draft Guide-5019

Comment 1: One commenter proposed removing the terms such as “could,” “likelihood,” and “likely to” from DG-5019. [NEI-21, 166]

Response: The NRC disagrees with this comment. The use of the terms "could," “likelihood," and "likely to" within DG-5019 is consistent with existing NRC reporting guidelines (NUREG-1022, “Event Report Guidelines for 10 CFR 50.72 and 50.73” (ADAMS Accession No. ML13032A220)).

Comment 2: One commenter proposed revising section 2.3.2, item r, of DG-5019 to include, "Confirmed cyber attacks on computer systems that adversely affected safety, security, and emergency preparedness systems are reportable" instead of, "may adversely affect" and removing item aa of section 2.3.2 due to redundancy. [NEI-171]

Response: The NRC agrees with this comment. The staff evaluated both items in section 2.3.2 of DG-5019 and revised RG 5.83 to reflect the proposed changes.

Comment 3: One commenter proposed revising section 2.3.2, item bb.(2), of DG-5019 to include the word "cyber" before security program and security measures. [NEI-172]

Response: The NRC agrees with this comment, yet has, for other reasons removed this material from the final guidance. The final guidance reflects changes made to the final rule that aligns more closely with § 73.54 (i.e., adverse impacts to SSEP functions), and in the process, the NRC staff determined that item bb.(4) was no longer required.

Comment 4: One commenter proposed revising section 2.3.2, item bb.(3), of DG-5019 to state that events caused inadvertently by an individual and not resulting in a threat to facility security, would be a recordable event, and events caused by a cyber attack resulting in an adverse impact to SSEP functions would be a one-hour reportable event. [NEI-173]

Response: The NRC agrees with this comment. The item was revised in RG 5.83 to distinguish recordable inadvertent non-threatening events from those cyber attacks causing adverse impacts, which are one-hour notifications.

Comment 5: One commenter recommended moving section 2.3.2, item bb.(4) from (one-hour notification examples) to section 2.6.2 (eight-hour notification examples) in DG-5019 regarding attempts by unauthorized persons. [NEI-174]

Response: The NRC disagrees with this comment, yet has, for other reasons, removed this material from the final guidance. The final guidance reflects changes made to the final rule that aligns more closely with § 73.54 (i.e., adverse impacts to SSEP functions), and in the process, staff determined that item bb.(4) was no longer required.

Comment 6: One commenter recommended moving section 2.3.2, item bb.(5), (one-hour notification examples) to section 2.6.2 (eight-hour notification examples) in DG-5019 regarding cyber attacks thwarted by security controls. [NEI-175]

Response: The NRC disagrees with this comment, yet has, for other reasons, removed this material from the final guidance. The final guidance reflects changes made to the final rule that aligns more closely with § 73.54 (i.e., adverse impacts to SSEP functions), and in the process, staff determined that item bb.(5) was no longer required.

Comment 7: One commenter proposed removing the terms “unauthorized software” and “firmware” from section 2.3.2, item cc, because of redundancy with the term malware. [NEI-176]

Response: The NRC disagrees with this comment, but for other reasons, the guidance has been revised. There is a difference between malware, and unauthorized software, or firmware, and therefore there is no redundancy. However, the staff re-evaluated the language and determined the example is not consistent with § 73.54 and RG 5.71. Therefore, the example was not included in RG 5.83.

Comment 8: One commenter proposed changes to section 2.3.2, item dd, of DG-5019 where the result was changed from compromising the CDA to an adverse impact to SSEP functions. [NEI-177]

Response: The NRC agrees with the proposed changes to the item; however, due to changes in the final rule language, this item was clarified and moved to a four-hour notification example within RG 5.83.

Comment 9: One commenter recommended removing section 2.3.2, item ee, of DG-5019, because there are no NRC regulations covering "sensitive cyber security data." [NEI-178]

Response: The NRC agrees with this comment. The item has been removed from RG 5.83.

