# RULEMAKING ISSUE
# (Affirmation)

November 20, 2014 SECY-14-0129

FOR: The Commissioners

FROM: Mark A. Satorius
Executive Director for Operations

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

PURPOSE:

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

DISCUSSION:

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

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

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

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

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

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

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

Significant Changes from the Proposed Rule to the Final Rule

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

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

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

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

Cumulative Effects of Regulation

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

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

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

Public Input to the Proposed Rule

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

Guidance Documents

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

- Regulatory Guide 5.83, "Cyber Security Event Notifications"

COMMITMENT:

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

RESOURCES:

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

RECOMMENDATIONS:

The staff recommends that the Commission take the following actions:

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

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

(3) Note the following:

- The staff has prepared a final regulatory analysis (Section VII of Enclosure 2).
- The staff has determined that this action is not a “major rule” as defined in the Congressional Review Act of 1996 (5 U.S.C. 804(2)) and has confirmed this determination with OMB. The staff will inform the appropriate Congressional and Government Accountability Office contacts.
- The staff has performed a final environmental assessment and reached a finding of no significant impact (Section VII of Enclosure 2).
- This final rule creates new information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). The staff will submit this rule to OMB for review and approval of the information collection requirements (Section XII of Enclosure 2).
- The staff will inform the appropriate Congressional committees.
- The Office of Public Affairs will issue a press release.

COORDINATION:

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

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

***/RA Michael R. Johnson for/***

Mark A. Satorius
Executive Director
for Operations

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

**History of the Cyber Security Event Notification Rulemaking Activities**

Section 161A of the Atomic Energy Act of 1954, as amended, confers on the Commission the authority to permit a licensee's or certificate holder's security personnel to possess and use weapons, devices, ammunition, or other firearms, notwithstanding local, State, and certain Federal firearms laws that may prohibit such possession and use. Section 161A.d requires the Commission to develop guidelines for the implementation of this authority (Firearms Guidelines) subject to the approval of the U.S. Attorney General.

On October 26, 2006, the U.S. Nuclear Regulatory Commission (NRC) published a proposed rule (71 FR 62664) to implement the Firearms Guidelines as part of the larger proposed power reactor security rule. In SECY-08-0050, "Firearms Guidelines Implementing Section 161A of the Atomic Energy Act of 1954 and Associated Policy Issues", dated April 17, 2008 (Agencywide Document Access and Management System (ADAMS) Accession No. ML072920440), the staff recommended that the power reactor security rule be bifurcated into two separate rules; one to address implementation of the Firearms Guidelines and physical security event notification requirements (e.g. enhanced weapons rule), and the other to address the remaining provisions of the October 2006 proposed rule. The staff stated that delays in finalizing the Firearms Guidelines and the time needed to publish a revised proposed rule, resolve any public comments, and then publish the final power reactor security rule could not accommodate the schedule at that time. The rule was bifurcated, and on March 27, 2009, the final power reactor security requirements were published in the *Federal Register* (74 FR 13926) without the Firearms Guidelines related requirements.

On October 19, 2010, in Staff Requirements Memorandum (SRM) SRM-SECY-10-0085, "Proposed Rule: Enhanced Weapons, Firearms Background Checks and Security Event Notifications" (ADAMS Accession No. ML102920342), the Commission directed the staff to publish a proposed enhanced weapons rule implementing the Firearms Guidelines, revise the physical security event notification requirements, and add new cyber security event notification requirements. The proposed enhanced weapons rule was published in the *Federal Register* (76 FR 6200) for public comment on February 3, 2011.

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 staff described discussions with the U.S. Department of Justice (DOJ) staff to revise the Firearms Guidelines so that only the security personnel for licensees and certificate holders that actually apply for Section 161A preemption authority would be subject to the firearms background check requirement. In SRM-SECY-12-0125 (ADAMS Accession No. ML12326A653), the Commission directed staff to revise the Firearms Guidelines accordingly and to publish a supplemental proposed enhanced weapons rule for public comment. The NRC staff reached agreement with DOJ staff on the proposed revisions to the Firearms Guidelines and the U.S. Attorney General approved the revised Firearms Guidelines on March 21, 2014 (ADAMS Accession No. ML14086A096).

On April 18, 2014, the staff sent to the Commission the revised Firearms Guidelines in SECY-14-0048, "Approval of Revised Firearms Guidelines" (ADAMS Accession No. ML14108A407). In SRM-SECY-14-0048 (ADAMS Accession No. ML14148A040) the Commission approved and authorized the publication of the revised Firearms Guidelines in the *Federal Register*. By November 2014, the staff will be sending to the Commission for review a supplemental proposed enhanced weapons rule for public comment that reflects the changes to the Firearms Guidelines.

The cyber security event notification requirements in the proposed enhanced weapons rule are independent of the revisions to Firearms Guidelines described above. The revision of the Firearms Guidelines and the publishing of a supplemental proposed enhanced weapons rule created an inherent schedule uncertainty and delayed the final publication of the important cyber security event notification requirements. Accordingly, the staff requested Commission approval in COMSECY-13-0031 “Bifurcation of the Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Rule” (ADAMS Accession No. ML13280A366) to bifurcate the enhanced weapons rule into two separate rulemakings; one rule would include the cyber security event notification requirements and the second rule would include the remaining requirements in the proposed enhanced weapons rule (i.e., the enhanced weapons requirements, firearms background check requirements, and physical security event notification requirements). In SRM-COMSECY-13-0031 "Bifurcation of the Enhanced Weapons, Firearms Background Checks, and Security Event Notification Rule" (ADAMS Accession No. ML14023A860) the Commission approved the staff’s plan to bifurcate the enhanced weapons rule to specifically separate the cyber security event notification requirements from the remaining requirements in the enhanced weapons rulemaking.

The bifurcation removed the schedule uncertainty for the cyber security event notification requirements by avoiding any future delays associated with enhanced weapons rulemaking. This allowed the staff to prepare the final cyber security event notification rulemaking package, including the associated regulatory guidance, expeditiously (i.e., approximately 9 months earlier than if it did not bifurcate the rules).

**[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 10 CFR 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: 301-287-3422; e-mail: Carol.Gallagher@nrc.gov. For technical questions, contact the individual(s) 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 in this document (if that document is available in ADAMS) is provided the first time that a document is referenced.

- **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 Document Access and Management System (ADAMS) Accession No. ML081650474), the 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 10 CFR 73.71 and appendix G to part 73, "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 10 CFR 73.71 and appendix G to 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 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 9, 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 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” (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”). 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 security posture). In addition, timely notifications assist 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 protect 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 handouts from the meeting are available (ADAMS 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 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 draft regulatory guide DG-5019 were identified and are addressed in this 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 by this final rule. The submittals containing comments specific to cyber security event notifications were consolidated (ADAMS Accession No. ML14226A596). In the proposed rule and draft guidance 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 10 CFR 73.54 with a focus on adverse impacts to SSEP functions.

### A. Public Comments on Proposed Rule

*Comment 1:* One commenter stated that neither 10 CFR 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 (CSEN) 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 CSEN 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 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 (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 CSEN 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 CSEN 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 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 10 CFR 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, 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 has been clarified to address suspected or actual cyber attacks initiated by personnel with physical or electronic access and was 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.

*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 10 CFR 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 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 (10 CFR 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. RG 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, RG 5.71, Appendix A and NEI 08-09, Appendix A. [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. 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

sabotage are not needed to provide clarity under this approach. RG 5.83 has been revised to reflect this new approach.

*Comment 9:* One commenter proposed revising the proposed rule language in appendix G I.(h)(2) to include language regarding the defense-in-depth protective strategies required by 10 CFR 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. RG 5.83 has been revised to reflect this approach.

*Comment 10:* One commenter proposed language to appendix G I.(c)(1) to report only instances of suspicious or surveillance activity or attempts to access systems, networks, or equipment that is within the scope of 10 CFR 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 appendix G I.(c)(1) appears to be misquoted. The changes proposed by the commenter would amend appendix G II.(c)(1). 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 10 CFR 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 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 with 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 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 10 CFR 73.54 regarding adverse impacts to SSEP functions.

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

*Response:* The NRC agrees that the proposed Appendix G.II(c)(2) is similar to Appendix G.I(h)(2); 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. RG 5.83 has been revised to reflect this new approach.

*Comment 16:* One commenter proposed rule language in appendix G.I(h)(2) 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. RG 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 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 10 CFR 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 10 CFR 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-33, 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 10 CFR 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. RG 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 10 CFR 73.54 and RG 5.71 and provides additional clarity on cyber security event notification criteria (i.e. adverse impact to SSEP functions). RG 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 10 CFR 73.54 (i.e., adverse impacts to SSEP functions), and in the process, 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 10 CFR 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 10 CFR 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 10 CFR 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 10 CFR 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 10 CFR 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 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 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 10 CFR 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. RG 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 appendix G, paragraph IV, section (a). [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. 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]

*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.

*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, 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. NRC form 366 will not be revised. RG 5.83 will provide the specific type of content that should be included in the abstract section of NRC 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. RG 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 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, 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. RG 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 10 CFR 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 10 CFR 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. 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. RG 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 CSEN final rulemaking now it may delay full implementation of 10 CFR 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 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 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.

**§ 73.8 Information collection requirements: OMB approval.**

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

**§ 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.

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

The NRC is amending § 73.54 to add a requirement to the end of paragraph (d), (d)(4) "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.

**§ 73.77 Cyber security event notifications.**

The NRC has moved cyber security event notifications from § 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) and previously issued security advisories (e.g., Information Assessment Team Advisory 12-02, “Situational Awareness – Importance of using the NRC Protected Web Server and continued licensee suspicious activity reporting”).

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., 10 CFR 50.72).

Section 73.77(c)(3) in the final rule was revised to remove a reference to paragraph III of appendix A in 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 NRC 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.”

## 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 Cumulative Effects of Regulation (CER) requirements promulgated by SRM-SECY-0032, "Consideration of the Cumulative Effects of Regulation in the Rulemaking Process", dated October 11, 2011 (ADAMS Accession No. ML112840466), 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. 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.

## 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.

The burden to the public for these information collections is estimated to average 19.1 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, (3150-0002 and 3150-0104), Office of Management and Budget, Washington, DC 20503.

**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 section § 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 Title 10 of the Code of Federal Regulations, 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.