Comment 10: One commenter recommended clarifying section 2.3.2, item ff, of DG-5019, and proposed the term "cyber intrusion detection capability" instead of the term "cyber intrusion detection system." [NEI-179]

Response: The NRC disagrees with this comment, yet has, for other reasons, removed this material from the final guidance. The item was not included in RG 5.83 because it was not consistent with § 73.54 and RG 5.71.

Comment 11: One commenter recommended section 2.3.2, item hh, of DG-5019 be revised to be consistent with § 73.54(a)(2) by removing the term uncompensated. [NEI-181]

Response: The NRC disagrees with this comment, yet has, for other reasons, removed this material from the final guidance. The staff reviewed the item and determined it was not consistent with 10 CFR 73.54 and RG 5.71 and removed it from RG 5.83.

Comment 12: The NRC received several comments regarding redundant material within section 2.3.2., item hh, of DG-5019. [NEI-180, 182, 185]

Response: The NRC agrees with this comment. Staff removed items gg, ii and ll from section 2.3.2 in RG 5.83 because they were redundant with item hh regarding unauthorized access to CDAs.

Comment 13: One commenter recommended moving section 2.3.2, item jj, of DG-5019 from the one-hour notification examples to the four-hour notification examples in section 2.5.2 regarding discovery of falsified identification badges. [NEI-183]

Response: The NRC agrees in part with this comment, that the item should be moved. However, under the new approach, this item is consistent with eight-hour notifications (i.e., activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack) and was moved in final guidance to the eight-hour notification examples.

Comment 14: One commenter recommended revising section 2.3.2, item kk, of DG-5019 replacing the term “could” with “would.” [NEI-184]

Response: The NRC disagrees with this comment, yet has, for other reasons, removed this material from the final guidance. The NRC staff re-evaluated this item, determined it was not consistent with the final rule, and deleted it from RG 5.83.

Comment 15: One commenter recommended removing section 2.3.2, item mm, of DG-5019 because it duplicates 2.3.2, item y, regarding safeguards reporting requirements. [NEI-186]

Response: The NRC agrees with this comment. The item has been removed from RG 5.83.

Comment 16: One commenter recommended removing section 2.3.2, item nn, of DG-5019 because there are no NRC requirements for maintaining cyber security response personnel staffing levels. [NEI-187]

Response: The NRC agrees with this comment. The item has been removed from RG 5.83.

Comment 17: One commenter recommended revising section 2.3.2, item oo, of DG-5019 to change the phrase, “could increase the likelihood of an attempted attack” to the phrase, “would result in an attack.” [NEI-188]

Response: The NRC disagrees with this comment, yet has, for other reasons, revised this material in the final guidance. This item has been revised in RG 5.83 to include any event that allows unauthorized or undetected access to a CDA that could be exploited in an attack to be reported within four hours of discovery.

Comment 18: One commenter recommended adding new examples to sections 2.3.2 and 2.5.2 of DG-5019. One example, (section 2.3.2) involved discovery of unauthorized user IDs and unauthorized configurations to cyber controls (e.g., firewall port opening, etc.). The other example (section 2.5.2) involved unauthorized attempts to probe CDAs including the use of social engineering techniques. [NEI-189, 190]

Response: The NRC agrees with the examples provided, and based on final rule text changes (cyber attacks initiated by personnel with physical or electronic access and activities that may indicate pre-operational planning), these items were included in RG 5.83.

Comment 19: One commenter recommended revising section 2.5.2, item kk, of DG-5019 to include the word cyber before the term security controls. [NEI-191]

Response: The NRC agrees with this comment. The item was revised in RG 5.83 to include the word cyber before security controls.

Comment 20: One commenter recommended removing section 2.5.2, item mm, of DG-5019 because it is redundant to section 2.5.2, item kk. [NEI-192]

Response: The NRC agrees with this comment. The item has been removed from RG 5.83.

Comment 21: One commenter recommended revising section 2.5.2, item oo, of DG-5019 to add Levels 3 and 4 to the description so the item is consistent with the definition provided in the glossary for a CDA. [NEI-193]

Response: The NRC disagrees with this comment, but for other reasons has revised the final guidance. The definition of a CDA in RG 5.83 was revised for consistency with the definition provided in RG 5.71.