In the Rules and Regulations section of this issue of the *Federal Register*, the NRC is issuing implementation guidance for this rule, RG 5.83, "Cyber Security Event Notifications" (Docket ID NRC-2014-0036). The guidance is also available in ADAMS under Accession No. ML14269A388. RG 5.83 is intended to describe a proposed method that the NRC staff considers acceptable for use in complying with the NRCs 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 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 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 |

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

**PART 73 -- PHYSICAL PROTECTION OF PLANTS AND MATERIALS**

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

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

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

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, 73.23, 73.24, 73.25, 73.26, 73.27, 73.37, 73.38, 73.40, 73.45, 73.46, 73.50, 73.51, 73.54, 73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 73.70, 73.71, 73.72, 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 new § 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 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 of this part.

(2) Notifications required by this section that contain Safeguards Information may be made to the NRC Headquarters Operations Center without using secure communications systems under the exception 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, as applicable.

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

(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 ___th day of , 2014.

For the Nuclear Regulatory Commission.

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

(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.

For the Nuclear Regulatory Commission.

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

ADAMS Accession No: ML14136A214 WITS: CMSY13-0031-1-NRR *Via E-Mail

| OFFICE | NRR/DPR/PRMB | NRR/DPR/PRMB* | NRR/DPR/PRMB* | NRR/DPR | NRR/DPR |
|---|---|---|---|---|---|
| NAME | RBeall | GLappert | TInverso | AMohseni | LKokajko |
| DATE | 07/28/14 | 09/03/14 | 07/28/14 | 07/30/2014 | 08/01/2014 |
| OFFICE | NSIR/CSD | NRO | OIS/IRSD* | ADM/DAS/RDB* | OE* |
| NAME | BWestreich | GTracy (MMayfield* for) | FMajeed | CBladey | RZimmerman (TMarenchin for) |
| DATE | 07/29/14 | 08/12/14 | 08/29/14 | 08/14/14 | 08/11/14 |
| OFFICE | CFO* | NSIR | OGC* | NRR | EDO |
| NAME | MWylie (ARossi for) | JWiggins | NStAmour (SClark for) | DDorman | MSatorius |
| DATE | 08/05/14 | 10/16/14 | 10/07/14 | 09/11/14 | / /14 |

**OFFICIAL RECORD COPY**

# Regulatory Analysis for Final Rule on Cyber Security Event Notifications (10 CFR Part 73)

**U.S. Nuclear Regulatory Commission**
Office of Nuclear Reactor Regulation
Office of Nuclear Security and Incident Response

**October 2014**

[Page intentionally left blank.]

# Table of Contents

[Page intentionally left blank.]

## 1. Introduction

This document presents a regulatory analysis of the U.S. Nuclear Regulatory Commission's (NRC's) final rule on cyber security event notifications (Agencywide Document Management System (ADAMS) Accession No. ML14136A214) and the associated Regulatory Guide 5.83, Revision 0, "Cyber Security Event Notifications" (ADAMS Accession No. ML14175A657). A discussion of backfitting of the final rule is presented in Appendix A. The recommended regulatory action establishes regulations under Title 10 of the *Code of Federal Regulations* (10 CFR) section 73.77 related to the process, timeliness, and reporting of cyber security event notifications that licensees submit to the NRC following cyber security events.

## 2. Statement of the Problem and Objective

The cyber security event notifications (CSEN) final rulemaking amends the NRC regulations to add timely notification requirements for certain cyber security events. This rulemaking increases the NRC's ability to respond to security-related plant events, evaluate ongoing suspicious activities for threat implications, and accomplish the Agency's strategic communications mission.

### 2.1. Background

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security to ensure that nuclear power plants continued to have effective security measures in place given the changing threat environment. Through a series of orders, the Commission specified a supplement to the Design Basis Threat (DBT), as well as requirements for specific training enhancements, access authorization enhancements, security officer work hours, and enhancements to defensive strategies, mitigative measures, and integrated response. Additionally, in generic communications, the Commission specified expectations for enhanced notifications to the NRC for certain security events or suspicious activities. As noted to recipients of the post-September 11, 2001 orders, the Commission's intent was to complete a thorough review of the existing physical protection program requirements and undertake a rulemaking that would codify generically-applicable security requirements.

In October 2006, the NRC issued a proposed power reactor security requirements rule to amend its security regulations and add new security requirements pertaining to nuclear power reactors (71 *Federal Register* (FR*)* 62664; October 26, 2006). The rule included: (1) security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001; (2) requirements for access to enhanced weapons and firearms background checks; and (3) new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises. One of the new security requirements in the proposed rule was the establishment of a cyber security program.

In March 2009, the NRC issued the power reactor security requirements final rule, which included adding section 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 at their facilities to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the DBT, as described in 10 CFR 73.1.

In February 2011, the NRC published a proposed enhanced weapons rule that would add new security requirements for enhanced weapons and firearms background checks, as well as revisions to existing regulations governing security event notifications (76 FR 6200; February 3, 2011). The proposed revisions to security event notification requirements included notification requirements related to imminent or actual hostile acts, physical intrusions, suspicious activities, unauthorized operation or tampering events, and cyber security events. The NRC included the CSEN requirements as part of the February 2011 proposed rule because CSEN requirements were not included in the March 2009 final power reactor security requirements rule.

Subsequently, the NRC bifurcated the February 2011 proposed enhanced weapons rule into two separate rulemakings. One rulemaking will address the CSEN requirements. The second rulemaking will address the remaining requirements, which include the enhanced weapons requirements, firearms background check requirements, and physical security event notification requirements. This regulatory analysis examines only the CSEN requirements.

## 2.2. Statement of the Problem

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, since 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. It is important for the NRC to have information about certain cyber security events to fulfill its strategic communications mission within the framework of the National Infrastructure Protection Plan (NIPP) developed by the Department of Homeland Security (DHS). The NIPP is carried out by Federal, state and local agencies and private sector entities all operating together voluntarily. The CSEN final rule removes the voluntary aspects of reporting certain cyber security events and provides regulatory stability and ensures the NRC is notified in a timely manner, including suspicious cyber security events, which plays an important role in our strategic communications mission, as well as certain cyber security events within the scope of 10 CFR 73.54 (e.g., adverse impacts to safety, security, or emergency preparedness functions).

In March 2009, the NRC published 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks,” as part of the power reactor security requirements final rule. This rule established a cyber security program under section 73.54, in which licensees provide high assurance that digital computer and communication systems, and networks are adequately protected against cyber attacks. However, the power reactor security rulemaking did not include CSEN requirements. Currently, there is no mandatory CSEN regulation or process that requires nuclear power reactor licensees to notify the NRC of any cyber attacks (successful, suspicious, or unsuccessful) in a timely manner for NRC response.

## 2.3. Objective

The objective of this final rulemaking is to amend Title 10 of the *Code of Federal Regulations* to add section 73.77, “Cyber Security Event Notifications,” to require licensees under 10 CFR parts 50 and 52 subject to the provisions of section 73.54, “Protection of Digital Computer and Communication Systems and Networks,” to report certain cyber security events to the NRC Headquarters Operations Center via the Emergency Notification System (ENS) within the timeliness requirements specified. Section 73.77 also requires these licensees to record cyber

security events in their site corrective action program. Finally, licensees are required to submit written security follow-up reports to the NRC for certain notifications made under section 73.77.

The February 2011 proposed enhanced weapons rule applied to operating power reactor sites, decommissioning power reactor sites, operating and decommissioning research and test reactor sites, hot cell sites, other reactor sites, Category I strategic special nuclear material sites, Category II and Category III special nuclear material sites, and independent spent fuel storage installations (ISFSIs). However the CSEN final rule applies only to power reactor licensees under 10 CFR Parts 50 and 52 subject to the provisions of 10 CFR 73.54. In conducting the quantitative analysis presented in this document, the NRC staff assumed that the following sites will be affected by the final rule: 58 sites with only reactors that are currently in commercial operation, two sites with both operating reactors and projected new power reactors for which a combined license (COL) already has been issued under 10 CFR Part 52, one site with both an operating reactor and a reactor under active construction under a 10 CFR Part 50 construction permit, and four sites with reactors that currently are in decommissioning. This results in 65 affected power reactor sites.

## 3. Identification and Analysis of Alternative Approaches

This section presents an analysis of the alternatives that the NRC staff considered in meeting the regulatory goals identified in Section 2. The NRC staff considered two alternatives for revising the Part 73 provisions, as discussed below.

### 3.1. Option 1: No Action

Under this option, the "no-action" alternative, the NRC would not amend the current regulations in Part 73 to add notification and reporting requirements related to certain cyber security events. Under this option, licensees would not be required to submit cyber security event notifications and reports to the NRC. Rather, the NRC would rely on the current voluntary reporting process for cyber security events by licensees. Voluntary reports can be submitted by the licensee at any time, such that the NRC may not be able to assess and evaluate issues with potential cyber security-related implications in a timely manner. This option would avoid any new costs to licensees in communicating, documenting, and reporting cyber security events. It also would avoid new costs to the NRC to review and respond to cyber security event notifications not voluntarily reported to the NRC. However, this option would not increase the NRC's ability to respond to cyber security-related plant events, evaluate ongoing suspicious activities for threat implications, or accomplish the Agency's strategic communications mission. The strategic communications mission is part of the NIPP framework and is designed to share information in an effort to protect critical infrastructure and key resources (CIKR). Under the CIKR reporting guidelines from DHS, licensees are encouraged but not required to report information concerning suspicious or criminal activity related to terrorism (e.g., physical security, cyber security, emergency preparedness).

There is specific guidance contained in the NRC's *Regulatory Analysis Technical Evaluation Handbook*[1] on how to handle voluntary initiatives, including credit to be given to voluntary actions by licensees. However, in this case, the voluntary actions (i.e., reporting suspicious

[1] NRC; *Regulatory Analysis Technical Evaluation Handbook* (NUREG/BR-0I84); Section 5.7, "Quantification of Attributes;" January 1997. Available at: http://pbadupws.nrc.gov/docs/ML0501/ML050190193.pdf, last accessed on July 29, 2014.

activity associated with cyber incidents) occur as part of the "no action" alternative. Thus, by definition, voluntary actions will occur provided that the NRC takes no action. While the final rule adds cyber security event notification requirements, under this option a regulatory baseline already exists. The NRC provides oversight of the licensee's corrective action program which includes cyber security events under the Physical Protection Program per section 73.55.