Comment 22: One commenter recommended revising section 2.5.2, item qq, of DG-5019 or removing it altogether because reporting the high number of malware attempts on lower security

level networks that do not have the degree of protection of CDAs would be burdensome on the NRC and the licensee. [NEI-195]

Response: The NRC agrees with this comment. Based on final rule text changes, this item was revised in RG 5.83 narrowing the scope to attacks discovered or manifested on a CDA, critical system or protected network reducing the number of potential notifications on the licensee and the NRC.

Comment 23: One commenter recommended revising section 2.5.2, item rr, of DG-5019 to clarify the term “cyber systems.” [NEI-196]

Response: The NRC agrees with this comment. In RG 5.83 this item was revised for consistency with RG 5.71 and uses the terms “critical systems” and “CDAs.”

Comment 24: One commenter recommended removing the 15-minute reference in section 2.5.2, item ss, of DG-5019. [NEI-197]

Response: The NRC agrees with this comment. The final rule text does not contain any 15-minute notifications related to cyber security, and therefore, this item was revised in the final guidance to a four-hour notification example.

Comment 25: One commenter recommended revising or removing the paragraph before section 2.6.2, item h, in DG-5019 regarding cyber security events that interrupt or degrade the facility’s SSEP functions. [NEI-198]

Response: The NRC agrees with this comment, yet has, for other reasons removed this material from the final guidance. The final guidance reflects changes made to the final rule that aligns more closely with § 73.54 (i.e., adverse impacts to SSEP functions), and in the process, staff determined that this item was no longer required.

Comment 26: One commenter recommended revising section 2.6.2, item l, of DG-5019. The commenter recommended removing the term “failed” because a CDA could fail for non-malicious reasons and not be the result of a cyber attack or unauthorized activity. [NEI-199]

Response: The NRC agrees with this comment. There are many reasons a critical digital asset can fail that are not related to unauthorized activity or cyber attacks. Regulatory Guide 5.83 has been revised to reflect this change.

Comment 27: One commenter recommended revising section 5.3, item n, of DG-5019 because the term “compensated” is not defined. [NEI-200]

Response: The NRC agrees with this comment. This item was removed from RG 5.83.

Comment 28: One commenter recommended clarifying section 5.3, item o, of DG-5019 regarding individuals who are incorrectly authorized access to a CDA. [NEI-201]

Response: The NRC agrees with this comment. This item was removed from RG 5.83.

Comment 29: One commenter recommending adding items to section 5.3 of DG-5019 to include examples of cyber events that are compensated as proposed by paragraph IV.(a) in appendix G of 10 CFR part 73. [NEI-203]

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. Regulatory Guide 5.83 has been revised to reflect this new approach.

Comment 30: One commenter recommended changes to the definitions provided in the glossary of DG-5019. The commenter proposed changing "cyber attack" to be consistent with the definition provided in NEI 08-09 and changing "CDA" to only include digital computer, communication systems, and networks that fall within level 3 or 4 boundaries as well as a general comment that all definitions in the glossary be synchronized with code requirements and regulatory guides. [NEI-138, 204, 205]

Response: The NRC agrees in part with this comment. 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.

Comment 32: One commenter stated that the cyber security plan templates published by the NRC and NEI do not contain guidance for licensees to differentiate between events that are recordable versus reportable. [NEI-20, 154]

Response: The NRC agrees with this comment. Neither cyber security plan template issued by the NRC or NEI contains guidance for licensees on which events are recordable or reportable. However, DG-5019 provided guidance to licensees on events that are reportable and recordable related to cyber security event notifications. Consistent with Commission policy, the NRC is publishing with this final rule, final guidance, RG 5.83, "Cyber Security Event Notifications," which provides guidance to licensees on an acceptable method for meeting regulatory requirements. The final guidance has been revised to provide examples that differentiate between events that are reportable and recordable.