### 3.2. Option 2: Amend Regulations to Add Cyber Security Event Notification Requirements

Under this option, the NRC would conduct a rulemaking to add notification and reporting requirements related to certain cyber security events. These changes would entail adding 10 CFR 73.77, "Cyber Security Event Notifications." Specifically, the NRC would require through rulemaking that licensees conduct notifications and submit reports to the NRC in the event of certain cyber security attacks. The cyber security events fall into three categories: one-hour notifications, four-hour notifications, and eight-hour notifications. For some of these cyber security events, licensees would be required to provide a written security follow-up report to the NRC within 60 days using NRC Form 366. These cyber security events include one-hour notifications (cyber attacks that adversely impacted safety, security, or emergency preparedness (SSEP) functions (section 73.77(a)(1))) and two of the four-hour notifications (cyber attacks that could have caused an adverse impact to SSEP functions (section 73.77(a)(2)(i)) and cyber attacks initiated by personnel with physical or electronic access (section 73.77(a)(2)(ii))). Licensees also would be required to record, in their site corrective action program, vulnerabilities, weaknesses, failures and deficiencies in their cyber security program and notifications made under section 73.77(a).

The NRC staff will review the information provided by licensees to determine appropriate response actions. These actions may include one or more of the following actions: (1) notifying the NRC Cyber Assessment Team, (2) determining necessary follow-up actions based on the event characteristics, (3) documenting reported events, (4) making additional notifications to other government agencies, and (5) issuing threat advisories to other licensees. The NRC also will use the information provided by licensees to effectively monitor ongoing licensee actions and inform other licensees in a timely manner of cyber security-significant events.

## 4. Evaluation of Benefits and Costs

This section examines the benefits and costs expected to result from this rulemaking, and are presented in two subsections. Section 4.1 identifies attributes that are expected to be affected by the rulemaking. Section 4.2 describes how benefits and costs have been analyzed.

### 4.1. Identification of Affected Attributes

The following attributes are expected to be affected by this rulemaking. Their impacts are quantified where possible. Impacts to accident-related attributes are qualified because estimates of occurrences of possible attacks and their successful repulsions are unknown. Further, even if reliable estimates were available, they would be considered Safeguards Information and not to be released for public dissemination.

- Safeguards and Security Considerations — The actions regarding cyber security event notifications will increase the NRC's ability to respond to cyber security events and to effectively monitor ongoing licensee actions and inform other licensees in a timely

manner of cyber security-significant events and thus, protect public health and safety, and the common defense and security.

- Industry Implementation — In implementing the regulatory action, licensees are expected to read the final rule and regulatory guide, and develop or upgrade their existing notification procedures. Licensees also are expected to develop and deliver initial and recurring notification training to designated personnel. For purposes of this analysis, the NRC staff estimates that 65 sites will be affected by the final rule. Estimated hours of burden for each of these activities can be found in:

  - Section 4.2.4.2: Development of Procedures
  - Section 4.2.4.3: Initial Notification Training
  - Section 4.2.4.10: Recurring Notification Training

- Industry Operation — The CSEN requirements of the final rule would result in operating expenses for industry. Specifically, the final rule will require licensees to make telephonic notifications and submit written security follow-up reports to the NRC. Written security follow-up reports must be prepared on NRC Form 366, which is currently used for physical security event notifications. Licensees also will need to record, in their existing site corrective action program, notifications made under section 73.77(a) and vulnerabilities, weaknesses, failures or deficiencies in their cyber security program. In addition, licensees will need to periodically supply NRC inspectors with cyber security event information to support security inspections, as needed. Finally, licensees will need to update and deliver recurring notification training.

The analysis includes three categories of cyber security events that will impact industry operations. The estimated rates of events per year for each notification requirement are based on the following:

- Voluntary Reporting Initiatives: The NRC has been collecting data from licensees under the voluntary reporting initiative. However, reporting is on a voluntary basis and it is not known if all of the cyber security events (within the voluntary initiative) are being reported to the NRC.

- 10 CFR 73.54 Requirements: As the implementation of the cyber security rule progresses, voluntary reporting has been decreasing.

Using information from the above two actions, the NRC staff generated the best estimate annual rates for the one-, four-, and eight-hour notifications as shown below:

- One-hour notifications: A cyber attack that adversely impacted SSEP functions (i.e., cyber security events covered under section 73.77(a)(1)). The NRC staff assumes that, on average, cyber attacks with adverse impacts occur once every two years (i.e., at a rate of 0.50 event per year) at each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license; cyber attacks with adverse impacts occur once every 20 years (i.e., at a rate of 0.05 event per year) at each site that has only reactors that currently are in decommissioning. In addition, the NRC staff assumes that each event would require one hour of licensee staff time to make a telephonic notification to the NRC Headquarters Operations Center.

- Four-hour notifications: A cyber attack that could have caused an adverse impact to SSEP functions (i.e., cyber security events covered under section 73.77(a)(2)(i)), cyber attacks initiated by personnel with physical or electronic access (section 73.77(a)(2)(ii)), or notification of a local, State, or other Federal agency (section 73.77(a)(2)(iii)). The NRC staff assumes that, on average, these types of events occur once a year at each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license; cyber attacks without adverse impacts to SSEP functions occur once every 10 years (i.e., at a rate of 0.10 event per year) at each site that has only reactors that currently are in decommissioning. The NRC staff also assumes that each event would require 0.5 hour of licensee staff time to make a telephonic notification to the NRC Headquarters Operations Center.

- Eight-hour notifications: Activities that may indicate intelligence gathering or preoperational planning related to a cyber attack (i.e., cyber security events covered under section 73.77(a)(3)). The NRC staff assumes that, on average, activities that may indicate intelligence gathering or preoperational planning related to a cyber attack occur 2.5 times a year at each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license; activities that may indicate intelligence gathering or preoperational planning related to a cyber attack occur once every two years (i.e., at a rate of 0.50 event per year) at each site that has only reactors that currently are in decommissioning. In addition, the NRC staff assumes that each event would require 0.50 hour of licensee staff time to make a telephonic notification to the NRC Headquarters Operations Center.

For events requiring entry in the site corrective action program, the NRC staff assumes that, on average, each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license will record 10 entries per year in its corrective action program; each site that has only reactors that currently are in decommissioning will record 2.5 entries per year in its corrective action program. The NRC staff also assumes that each site will require 0.50 hour of licensee staff time to record one entry in the site corrective action program. This final rule specifies certain cyber security events for entry into the site corrective action program and those hours are included in the regulatory baseline as required under the Physical Protection Program per section 73.55.

The NRC staff estimates that 65 sites will be affected by the final rule and will be required to conduct all of the above activities.

- NRC Implementation — The NRC implementation costs include the labor cost for the development of the final rule and the associated regulatory guidance.

- NRC Operation — The NRC activities under the final rule include the review of information received during a cyber security event notification for follow-up, activation of the NRC's Headquarters Operations Center, or immediate communication to DHS and other licensees, as needed. The NRC staff also will review written security follow-up reports received after initial telephonic notifications. In addition, the NRC staff may review information on cyber security events recorded in the site corrective action program during an inspection.

- Regulatory Efficiency — The regulatory action is expected to result in enhanced regulatory efficiency involving the NRC's ability to monitor ongoing cyber security events at a range of licensed facilities, and the ability to rapidly communicate information on cyber security events at such facilities to other NRC-regulated facilities and other government agencies, as necessary.

- Public Health (Accident) — The regulatory action is expected to reduce the risk that public health will be affected by radiological releases because of the increased likelihood of a successful repulsion of an attack.

- Occupational Health (Accident) — The regulatory action is expected to reduce the risk that occupational health will be affected by radiological releases because of the increased likelihood of a successful repulsion of an attack.

- Off-Site Property — The regulatory action is expected to reduce the risk that off-site property will be affected by radiological releases because of the increased likelihood of a successful repulsion of an attack.

- On-Site Property — The regulatory action is expected to reduce the risk that on-site property will be affected by radiological releases because of the increased likelihood of a successful repulsion of an attack.

- Other Government Agencies — The CSEN final rule will not have an effect on other Government agencies because the reporting of suspicious or criminal activity related to terrorism (e.g., physical security, cyber security) is captured under the NIPP and part of the NRC's strategic communications mission. In addition, certain cyber security events reported to the NRC that fall within the scope of 10 CFR 73.54 will not need to be reported to other Government agencies.

Attributes that are not expected to be affected by this rulemaking include the following: occupational health (routine); public health (routine); environmental considerations; general public; improvements in knowledge; and antitrust considerations.

## 4.2. Analytical Methodology

This section describes the process used to evaluate benefits and costs associated with the final rule. The benefits of the final rule include any desirable changes in affected attributes (e.g., monetary savings, improved safety, improved security) while the costs include any undesirable changes in affected attributes (e.g., monetary costs, increased exposures).

Of the 11 affected attributes, the analysis evaluates four—industry implementation, industry operation, NRC implementation, and NRC operation—on a quantitative basis. Quantitative analysis requires a baseline characterization of the affected universe, including characterization of factors such as the number of affected entities and the types of procedures that licensees would implement as a result of the final rule. Sections 4.2.1 through 4.2.4 describe the most significant analytical data and assumptions used in the quantitative analysis of these attributes.

The analysis primarily relies on a qualitative (rather than quantitative) evaluation of the remaining seven affected attributes (safeguards and security considerations, regulatory efficiency, public health (accident), occupational health (accident), off-site property, on-site

property, and other government agencies) because of the uncertainties associated with monetizing the impact that the cyber security event notifications under the final rule would have on these affected attributes. Monetizing the impact on any of these attributes would require estimation of factors such as the frequency with which radiological sabotage attempts are (i.e., pre-rule) and will be (i.e., post-rule) successful, and the impacts associated with successful radiological sabotage attempts. Because these factors preclude monetization of these seven affected attributes, this analysis discusses them qualitatively in Section 4.1.

### 4.2.1. Baseline for Analysis

This regulatory analysis measures the incremental costs of the final rule relative to a "baseline" that reflects anticipated behavior in the event the NRC undertakes no regulatory action (Option 1, the "no-action" alternative). As part of the baseline used in this analysis, the NRC staff assumes full licensee compliance with existing NRC regulations, which includes the NRC's oversight of the licensee's corrective action program to include cyber security events as part of the physical protection program per section 73.55. Section 5 presents the estimated incremental costs of the final rule relative to this baseline.