Comment 33: One commenter recommended revisions to NRC Form 366. The commenter recommended the NRC specify the type of content licensees should include in the abstract section of the form. [NEI-44, 118]

Response: The NRC disagrees with this comment. The NRC's Form 366 will not be revised. Regulatory Guide 5.83 will provide the specific type of content that should be included in the abstract section of NRC's Form 366.

Comment 34: One commenter recommended clarifying the guidance regarding elicitation of information from facility personnel relating to security or safe operation of the facility. The

commenter suggested adding the phrase “non-routine” regarding the elicitation of information to distinguish general public or media inquiries from elicitations that could be indicative of suspicious activity. [NEI-52, 95, 99]

Response: The NRC agrees with this comment. Regulatory Guide 5.83 has been revised to provide a distinction between common inquiries (e.g., public and media inquiries) and uncommon inquiries (e.g., activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack).

Comment 35: One commenter recommended clarifying the examples of one-hour notifications and including “real life” examples. [NEI-71]

Response: The NRC agrees with this comment. The NRC staff reviewed previous “real life” examples and included them in final guidance. In addition, the new approach for one-hour notifications (i.e., adverse impacts to SSEP functions) provides additional clarity.

Comment 36: One commenter recommended changes to the examples involving the compromise of CDAs. The commenter stated that section 2.3.2 of DG-5019, items (aa) and (bb) were duplicative, and that two supporting examples (4 and 5) were not within the scope of one-hour notifications (i.e., adverse impact to SSEP functions). [NEI-94]

Response: The NRC agrees with this comment. Regulatory Guide 5.83 has been revised to delete one of the duplicate items and to remove the two supporting examples from the remaining item.

Comment 37: One commenter recommended moving an example related to unauthorized attempts to steal business secrets or sensitive information to the cyber security event notification examples. [NEI-100]

Response: The NRC disagrees with this comment. The final rule reflects an approach that aligns more closely with § 73.54 and RG 5.71, and provides clarity to cyber security event notification criteria. Unauthorized attempts to access business and trade sensitive information is outside the scope of § 73.54, and no changes to the rule or RG 5.83 were made based on this comment

Comment 38: One commenter recommended clarifying the example regarding unsubstantiated cyber threats related to harassment, including threats that could represent tests of response capabilities. The commenter stated the example was confusing and too broad in scope. [NEI-111]

Response: The NRC agrees with this comment. The NRC has revised the example to clarify the scope of the cyber attacks to be reported (i.e., a cyber attack that could have caused an adverse impact to SSEP functions).

Comment 39: One commenter requested NRC clarify the guidance on unplanned missed cyber vulnerability assessments. [NEI-131]

Response: The NRC agrees with this comment. Regulatory Guide 5.83 was revised to clarify the treatment of missed cyber vulnerability assessments. The CSP states the periodicity that cyber vulnerability assessments are performed (quarterly). If a cyber vulnerability assessment exceeds the periodicity specified in the CSP, it would be considered a 24-hour recordable event.

C. Public Comments on Proposed Implementation Date from July 31, 2014, Public Meeting

Comment 1: One commenter raised a concern that by issuing the Cyber Security Event Notifications (CSEN) final rulemaking now it may delay full implementation of § 73.54 because of the impact on resources. The commenter stated that licensees may have to divert some resources from implementing the cyber security program to implementing the CSEN requirements.

Response: The NRC agrees in part with this comment. The NRC staff recognizes that this rule will have an impact on licensee resources (similar skillsets required for CSEN and cyber security program implementation). The NRC staff acknowledges this and is conducting CER 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., §§ 50.72 and 73.71) and aligns closely with § 73.54 and the current voluntary reporting initiatives 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 (*see* http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf). 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.

Section 73.8, Information collection requirements: OMB approval.

The NRC is amending § 73.8 to add § 73.77 to paragraph (b) that provides the approved information collection requirements contained in 10 CFR part 73 under control number 3150-0002. In addition, the NRC is amending § 73.8 to add § 73.77 to paragraph (c)(1) that provides that NRC Form 366 is approved under control number 3150-0104.