### 4.2.2. Affected Universe

The NRC staff estimates that 65 U.S. commercial nuclear power reactor sites will be affected by the final rule.[2] This estimate includes sites with:

- Operating power reactors (one, two, or three units);
- Projected new power reactors for which a combined license (COL) already has been issued under Part 52;
- Power reactors under active construction under a Part 50 license (i.e., Watts Bar Nuclear Plant Unit 2 );[3] and
- Decommissioning reactors.

The analysis evaluates the incremental costs of the final rule on a site (65) basis rather than on a per unit (116) basis. For each type of site included in the analysis, Table 4-1 presents the number of sites and the average number of years that sites are expected to be subject to the final rule requirements (i.e., final rule applicability period).

The final rule applicability period was derived as follows:

- Sites with only reactors that are currently in commercial operation - The final rule applicability period for this type of site is estimated to be 34 years. This estimate is based on the sum of the average remaining operating life across all sites and then adding a 15-year decommissioning period. For each site, the staff identified the operating reactor unit with the latest license expiration date.[4] The staff then used that

[2] The Bellefonte Nuclear Power Station is not included in this analysis because the site will not be affected by the final rule. The site does not have any operating units, has no fuel on site, and new construction is indefinitely delayed. Bellefonte Units 1 and 2 are under the Commission Policy Statement on Deferred Plants (52 *FR* 38077; October 14, 1987).

[3] Watts Bar Nuclear Plant Unit 2 is currently under active construction.

[4] Based on information obtained from NRC, 2013-2014 Information Digest (NUREG-1350, Volume 25), "Appendix H: U.S. Commercial Nuclear Power Reactor Operating Licenses - Expiration by Year, 2013–2049," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014.

license expiration date to calculate the remaining operating life for the site. For example, for a site where the last unit license expiration date will occur in 2017, the staff calculated the remaining operating life to be 2 years (i.e., 2017 – 2015). The staff assumed that all operating licenses go to term with the exception of: (1) early terminations already announced (i.e., Vermont Yankee plans to terminate commercial operation in December 2014 and Oyster Creek plans to terminate commercial operation in 2019) and (2) license renewal applications already under consideration (i.e., Indian Point Nuclear Generating) for which the staff assume that the license renewal is granted. After the staff calculated the remaining operating life for each site, the staff then calculated the average remaining operating life across all sites. Finally, the staff added a 15-year decommissioning period. (Refer to "sites with only reactors that currently are in decommissioning" for information on the derivation of the 15-year decommissioning period).

- Sites with both operating reactors and projected new reactors under a Part 52 license - The final rule applicability period for this type of site is estimated to be 59 years. This estimate is based on the sum of the average estimated remaining operating life across all sites and then adding a 15-decommissioning period. For each site, the staff identified the reactor unit with the latest license expiration date.[5, 6, 7] The staff then used that license expiration date to calculate the remaining operating life for the site. The staff assumed that all licenses go to term. After the staff calculated the remaining operating life for each site, the staff then calculated the average remaining operating life across all sites. Finally, the staff added a 15-year decommissioning period. (Refer to "sites with only reactors that currently are in decommissioning" for information on the derivation of the 15-year decommissioning period).

- Sites with both operating reactors and reactors under active construction under a Part 50 license – The final rule applicability period for this type of site is estimated to be 55 years. This estimate is based on the remaining operating life of the only site with reactors under active construction under a Part 50 license (i.e., the Watts Bar Nuclear Plant) and then adding a 15-year decommissioning period. (Refer to "sites with only reactors that currently are in decommissioning" for information on the derivation of the 15-year decommissioning period).

[5] Based on information obtained from NRC, 2013-2014 Information Digest (NUREG-1350, Volume 25), "Appendix H: U.S. Commercial Nuclear Power Reactor Operating Licenses - Expiration by Year, 2013–2049," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014.

[6] Based on information obtained from NRC, 2013-2014 Information Digest (NUREG-1350, Volume 25), "Appendix A: U.S. Commercial Nuclear Power Reactors - Operating Reactors under Active Construction or Deferred Policy," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014

[7] For a Part 52 license, the 40-year term of the license does not begin until after the 10 CFR 52.103(g) finding, which occurs after construction is completed. Summer Units 2 and 3 are expected to begin commercial operation in 2016 and 2019, respectively. Vogtle Units 3 and 4 are expected to begin commercial operation in 2017 and 2018, respectively.

- Sites with only reactors that currently are in decommissioning – The final rule applicability period for this type of site is estimated to be 15 years. This estimate is based on information on time periods contained in Irradiated Fuel Transfer Plans submitted, pursuant to 10 CFR 50.54(bb), by licensees that have prematurely shutdown their reactor units.[8]

In estimating the costs to sites, the NRC staff classified sites with more than one type of reactor under the site category with the longest final rule applicability period. For example, a site with one operating reactor and one decommissioning reactor is categorized as a "site with only reactors that are currently in commercial operation" because the final rule applicability period for an operating reactor exceeds the period for a reactor that already is decommissioning.

Appendix B to this analysis presents additional information on the sites affected by the final rule, including information on the categorization of the individual sites.

[8] Kewaunee permanently ceased commercial operation on May 7, 2013. The licensee expects to have all of Kewaunee's spent fuel transferred from the spent fuel pool to the ISFSI by the end of year 2016 (e.g., transfer within 4 years of ceasing commercial operation). Crystal River Unit 3 permanently ceased commercial operation on February 20, 2013, which is when the licensee transferred fuel from the reactor vessel to the spent fuel pool. The licensee expects to have all of Crystal River Unit 3's spent fuel transferred from the spent fuel pool to the ISFSI by the end of year 2019 (e.g., transfer within 6 years of ceasing commercial operation). Based on these representative plans, it is reasonable to estimate that licensees will transfer all spent fuel to ISFSI (e.g., dry cask storage) within 15 years of ceasing commercial operation.

## Table 4-1. U.S. Commercial Nuclear Power Reactor Sites Affected by the Final Rule [a]

| Type of Site | Number of Sites | Final Rule Applicability Period (years) |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | 58 | 34 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | 2 | 59 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | 1 | 55 |
| Sites with only reactors that currently are in decommissioning | 4 | 15 |
| **Total** | **65** | **Not applicable** |

[a] Sites with more than one type of reactor were included under the site category with the longest final rule applicability period. Refer to Appendix B for information on the categorization of the individual sites.

**Sources:**

(1) NRC, "Operating Nuclear Power Reactors (by Location or Name)" Web page, www.nrc.gov. Data current as of March 19, 2014. Available at: http://www.nrc.gov/info-finder/reactor/, last accessed on July 7, 2014.
(2) NRC, 2013-2014 Information Digest (NUREG-1350, Volume 25), "Appendix H: U.S. Commercial Nuclear Power Reactor Operating Licenses - Expiration by Year, 2013–2049," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014.
(3) NRC, "Combined License Applications for New Reactors" Web page, www.nrc.gov. Data current as of July 1, 2014. Available at: http://www.nrc.gov/reactors/new-reactors/col.html, last accessed on July 7, 2014.
(4) NRC, 2013-2014 Information Digest (NUREG-1350, Volume 25), "Appendix A: U.S. Commercial Nuclear Power Reactors - Operating Reactors under Active Construction or Deferred Policy," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014.
(5) NRC, "Locations of Power Reactor Sites Undergoing Decommissioning" Web page, www.nrc.gov. Data current as of April 24, 2014. Available at: http://www.nrc.gov/info-finder/decommissioning/power-reactor/, last accessed on July 7, 2014.

### 4.2.3. Labor Rates

In estimating the incremental costs of the final rule, the analysis uses two hourly labor rates that include salary, fringe benefits (e.g., paid leave and health benefits), and indirect costs:

- The average labor rate for licensee staff is estimated to be $125 per hour.[9]
- The average labor rate for NRC staff is estimated to be $121 per hour.[10]

Both average labor rates are in 2014 dollars.

### 4.2.4. Assumptions

This subsection discusses the analysis of the costs associated with the implementation of the final rule. The analysis employs the following assumptions and considerations:

- All licensees are assumed to be in full compliance with the existing baseline requirements. The costs to comply with the baseline requirements are not expected to change with the final rule. Therefore, this analysis only presents the incremental costs associated with the final rule changes.
- All costs presented in this subsection are in 2014 dollars.
- Implementation costs are assumed to be incurred in 2015.
- Licensees will incur costs over the final rule applicability period, as presented in Table 4-1. The actual time period that each site will be operated will depend on the term of the operating license, and on whether the licensee chooses to operate the site for the duration of the licensed period.
- The costs incurred in each year of the analysis are discounted to the present using a 7 percent and 3 percent discount rate, in accordance with NUREG/BR-0058, Rev. 4, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission." (See Section 5 for these results).
- For purposes of this analysis, the costs under the final rule were categorized as follows:
    - One-time costs:
        - Rulemaking activities;
        - Development of procedures; and
        - Initial notification training.

[9] Based on data developed by the Bureau of Labor Statistics for "Power Plant Operators, Distributors, and Dispatchers" (Standard Occupational Code 51-8010) and for "Nuclear Power Reactor Operators" (Standard Occupational Code 51-8011), hourly labor rates for industry range from about $89 to $98. As a conservative assumption, this analysis uses an hourly labor rate of $125.

[10] NRC, Rulemaker@nrc.gov, "NRC Labor Rates for Use in Regulatory Analyses (as of October 2013)," January 2, 2014.

- Annual costs:
  - One-hour notifications;
  - Four-hour notifications;
  - Eight-hour notifications;
  - Twenty-four-hour recordable events;
  - Written security follow-up reports;
  - Inspections; and
  - Recurring notification training.

The remainder of this subsection describes the derivation of the estimated per site costs for each of the cost categories.

#### 4.2.4.1. Rulemaking Activities

In implementing the regulatory action, the NRC will perform rulemaking activities that include development and publication of the final rule and regulatory guidance. To estimate the costs associated with NRC's rulemaking activities, the analysis employs the following assumptions:

- 1 person-year of NRC staff time (i.e., 1,375 hours) will be required for performing the final rulemaking activities.[11]

- The NRC published a proposed enhanced weapons rule in 2011 that contained new security requirements for enhanced weapons and firearms background checks along with proposed cyber security event notification requirements. The proposed cyber security event notification requirements were a part of the much larger proposed enhanced weapons and firearms background checks proposed rule. The NRC is unable to determine the costs of the proposed cyber security event notification requirements separate from the enhanced weapons activities. As such, only the hours for the final cyber security event notification rulemaking activities are being reported in this analysis.

Based on the above, the NRC's one-time cost for rulemaking activities is estimated to be $166,375 (i.e., 1,375 hours x $121/hour).

#### 4.2.4.2. Development of Procedures

In implementing the regulatory action, licensees are expected to read the final rule and develop/revise procedures (e.g., site security plan). To estimate the costs associated with the development of procedures, the analysis employs the following assumptions:

- On average, each site will require 88 hours of licensee staff time to read the final rule and regulatory guide (RG), and develop 2 procedures for plant staff and security staff. The following are the estimated hours to perform each task:

  - 1 person – review final rule/RG = 8 hours
  - 1 person – modify/create procedures = 40 hours
  - 1 person – review procedures = 24 hours

[11] Number of productive hours in one person-year obtained from NRC, Rulemaker@nrc.gov, "NRC Labor Rates for Use in Regulatory Analyses (as of October 2013)," January 2, 2014.

- Approval process (Site Management and Plant Operating Review Committee (PORC)):
  - Procedures Review – 2 hours * 6 people = 12 hours
  - PORC Meeting – ¼ hour * 6 people = 1.5 hours
- 1 person – Enter procedures into plant document control system = 2 hours
- *Total is 87.5 hours, rounded up to 88 hours*

Table 4-2 shows the estimated one-time cost per site for development of procedures, by type of site.

**Table 4-2. Estimated One-Time Cost per Site for Development of Procedures (2014 Dollars)**

| Type of Site | One-Time Cost to Industry [a, b] | One-Time Cost to the NRC |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $11,000 | Not applicable |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $11,000 | Not applicable |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $11,000 | Not applicable |
| Sites with only reactors that currently are in decommissioning | $11,000 | Not applicable |

[a] One-Time Cost to Industry = [88 hours] x [$125/hour].

[b] Costs in the table are rounded to the nearest whole number.

#### 4.2.4.3. Initial Notification Training

In implementing the regulatory action, licensees are expected to revise their notification training and deliver the revised training to designated personnel. To estimate the costs associated with the initial notification training, the analysis employs the following assumptions:

Operating Reactors

- On average, each operating reactor site will require 286 hours of licensee staff time to develop, approve, and deliver the initial notification training to 800 licensee staff members. This time includes 36 hours to develop the training and 250 hours to deliver the training. The following are the estimated hours to perform each task:

  - Read Final Rule/Regulatory Guide
    - 1 person from Licensing department = 8 hours
    - 1 person from Cyber Security Assessment Team (CSAT) = 8 hours
    - 1 person from Training department = 8 hours
  - *Sub-total 24 hours*

  - Training Material Development
    - 1 person to develop training materials/lesson plans = 8 hours
    - 1 person to review training materials/lesson plans = 4 hours
  - *Sub-total 12 hours*

- *Total Training Development Time = 36 hours*

- Initial Training of Plant Staff on CSEN Rule
  - Operations/Engineering/Administrative staff: 600 people * 0.25 hour = 150 hours
  - Security and CSAT staff: 200 people * 0.50 hours = 100 hours
- *Total Initial Training Time = 250 hours*

*Grand Total: 36 hours + 250 hours = 286 hours*

Decommissioning Reactors

- On average, each decommissioning site will require 136 hours of licensee staff time to develop, approve, and deliver the initial notification training to 300 licensee staff members. This time includes 36 hours to develop the training and 100 hours to deliver the training. The following are the estimated hours to perform each task:

  - Read Final Rule/Regulatory Guide
    - 1 person from Licensing department = 8 hours
    - 1 person from Cyber Security Assessment Team (CSAT) = 8 hours
    - 1 person from Training department = 8 hours
  - *Sub-total 24 hours*

  - Training Material Development
    - 1 person to develop training materials/lesson plans = 8 hours
    - 1 person to review training materials/lesson plans = 4 hours
  - *Sub-total 12 hours*

  - *Total Training Development Time = 36 hours*

  - Initial Training of Plant Staff on CSEN Rule
    - Operations/Engineering/Administrative staff: 200 people * 0.25 hours = 50 hours
    - Security and CSAT staff: 100 people * 0.50 hours = 50 hours
  - *Total Training Development Time = 100 hours*

  *Grand Total: 36 hours + 100 hours = 136 hours*

Table 4-3 shows the estimated one-time cost per site for initial notification training, by type of site.

**Table 4-3. Estimated One-Time Cost per Site for Initial Notification Training (2014 Dollars)**

| Type of Site | One-Time Cost to Industry [a, b] | One-Time Cost to the NRC |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $35,750 | Not applicable |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $35,750 | Not applicable |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $35,750 | Not applicable |
| Sites with only reactors that currently are in decommissioning | $17,000[c] | Not applicable |

[a] One-Time Cost to Industry = [286 hours] x [$125/hour].

[b] Costs in the table are rounded to the nearest whole number.

[c] One-Time Cost to Industry = [136 hours] x [$125/hour].

#### 4.2.4.4. One-Hour Notifications

Licensees subject to the provisions of 10 CFR 73.54 must make a telephonic notification of the cyber security events identified at 10 CFR 73.77(a)(1) to the NRC within one hour after discovery. Notifications must be made according to 10 CFR 73.77(c).

To estimate the costs associated with one-hour notifications, the analysis employs the following assumptions:

- On average, cyber security events occur once every two years (i.e., at a rate of 0.50 event per year) at each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license; cyber security events occur once every 20 years (i.e., at a rate of 0.05 event per year) at each site that has only reactors that currently are in decommissioning. This rate of occurrence is based on data collected by the NRC since inception of the voluntary reporting initiatives and 10 CFR 73.54.

- On average, each site will require 1 hour of licensee staff time to make a telephonic notification.

  On average, the NRC will require 5 hours of NRC staff time to review the information provided by licensees and respond to a cyber security event telephonic notification. The estimated hours are based on the NRC staff actions when a notification is received from the voluntary reporting initiatives. Response actions may include one or more of the following actions: (1) notifying the Cyber Assessment Team; (2) activation of the NRC's Headquarters Operations Center; (3) determining necessary follow-up actions based on the event characteristics; (4) documenting reported events; (5) making additional notifications to other government agencies (e.g., DHS); and (6) issuing threat advisories to other licensees.

Table 4-4 shows the estimated annual cost per site for one-hour notifications, by type of site.

**Table 4-4. Estimated Annual Cost per Site for One-Hour Notifications (2014 Dollars)**

| Type of Site | Annual Cost to Industry [a, c] | Annual Cost to the NRC [b, c] |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $63 | $303 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $63 | $303 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $63 | $303 |
| Sites with only reactors that currently are in decommissioning | $6 | $30 |

[a] Annual Cost to Industry = [Annual number of cyber security events per site] x [1 hour/event] x [$125/hour]. The "annual number of cyber security events per site" is 0.50 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.05 for sites that have only reactors that currently are in decommissioning.

[b] Annual Cost to the NRC = [Annual number of cyber security events per site] x [5 hours/event] x [$121/hour]. The "annual number of cyber security events per site" is 0.50 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.05 for sites that have only reactors that currently are in decommissioning.

[c] Costs in the table are rounded to the nearest whole number.

#### 4.2.4.5. Four-Hour Notifications

Licensees subject to the provisions of 10 CFR 73.54 must make a telephonic notification of the cyber security events identified at 10 CFR 73.77(a)(2)(i)-(iii) to the NRC within four hours after discovery. Notifications must be made according to 10 CFR 73.77(c).

To estimate the costs associated with four-hour notifications, the analysis employs the following assumptions:

- On average, cyber security events occur once a year at each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license; cyber security events occur once every 10 years (i.e., at a rate of 0.10 event per year) at each site that has only reactors that currently are in decommissioning. This rate of occurrence is based on data collected by the NRC since inception of the voluntary reporting initiatives and 10 CFR 73.54.

- On average, each site will require 0.50 hour of licensee staff time to make a telephonic notification.

- On average, the NRC will require 5 hours of NRC staff time to respond to a cyber security event telephonic notification, including notifying the Cyber Assessment Team and determining necessary follow-up actions. The estimated hours are based on the NRC staff actions when a notification is received from the voluntary reporting initiatives.

Table 4-5 shows the estimated annual cost per site for four-hour notifications, by type of site.

**Table 4-5. Estimated Annual Cost per Site for Four-Hour Notifications (2014 Dollars)**

| Type of Site | Annual Cost to Industry [a, c] | Annual Cost to the NRC [b, c] |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $63 | $605 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $63 | $605 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $63 | $605 |
| Sites with only reactors that currently are in decommissioning | $6 | $61 |

[a] Annual Cost to Industry = [Annual number of cyber security events per site] x [0.5 hour/event] x [$125/hour]. The "annual number of cyber security events per site" is 1 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.10 for sites that have only reactors that currently are in decommissioning.

[b] Annual Cost to the NRC = [Annual number of cyber security events per site] x [5 hours/event] x [$121/hour]. The "annual number of cyber security events per site" is 1 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.10 for sites that have only reactors that currently are in decommissioning.

[c] Costs in the table are rounded to the nearest whole number.

#### 4.2.4.6. Eight-Hour Notifications

Licensees subject to the provisions of 10 CFR 73.54 must make a telephonic notification of the cyber security events identified at 10 CFR 73.77(a)(3) to the NRC within eight hours after discovery. Notifications must be made according to 10 CFR 73.77(c).

To estimate the costs associated with eight-hour notifications, the analysis employs the following assumptions:

- On average, cyber security events occur 2.5 times a year at each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license; cyber security events occur once every two years (i.e., at a rate of 0.50 event per year) at each site that has only reactors that currently are in decommissioning. This rate of occurrence is based on data collected by the NRC since inception of the voluntary reporting initiatives and 10 CFR 73.54.

- On average, each site will require 0.50 hour of licensee staff time to make a telephonic notification.