Section 73.22, Protection of Safeguards Information: Specific requirements.

The NRC is amending § 73.22(f)(3) to add the sentence, "Cyber security event notifications required to be reported pursuant to § 73.77 are considered to be extraordinary conditions" to the end of the paragraph.

Section 73.54, Protection of digital computer and communication systems and networks.

The NRC is amending § 73.54 to add a new paragraph (d)(4) that reads, "Conduct cyber security event notifications in accordance with the provisions of § 73.77." This new requirement guides the licensee to the correct 10 CFR part 73 section for conducting cyber security event notifications.

Section 73.77, Cyber security event notifications.

The NRC has moved cyber security event notifications requirements that were proposed to be added to § 73.71 and appendix G to a newly created section (§ 73.77) within 10 CFR part 73.

Section 73.77(a)(1) requires licensees to notify the NRC 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. This requirement differs from the proposed rule language, it has been revised to more closely align with § 73.54 and to remove the term “uncompensated cyber security events” because it was unclear and not defined within the CSP.

Section 73.77(a)(2) requires licensees to notify the NRC within four-hours.

Section 73.77(a)(2)(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. This requirement differs from the proposed rule; it has been revised to more closely align with § 73.54. In addition, the final rule distinguishes between four-hour and eight-hour notifications.

Section 73.77(a)(2)(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. This requirement differs from the proposed rule; it has been revised to capture cyber attacks (e.g., tampering) that may not have any impact on SSEP functions, but may indicate an internal threat.

Section 73.77(a)(2)(iii) after notification of a local, State, or other Federal agency (e.g., local law enforcement, FBI, etc.) of an event related to implementation of their cyber security program. The final rule includes other types of agencies besides law enforcement (e.g., DHS, etc.) to maintain consistency with existing NRC reporting requirements (e.g., § 50.72).

Section 73.77(a)(3) requires licensees to notify the NRC 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. Requirements for “suspicious cyber events” have been revised and moved from four-hour notifications in the proposed rule to eight-hour notifications in the final rule. This requirement now captures activities that are associated with precursors to a cyber attack (e.g., activities related to intelligence gathering or pre-operational planning).

Section 73.77(b) requires licensees to record certain cyber security events in their site corrective action program (CAP) within 24-hours of their discovery. The proposed rule required licensees to use a Safeguards Event Log; to prevent duplication of effort, the final rule requires licensees to use their site CAP.

Section 73.77(b)(1) requires licensees to use their site CAP to record vulnerabilities, weaknesses, failures, and deficiencies in their § 73.54 cyber security program. This requirement has been revised to align with NRC physical protection program requirements in § 73.55(b)(10) regarding the use of the site CAP to track, trend, correct, and prevent recurrence of failures and deficiencies.

Section 73.77(b)(2) requires licensees to record notifications made under paragraph (a) of § 73.77.

Section 73.77(c) provides the process for conducting cyber security event notifications.

Section 73.77(c)(1) has been revised from the proposed rule to include the Emergency Notification System (ENS) as the primary means for conducting notifications, instead of any

available telephone system. Using the ENS is consistent with existing NRC regulations for conducting notifications (e.g., § 50.72).

Section 73.77(c)(3) in the final rule was revised to remove a reference to paragraph III in appendix A of 10 CFR part 73 that provided instructions on requesting a transfer to a secure phone. The current appendix A in 10 CFR part 73 does not contain a paragraph III and conforming changes to appendix A are not part of this final rule. Section 73.77(c)(3) was revised to reference appendix A and request transfer to a secure phone.

Sections 73.7(c)(6), "Declaration of emergencies," and 73.77(c)(7), "Elimination of duplication," were moved in the final rule from the "Written Security Follow-up Reports" section into the "Notification Process" section because they contain notification-specific information. In addition, due to the narrowed scope of this final rule, the proposed rule referenced several sections of the NRC's regulations (e.g., § 70.50) that are not being revised by this final rule.

Section 73.77(d), "Written security follow-up reports," establishes the necessary regulatory framework to facilitate consistent application of Commission requirements for written security follow-up reports for cyber security event notifications.

VI. Regulatory Flexibility Certification.

Under the Regulatory Flexibility Act (5 U.S.C. 605(b)), the NRC certifies that this rule does not have a significant economic impact on a substantial number of small entities. This final rule affects only the licensing and operation of nuclear power plants. The companies that own these plants do not fall within the scope of the definition of "small entities" set forth in the Regulatory Flexibility Act or the size standards established by the NRC (10 CFR 2.810).

VII. Regulatory Analysis.

The NRC has prepared a final regulatory analysis for this final rule. The analysis examines the costs and benefits of the alternatives considered by the NRC. The regulatory analysis is available as indicated in Section XVII., "Availability of Documents," of this document.

VIII. Backfitting and Issue Finality.

The final rule imposing new cyber security event notifications affects information collection and reporting requirements and is not considered to be a backfit, as presented in the charter for NRC's Committee to Review Generic Requirements. Therefore, a backfit analysis has not been completed for any of the provisions of this final rule.

IX. Cumulative Effects of Regulation.

While the proposed rule was issued prior to the formal CER requirements promulgated by SRM-SECY-0032, the intent of CER was still met. For example, the draft guidance was issued for comment concurrent with the proposed rule, a public meeting was conducted during the development of the proposed rule, a public meeting on implementation was conducted during the final rule stage, and the final guidance will be issued with the final rule.

The NRC staff engaged external stakeholders at public meetings and by soliciting public comments on the proposed rule and draft guidance documents. A public meeting was held at NRC Headquarters on June 1, 2011, to discuss the proposed rule, the draft implementation plan, and draft guidance.

In addition, on July 31, 2014, a public meeting was held at the NRC Headquarters on the draft final implementation plan for the final rule (a type of meeting specifically contemplated by

the NRC's CER effort). Prompt notification of a cyber attack is vital to the NRC's ability to take immediate action in response to a cyber attack, which contributes to protecting the public health and safety or the common defense and security. The NRC's strategic communications mission 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. Environmental Assessment and Final Finding of No Significant Environmental Impact.

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.

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 3150-0230 and 3150-0104.

The burden to the public for these information collections is estimated to average 39.4 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments on any aspect of these information collections, including suggestions for reducing the burden, to the Freedom of Information Act, Privacy, and Information Collections Branch (T-5 F53), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0230 and 3150-0104), Office of Management and Budget, Washington, DC 20503 or by e-mail to oira_submission@omb.eop.gov.

Public Protection Notification.

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

XIII. Congressional Review Act.

In accordance with the Congressional Review Act of 1996 (5 U.S.C. 801-808), the NRC has determined that this action is not a major rule and has verified this determination with the Office of Information and Regulatory Affairs of OMB.

XIV. Criminal Penalties.

For the purposes of Section 223 of the Atomic Energy Act of 1954, as amended (AEA), the NRC is issuing this final rule that would amend §§ 73.8, 73.22, and 73.54, and add § 73.77 under one or more of Sections 161b, 161i, or 161o of the AEA. Willful violations of the rule would be subject to criminal enforcement. Criminal penalties as they apply to regulations in 10 CFR part 73 are discussed in § 73.81(a).

XV. Compatibility of Agreement State Regulations.

Under the "Policy Statement on Adequacy and Compatibility of Agreement State Programs," approved by the Commission on June 20, 1997, and published in the *Federal Register* (62 FR 46517; September 3, 1997), this rule is classified as compatibility "NRC." Compatibility is not required for Category "NRC" regulations. The NRC program elements in this category are those that relate directly to areas of regulation reserved to the NRC by the AEA or the provisions of 10 CFR, and although an Agreement State may not adopt program elements reserved to the NRC, it may wish to inform its licensees of certain requirements via a mechanism that is consistent with a particular State's administrative procedure laws, but does not confer regulatory authority on the State.