- On average, the NRC will require 5 hours of NRC staff time to respond to a cyber security event telephonic notification, including notifying the Cyber Assessment Team and determining necessary follow-up actions. The estimated hours are based on the NRC staff actions when a notification is received from the voluntary reporting initiatives.

Table 4-6 shows the estimated annual cost per site for eight-hour notifications, by type of site.

**Table 4-6. Estimated Annual Cost per Site for Eight-Hour Notifications (2014 Dollars)**

| Type of Site | Annual Cost to Industry [a, c] | Annual Cost to the NRC [b, c] |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $156 | $1,513 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $156 | $1,513 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $156 | $1,513 |
| Sites with only reactors that currently are in decommissioning | $31 | $303 |

[a] Annual Cost to Industry = [Annual number of cyber security events per site] x [0.5 hour/event] x [$125/hour]. The "annual number of cyber security events per site" is 2.5 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.50 for sites that have only reactors that currently are in decommissioning.

[b] Annual Cost to the NRC = [Annual number of cyber security events per site] x [5 hours/event] x [$121/hour]. The "annual number of cyber security events per site" is 2.5 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.50 for sites that have only reactors that currently are in decommissioning.

[c] Costs in the table are rounded to the nearest whole number.

#### 4.2.4.7. Twenty-Four-Hour Recordable Events

Under 10 CFR 73.77(b), licensees must use the site corrective action program to record vulnerabilities, weaknesses, failures and deficiencies in their 10 CFR 73.54 cyber security program. Licensees also must use the site corrective action program to record notifications made under section 73.77(a).

To estimate the costs associated with twenty-four-hour recordable events, the analysis employs the following assumptions:

- On average, each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license will record 10 entries per year in its corrective action program (i.e., 4 entries on notifications made under section 73.77(a) and 6 entries on vulnerabilities, weaknesses, deficiencies and failures within the cyber security program that do not fall into the cyber security events under section 73.77(a)). For each site that has only reactors that currently in decommissioning will record 2.5 entries per year in its corrective action program (i.e., 0.65 entries for notifications made under section 73.77(a) and 1.85 entries on vulnerabilities, weaknesses, deficiencies and failures within the cyber security program that do not fall into the cyber security events under section 73.77(a)). This rate of occurrence is based on data collected by the NRC since inception of the voluntary reporting initiatives and 10 CFR 73.54.

- On average, each site will require 0.50 hour of licensee staff time to record one entry in the site corrective action program. The time required to perform corrective actions, trends, etc., are not part of this regulation. Those hours are included in the regulatory baseline as required under the physical protection program per section 73.55.

Table 4-7 shows the estimated annual cost per site for twenty-four-hour recordable events, by type of site.

**Table 4-7. Estimated Annual Cost per Site for Twenty-Four-Hour Recordable Events (2014 Dollars)**

| Type of Site | Annual Cost to Industry [a, b] | Annual Cost to the NRC |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $625 | Not applicable |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $625 | Not applicable |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $625 | Not applicable |
| Sites with only reactors that currently are in decommissioning | $156 | Not applicable |

[a] Annual Cost to Industry = [Annual number of recordable events per site] x [0.5 hour/event] x [$125/hour]. The "annual number of recordable events per site" is 10 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 2.5 for sites that have only reactors that currently are in decommissioning.

[b] Costs in the table are rounded to the nearest whole number.

#### 4.2.4.8. Written Security Follow-Up Reports

Under 10 CFR 73.77(d), licensees making an initial telephonic notification of cyber security events to the NRC according to the provisions of 10 CFR 73.77(a)(1), (a)(2)(i) and (a)(2)(ii) also must submit a written security follow-up report to the NRC within 60 days of the telephonic notification. However, licensees are not required to submit a written security follow-up report following a telephonic notification made under 10 CFR 73.77(a)(2)(iii) (i.e., notification to a local, State, or other Federal agency) and 10 CFR 73.77(a)(3) (i.e., notification regarding activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack).

To estimate the costs associated with written security follow-up reports, the analysis employs the following assumptions:

- On average, each site that has reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license will submit 1.5 written security follow-up reports to the NRC every year; each site that has only reactors that currently are in decommissioning will submit 1 written security follow-up report to the NRC approximately every 6.67 years (i.e., at a rate of 0.15 reports per year). This rate of occurrence is based on the estimated rates of events per year for the one and four hour notifications.

- On average, each site will require 80 hours[12] of licensee staff time to prepare and submit a written security follow-up report. The estimated time to complete the NRC Form 366 to

[12] Includes recordkeeping (16 hrs), and time to prepare, review, approve, and submit the follow-up report (64 hrs).

report a cyber security event is similar to other reportable events already used by this form. No additional information is being collected beyond what is already required by the use of the form. The most recent information collection review included contacting nine licensees to refine the burden estimate. The data collected determined that the estimate of 80 hours of burden (including 16 hours of recordkeeping) is still valid.

- On average, the NRC will require 1 hour of NRC staff time to review a written security follow-up report. Information in these reports will be used by the NRC to get a clearer understanding of the event, and to assess trends and patterns.

Table 4-8 shows the estimated annual cost per site for written security follow-up reports, by type of site.

**Table 4-8. Estimated Annual Cost per Site for Written Security Follow-Up Reports (2014 Dollars)**

| Type of Site | Annual Cost to Industry [a, c] | Annual Cost to the NRC [b, c] |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $15,000 | $182 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $15,000 | $182 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $15,000 | $182 |
| Sites with only reactors that currently are in decommissioning | $1,500 | $18 |

[a] Annual Cost to Industry = [Annual number of reports per site] x [80 hours/report] x [$125/hour]. The "annual number of reports per site" is 1.5 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.15 for sites that have only reactors that currently are in decommissioning.

[b] Annual Cost to the NRC = [Annual number of reports per site] x [1 hour/report] x [$121/hour]. The "annual number of reports per site" is 1.5 for sites that have reactors that are currently in commercial operation, projected new reactors under a Part 52 license, and/or reactors under active construction under a Part 50 license and 0.15 for sites that have only reactors that currently are in decommissioning.

[c] Costs in the table are rounded to the nearest whole number.

#### 4.2.4.9. Inspections

Licensees must provide information on cyber security events recorded in the site corrective action program during an inspection. On average, each site will be inspected by the NRC once every two years (i.e., at a rate of 0.50 inspection per year). Inspectors are assumed to perform their own queries of the site CAP to assist with their inspection activities. Also, time spent on inspecting a site's cyber security event notification requirements will be part of a larger security inspection of the licensee so any costs will be offset by equivalent efforts in other areas. Thus, although the inspection will occur, there will be no incremental cost to industry or the NRC.

#### 4.2.4.10. Recurring Notification Training

Licensees are expected to deliver their notification training to designated personnel. To estimate the costs associated with the recurring notification training, the analysis employs the following assumptions:

- On average, each site will deliver the recurring notification training that includes the cyber security event notification requirements once a year as part of their annual training program.

Operating Reactors

- On average, each site will require 84 hours of licensee staff time to deliver the recurring notification training to 800 licensee staff members at each site for operating reactors.
    - Operations/Engineering/Administrative staff: 600 people * 0.083 hours = 50 hours
    - Security and CSAT staff: 200 people * 0.17 hours = 34 hours
    - *Total 84 hours*

Decommissioning Reactors

- On average, each site will require 34 hours of licensee staff time to deliver the recurring notification training for to 300 licensee staff members at each site decommissioning reactors.
    - Operations/Engineering/Administrative staff: 200 people * 0.083 hour = 17 hours
    - Security and CSAT staff: 100 people * 0.17 hours = 17 hours
    - *Total 34 hours*

Table 4-9 shows the estimated annual cost per site for recurring notification training, by type of site.

**Table 4-9. Estimated Annual Cost per Site for Recurring Notification Training (2014 Dollars)**

| Type of Site | Annual Cost to Industry [a, b] | Annual Cost to the NRC |
|---|---|---|
| Sites with only reactors that are currently in commercial operation | $10,500 | Not applicable |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $10,500 | Not applicable |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $10,500 | Not applicable |
| Sites with only reactors that currently are in decommissioning | $4,250[c] | Not applicable |

[a] Annual Cost to Industry = [1 recurring notification training per year] x [84 hour/training] x [$125/hour].

[b] Costs in the table are rounded to the nearest whole number.

[c] Annual Cost to Industry = [1 recurring notification training per year] x [34 hour/training] x [$125/hour].

# 5. Results

This section organizes the analytical results into four separate sections. Section 5.1 presents results on the benefits and costs of the final rule as a whole, as well as disaggregated results for each of the regulatory requirements that comprise the final rule. Section 5.2 presents the results of a sensitivity analysis conducted to determine whether, and to what extent, the results of the analysis are sensitive to changes in key assumptions and numeric inputs. Section 5.3 evaluates disaggregation of the requirements in the final rule. Section 5.4 addresses the applicability of a safety goal evaluation to the final rule.

## 5.1. Benefits and Costs of the Final Rule

This section discusses the benefits and costs estimated for the final rule.

### 5.1.1. Summary of Benefits and Costs

Tables 5-1 through 5-3 summarize the benefits and costs of the final rule as a whole, and for each quantifiable regulatory requirement contained in the final rule.

The final rule as a whole (Option 2) would result in a quantitative cost estimated between $27.9 million and $42.6 million (at a 7 percent and 3 percent discount rate, respectively). These costs are associated with four affected attributes—industry implementation, industry operation, NRC implementation, and NRC operation. Section 4.2.4 provides detail on the incremental activities under the final rule, and estimates the one-time and annual costs associated with these activities.

The analysis does not quantify the benefits associated with Option 2, but it does describe them qualitatively in Table 5-1. The NRC staff assumes that Option 2 would result in qualitative benefits in the following attributes: safeguards and security considerations, regulatory efficiency, public health (accident), occupational health (accident), off-site property, on-site property, and other government agencies.

Overall, the benefits include an increased ability to protect digital computers, communication systems, and networks associated with safety-related; important-to-safety; security; emergency preparedness, to include offsite communications (SSEP); and support systems and equipment which, if compromised, would adversely impact SSEP functions. Notifications 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).

## Table 5-1. Summary of Overall Benefits and Costs (Quantitative and Qualitative)

| | Benefits | Costs (2014 Dollars) |
|---|---|---|
| **Option 2: Final Rule** | **Safeguards and Security Considerations –** Increased NRC's ability to respond to cyber security events and to effectively monitor ongoing licensee actions and inform other licensees in a timely manner of cyber security-significant events and thus, protect public health and safety and the common defense and security.<br><br>**Regulatory Efficiency –** The regulatory action will enhance regulatory efficiency by establishing staff-approved guidance that licensees may use to track, correct, and prevent cyber security events. Consequently, licensees and the NRC will face less uncertainty in determining compliance with the regulatory requirements in the final rule.<br><br>**Public Health (Accident) –** Timely notification of potential and/or imminent cyber attacks will improve the ability of the NRC and other licensees to respond and take actions necessary to mitigate the adverse impacts of cyber attacks directed against nuclear power reactors. These actions are expected to avert potential radiation exposure to the public following an attack.<br><br>**Occupational Health (Accident) –** Timely notification of potential and/or imminent cyber attacks will improve the ability of the NRC and other licensees to respond and take actions necessary to mitigate the adverse impacts of cyber attacks directed against nuclear power reactors. These actions are expected to avert potential radiation exposure to site workers following an attack.<br><br>**Off-Site Property –** Timely notification of potential and/or imminent cyber attacks will improve the ability of the NRC and other licensees to respond and take actions necessary to mitigate the adverse impacts of cyber attacks directed against nuclear power reactors. These actions are expected to avert potential off-site property damage and costs that may result from an attack.<br><br>**On-Site Property –** Timely notification of potential and/or imminent cyber attacks will improve the ability of the NRC and other licensees to respond and take actions necessary to mitigate the adverse impacts of cyber attacks directed against nuclear power reactors. These actions are expected to avert potential on-site property damage and costs that may result from an attack.<br><br>**Other Government Agencies** – The CSEN final rule will not have an effect on other Government agencies because the reporting of suspicious or criminal activity related to terrorism (e.g., physical security, cyber security) is captured under the NIPP and part of the NRC's strategic communications mission. In addition, certain cyber security events reported to the NRC that fall within the scope of 10 CFR 73.54 will not need to be reported to other Government agencies. | **Industry Implementation:**<br><br>$3.0 million<br><br>**Industry Operation:**<br><br>$22.5 million using a 7% discount rate<br>$35.9 million using a 3% discount rate<br><br>**NRC Implementation:**<br><br>$166,375<br><br>**NRC Operation:**<br><br>$2.2 million using a 7% discount rate<br>$3.5 million using a 3% discount rate<br><br>**Total Costs:**<br><br>$27.9 million using a 7% discount rate<br>$42.6 million using a 3% discount rate |

**Table 5-2. Summary of Quantified One-Time, Annual, and Overall Costs of the Final Rule (2014 Dollars)**

| Cost Category | One-Time Costs | Annual Costs | Present Value | |
|---|---|---|---|---|
| | | | 7% Discount Rate | 3% Discount Rate |
| Rulemaking activities | $166,375 | $0 | $166,375 | $166,375 |
| Development of procedures | $715,000 | $0 | $715,000 | $715,000 |
| Initial notification training | $2,248,750 | $0 | $2,248,750 | $2,248,750 |
| One-hour notifications | $0 | $22,470 | $309,810 | $494,647 |
| Four-hour notifications | $0 | $41,016 | $565,497 | $902,861 |
| Eight-hour notifications | $0 | $103,145 | $1,419,390 | $2,263,996 |
| Recordable events | $0 | $38,749 | $532,733 | $849,332 |
| Written security follow-up reports | $0 | $932,174 | $12,852,172 | $20,519,587 |
| Inspections | $0 | $0 | $0 | $0 |
| Recurring notification training | $0 | $657,500 | $9,013,419 | $14,348,917 |
| **Total** | **$3,130,125** | **$1,795,054** | **$27,823,147** | **$42,509,465** |

**Table 5-3. Summary of Quantified One-Time, Annual, and Overall Costs to Industry and the NRC, by Regulatory Requirement (2014 Dollars)**

| Cost Category | Costs to Industry | | | | Costs to the NRC | | | |
|---|---|---|---|---|---|---|---|---|
| | One-Time Costs | Annual Costs | Present Value | | One-Time Costs | Annual Costs | Present Value | |
| | | | 7% Discount Rate | 3% Discount Rate | | | 7% Discount Rate | 3% Discount Rate |
| Rulemaking activities | $0 | $0 | $0 | $0 | $166,375 | $0 | $166,375 | $166,375 |
| Development of procedures | $715,000 | $0 | $715,000 | $715,000 | $0 | $0 | $0 | $0 |
| Initial notification training | $2,248,750 | $0 | $2,248,750 | $2,248,750 | $0 | $0 | $0 | $0 |
| One-hour notifications | $0 | $3,867 | $53,320 | $85,134 | $0 | $18,603 | $256,490 | $409,512 |
| Four-hour notifications | $0 | $3,867 | $53,320 | $85,134 | $0 | $37,149 | $512,177 | $817,727 |
| Eight-hour notifications | $0 | $9,640 | $132,661 | $211,603 | $0 | $93,505 | $1,286,730 | $2,052,393 |
| Recordable events | $0 | $38,749 | $532,733 | $849,332 | $0 | $0 | $0 | $0 |
| Written security follow-up reports | $0 | $921,000 | $12,698,110 | $20,273,610 | $0 | $11,174 | $154,063 | $245,977 |
| Inspections | $0 | $0 | $0 | $0 | $0 | $0 | $0 | $0 |
| Recurring notification training | $0 | $657,500 | $9,013,419 | $14,348,917 | $0 | $0 | $0 | $0 |
| **Total** | **$2,963,750** | **$1,634,623** | **$25,447,313** | **$38,817,482** | **$166,375** | **$160,431** | **$2,375,834** | **$3,691,983** |

### 5.1.2. Incremental Costs by Type of Site

Tables 5-4 and 5-5 show the costs to industry and the NRC based on type of site, respectively. The tables also show the per-site costs and number of sites used to estimate total costs.

**Table 5-4. Summary of Estimated Costs to Industry under the Final Rule, by Type of Site (2014 Dollars)**

| Type of Site | Per-Site Costs | Number of Sites | Total Costs |
|---|---|---|---|
| **One-Time Costs** | | | |
| Sites with only reactors that are currently in commercial operation | $46,750 | 58 | $2,711,500 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $46,750 | 2 | $93,500 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $46,750 | 1 | $46,750 |
| Sites with only reactors that currently are in decommissioning | $28,000 | 4 | $112,000 |
| | | **Total One-Time Costs** | **$2,963,750** |
| **Annual Costs** | | | |
| Sites with only reactors that are currently in commercial operation | $26,407 | 58 | $1,531,606 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $26,407 | 2 | $52,814 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $26,407 | 1 | $26,407 |
| Sites with only reactors that currently are in decommissioning | $5,949 | 4 | $23,796 |
| | | **Total Annual Costs** | **$1,634,623** |

**Table 5-5. Summary of Estimated Costs to the NRC under the Final Rule, by Type of Site (2014 Dollars)**

| Type of Site | Per-Site Costs | Number of Sites | Total Costs |
|---|---|---|---|
| **One-Time Costs** | | | |
| All sites | Not Applicable | 65 | $166,375 |
| | | **Total One-Time Costs** | **$166,375** |
| **Annual Costs** | | | |
| Sites with only reactors that are currently in commercial operation | $2,603 | 58 | $150,974 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $2,603 | 2 | $5,206 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $2,603 | 1 | $2,603 |
| Sites with only reactors that currently are in decommissioning | $412 | 4 | $1,648 |
| | | **Total Annual Costs** | **$160,431** |

.

Tables 5-6 and 5-7 summarize the estimated per-site costs associated with each of the cost categories for industry and the NRC, respectively.

**Table 5-6. Estimated Per-Site Costs to Industry under the Final Rule (2014 Dollars)**

| Cost Category | Sites with Only Reactors that are Currently in Commercial Operation | Sites with Both Operating Reactors and Projected New Reactors under a Part 52 License | Sites with Both Operating Reactors and Reactors under Active Construction under a Part 50 License | Sites with Only Reactors that Currently are in Decommissioning |
|---|---|---|---|---|
| **One-Time Costs** | | | | |
| Develop procedures | $11,000 | $11,000 | $11,000 | $11,000 |
| Develop and deliver initial notification training to designated personnel | $35,750 | $35,750 | $35,750 | $17,000 |
| **Total One-Time Costs** | **$46,750** | **$46,750** | **$46,750** | **$28,000** |
| **Annual Costs** | | | | |
| Make one-hour notifications (10 CFR 73.77(a)(1) and (c)) | $63 | $63 | $63 | $6 |
| Make four-hour notifications (10 CFR 73.77(a)(2)(i)-(iii) and (c)) | $63 | $63 | $63 | $6 |
| Make eight-hour notifications (10 CFR 73.77(a)(3) and (c)) | $156 | $156 | $156 | $31 |
| Record events in site's corrective action program (10 CFR 73.77(b)) | $625 | $625 | $625 | $156 |
| Prepare and submit written security follow-up reports (10 CFR 73.77(d)) | $15,000 | $15,000 | $15,000 | $1,500 |
| Provide information during Inspections (10 CFR 73.77(b)) | $0 | $0 | $0 | $0 |
| Update and deliver recurring notification training to designated personnel (10 CFR 73.77) | $10,500 | $10,500 | $10,500 | $4,250 |
| **Total Annual Costs** | **$26,407** | **$26,407** | **$26,407** | **$5,949** |

**Table 5-7. Estimated Per-Site Costs to the NRC under the Final Rule (2014 Dollars)**

| Cost Category | Sites with Only Reactors that are Currently in Commercial Operation | Sites with Both Operating Reactors and Projected New Reactors under a Part 52 License | Sites with Both Operating Reactors and Reactors under Active Construction under a Part 50 License | Sites with Only Reactors that Currently are in Decommissioning |
|---|---|---|---|---|
| **One-Time Costs** | | | | |
| Perform rulemaking activities | $166,375 | | | |
| **Annual Costs** | | | | |
| Respond to one-hour notifications (10 CFR 73.77(a)(1) and (c)) | $303 | $303 | $303 | $30 |
| Respond to four-hour notifications (10 CFR 73.77(a)(2)(i)-(iii) and (c)) | $605 | $605 | $605 | $61 |
| Respond to eight-hour notifications (10 CFR 73.77(a)(3) and (c)) | $1,513 | $1,513 | $1,513 | $303 |
| Review written security follow-up reports (10 CFR 73.77(d)) | $182 | $182 | $182 | $18 |
| Review information during inspections (10 CFR 73.77(b)) | $0 | $0 | $0 | $0 |
| **Total Annual Costs** | **$2,603** | **$2,603** | **$2,603** | **$412** |

## 5.2. Sensitivity Analysis

This section presents a sensitivity analysis in order to determine whether, and to what extent, the results of the analysis are sensitive to costs according to the following alternative sets of parameters:

- Best Estimate. The NRC's best estimate for key parameters is based on historic data from voluntary cyber security reports from licensees. These values reflect the key assumptions and numeric inputs discussed in Section 4.