XVI. Availability of Guidance.

The NRC is issuing implementation guidance for this rule, RG 5.83, "Cyber Security Event Notifications" (Docket ID NRC-2014-0036). The guidance is available in ADAMS under Accession No. ML14269A388. Regulatory Guide 5.83 is intended to describe a proposed method that the NRC staff considers acceptable for use in complying with the NRC's regulations on cyber security event notifications. Because the regulatory analysis for the final rule provides sufficient explanation for the rule and the implementing guidance, a separate regulatory analysis was not prepared for the regulatory guide.

XVII. Availability of Documents.

The documents identified in the following table are available to interested persons through the following methods, as indicated.

DOCUMENT	**ADAMS ACCESSION NO. / *FEDERAL REGISTER* (FR) CITATION**
SECY-10-0085 – Proposed Rule: "Enhanced Weapons, Firearms Background Checks and Security Event Notifications" (RIN: 3150-AI49) (June 27, 2010)	ML101110121
Staff Requirements – SECY-10-0085 – Proposed Rule: Enhanced Weapons, Firearms Background Checks and Security Event Notifications (RIN: 3150-AI49) (October 19, 2010)	ML102920342
Proposed Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule (February 3, 2011)	76 FR 6199
DG-5019, "Reporting and Recording Safeguards Events" (February 3, 2011)	76 FR 6085
Summary of the June 1, 2011, Public Meeting to Discuss the Proposed Enhanced Weapons, Firearms Background Checks and Security Event Notifications Rulemaking (June 24, 2011)	ML111720007

Bifurcation of the Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule (December 20, 2013)	ML13280A366
Staff Requirements – COMSECY-13-0031 – Bifurcation of the Enhanced Weapons, Firearms Background Checks, and Security Event Notification Rule (January 22, 2014)	ML14023A860
Regulatory Analysis for Final Rule on Cyber Security Event Notifications (10 CFR Part 73)	ML14170B076
Summary of the July 31, 2014, Public Meeting to Discuss the Proposed Implementation Date of the Draft Cyber Security Event Notification Final Rule (August 29, 2014)	ML14240A404
Regulatory Guide 5.83, "Cyber Security Event Notifications" (March 2015)	ML14269A388
CSEN Public Comments Associated with Final Rule	ML14226A596
Final Rule: Cyber Security Event Notification OMB Supporting Statement	ML15203A233

List of Subjects for 10 CFR Part 73

Criminal penalties, Exports, Hazardous materials transportation, Incorporation by reference, Imports, Nuclear energy, Nuclear materials, Nuclear power plants and reactors, Penalties, Reporting and recordkeeping requirements, Security measures.

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 of 1954, secs. 53, 147, 149, 161, 170D, 170E, 170H, 170I, 223, 229, 234, 1701 (42 U.S.C. 2073, 2167, 2169, 2201, 2210d, 2210e, 2210h, 2210i, 2273, 2278a, 2282, 2297f); Energy Reorganization Act of 1974, secs. 201, 202 (42 U.S.C. 5841, 5842); Nuclear Waste Policy Act of 1982, secs. 135, 141 (42 U.S.C. 10155, 10161); 44 U.S.C. 3504 note.

Section 73.37(b)(2) also issued under Sec. 301, Public Law 96-295, 94 Stat. 789 (42 U.S.C. 5841 note).

2. In § 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, 73.24, 73.25, 73.26, 73.27, 73.37, 73.38, 73.40, 73.45, 73.46, 73.50, 73.54, 73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 73.70, 73.71, 73.72, 73.73, 73.74, 73.77 and appendices B, C, and G to this part.

(c) * * *

(1) In §§ 73.71 and 73.77, NRC Form 366 is approved under control number 3150-0104.

* * * * *

3. In § 73.22, add a sentence to the end of 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 § 73.77 are considered to be extraordinary conditions.

* * * * *

4. In § 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 § 73.77.

* * * * *

5. Add § 73.77 to read as follows:

§ 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.

Dated at Rockville, Maryland, this 23rd day of October, 2015.

For the Nuclear Regulatory Commission.

/RA/

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