- Alternative Estimate. Higher estimates for the frequency of cyber security events. These key parameters were selected for the sensitivity analysis because of the uncertainty resulting from limited availability of data on the frequency of cyber security events. The alternative estimates are based on the increased frequency of cyber security events within the Federal Government which could potentially affect other critical infrastructures and resources (i.e. nuclear sector). The NRC used these two parameters to estimate the alternative annual frequencies a site could see in a higher threat situation.

Table 5-8 presents the assumptions associated with key parameters used in the sensitivity analysis.

**Table 5-8. Assumptions Associated with Key Parameters Used in Sensitivity Analysis**

| Data Element | Type of Site | Best Estimate | Alternative Estimate |
|---|---|---|---|
| Annual Number of Events that Will Require a One-Hour Notification | Sites with only reactors that are currently in commercial operation | 0.50 | 5 |
| | Sites with both operating reactors and projected new reactors under a Part 52 license | 0.50 | 5 |
| | Sites with both operating reactors and reactors under active construction under a Part 50 license | 0.50 | 5 |
| | Sites with only reactors that currently are in decommissioning | 0.05 | 1 |
| Annual Number of Events that Will Require a Four-Hour Notification | Sites with only reactors that are currently in commercial operation | 1 | 10 |
| | Sites with both operating reactors and projected new reactors under a Part 52 license | 1 | 10 |
| | Sites with both operating reactors and reactors under active construction under a Part 50 license | 1 | 10 |
| | Sites with only reactors that currently are in decommissioning | 0.10 | 2 |
| Annual Number of Events that Will Require an Eight-Hour Notification | Sites with only reactors that are currently in commercial operation | 2.5 | 15 |
| | Sites with both operating reactors and projected new reactors under a Part 52 license | 2.5 | 15 |
| | Sites with both operating reactors and reactors under active construction under a Part 50 license | 2.5 | 15 |
| | Sites with only reactors that currently are in decommissioning | 0.50 | 3.5 |

**Table 5-8. Assumptions Associated with Key Parameters Used in Sensitivity Analysis**

| Data Element | Type of Site | Best Estimate | Alternative Estimate |
|---|---|---|---|
| Annual Number of Entries in the Site's Corrective Actions Program | Sites with only reactors that are currently in commercial operation | 10 | 30 |
| | Sites with both operating reactors and projected new reactors under a Part 52 license | 10 | 30 |
| | Sites with both operating reactors and reactors under active construction under a Part 50 license | 10 | 30 |
| | Sites with only reactors that currently are in decommissioning | 2.5 | 5 |
| Annual Number of Written Follow-Up Report after Initial Cyber Security Event Notification | Sites with only reactors that are currently in commercial operation | 1.5 | 20 |
| | Sites with both operating reactors and projected new reactors under a Part 52 license | 1.5 | 20 |
| | Sites with both operating reactors and reactors under active construction under a Part 50 license | 1.5 | 20 |
| | Sites with only reactors that currently are in decommissioning | 0.15 | 4.5 |

In conducting the sensitivity analysis, the NRC re-computed the annual costs of the final rule using the alternative estimate parameters shown in Table 5-8. The results of the sensitivity analysis are presented in Table 5-9. Appendix C provides additional detail on the estimation of the overall costs of the final rule based on the sensitivity analysis.

**Table 5-9. Overall Costs of the Final Rule Based on the Sensitivity Analysis (2014 Dollars)**

| Set of Data Elements | 7% Discount Rate | | 3% Discount Rate | |
|---|---|---|---|---|
| | Present Value | Annualized | Present Value | Annualized |
| Best Estimate | $27.9 million | $1.8 million | $42.6 million | $1.8 million |
| Alternative Estimate | $203.4 million | $14.6 million | $322.5 million | $14.8 million |

As shown in the table, the overall costs of the final rule are estimated to be between $27.9 million and $322.5 million (2014 dollars), depending on the alternative set of parameters used to estimate the costs. In all cases, NRC concludes that the final rule is not an "economically significant regulatory action" under Section 3(f)(1) of Executive Order 12866.

## 5.3. Disaggregation

The NRC staff has evaluated the rulemaking to determine whether specific requirements have to be considered separately, but has determined that the requirements in the final rule are narrowly focused. Therefore, the analysis of disaggregated requirements is not necessary.

## 5.4. Safety Goal Evaluation

The analysis relies primarily on a qualitative (rather than quantitative) evaluation of several of the affected attributes (safeguards and security considerations, regulatory efficiency, public health (accident), occupational health (accident), off-site property, and on-site property) due to the difficulty in quantifying the impact of the current rulemaking. These attributes will be affected by the regulatory options through the associated reduction in the risks of radiological sabotage and damage to the reactor core and the spent fuel. Quantification of any of these attributes would require estimation of factors such as: (1) the frequency of attempted radiological sabotage, (2) the frequency with which radiological sabotage attempts are (i.e., pre-rule) and will be (i.e., post-rule) successful, and (3) the impacts associated with successful radiological sabotage attempts.

Safety goal evaluations are applicable only to regulatory initiatives considered to be generic safety enhancement backfit subject to the substantial additional protection standard at section 50.109(a)(3).4. Some aspects of this rule may qualify as generic safety enhancements because they may affect the likelihood of core damage or spent fuel damage, which generally are the focus of a quantitative safety goal evaluation. However, the magnitude of this change is not readily quantifiable due to uncertainties discussed in Section 4.2 above. A more dominant effect of this rule is to reduce the probability of other types of damage associated with a wide array of acts of sabotage, although this effect is equally difficult to quantify. Because the change in safety associated with the rulemaking cannot be quantified, the regulatory changes cannot be compared to the NRC's safety goals.

## 6. Decision Rationale for Selection of the Proposed Action

Relative to the "no-action" alternative, the final rule would cost industry between $27.7 million and $41.1 million (at a 7-percent and 3-percent discount rate, respectively). The NRC costs are estimated between $2.4 million and $3.7 million (at a 7-percent and 3-percent discount rate, respectively). Therefore, the total cost of this final rule is estimated to range from $30.1 million (7-percent discount rate) to $44.8 million (3-percent discount rate). (Costs are presented at a high level; more detailed information is presented in Sections 4 and 5).

Although the NRC did not quantify the benefits of this final rule, the staff did qualitatively examine benefits and concluded that the rule would provide safety and security-related benefits. The NRC believes that prompt notification of a cyber attack is vital to the NRC's ability to take immediate action in response to a cyber attack and, if necessary, to notifiy 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 addition, reporting suspicious cyber activities and incidents, even though their significance may seem minor, is a substantial safety enhancement because it increases awareness of cyber security threats and allows time to plan for appropriate response if an attack is substantiated.

Based on the NRC's assessment of the costs and benefits of the final rule on licensee facilities, the NRC has concluded that the final rule provisions would be justified to support the NRC's strategic communications mission as well as protecting the public health and safety or the common defense and security.

## 7. Implementation

The final rule is to take effect 30 days after publication in the *Federal Register* with a compliance date within 180 days after publication in the *Federal Register* for those licensed to operate under 10 CFR Parts 50 and 52, and subject to 10 CFR 73.54. The NRC staff does not expect this rule to have any impact on other requirements.

## 8. List of Tables

## 9. References

Dominion Energy Kewaunee, Inc.; "Dominion Energy Kewaunee, Inc., Kewaunee Power Station, Certification of Permanent Cessation of Power Operations;" February 25, 2013. ADAMS Accession No. ML13058A065. Available at: http://pbadupws.nrc.gov/docs/ML1305/ML13058A065.pdf, last accessed on August 13, 2014.

Dominion Energy Kewaunee, Inc.; "Dominion Energy Kewaunee Inc., Kewaunee Power Station, Update to Irradiated Fuel Management Plan pursuant to 10 CFR 50.54(bb);" April 15, 2014. ADAMS Accession No. ML14219A738. Available at: http://pbadupws.nrc.gov/docs/ML1421/ML14219A738.pdf, last accessed on August 13, 2014.

Duke Energy, "Crystal River Unit 3 – Certification of Permanent Cessation of Power Operations and that Fuel Has Been Permanently Removed from Reactor," February 20,2013. ADAMS Accession No. ML13056A005. Available at: http://pbadupws.nrc.gov/docs/ML1305/ML13056A005.pdf, last accessed on August 13, 2014.

U.S. Department of Labor, Bureau of Labor Statistics; "May 2013 National Occupational Employment and Wage Estimates, United States;" April 1, 2014. Available at: http://www.bls.gov/oes/2013/may/oes_nat.htm, last accessed on July 7, 2014.

U.S. Department of Labor, Bureau of Labor Statistics; *Employment Cost Index, Historical Listing – Volume V;* "Table 8. Employment Cost Index for wages and salaries, for civilian workers, by occupation and industry, continuous occupational and industry series (not seasonally adjusted);" April 2014. Available at: http://www.bls.gov/web/eci/ecicois.pdf, last accessed on July 7, 2014.

U.S. Department of Labor, Bureau of Labor Statistics; *News Release, Employer Costs for Employee Compensation – March 2014*; "Table 1. Employer costs per hour worked for employee compensation and costs as a percent of total compensation: Civilian workers, by major occupational and industry group, March 2014;" June 11, 2014. Available at: http://www.bls.gov/news.release/archives/ecec_06112014.pdf, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission, "Locations of Power Reactor Sites Undergoing Decommissioning" Web page, www.nrc.gov. Data current as of April 24, 2014. Available at: http://www.nrc.gov/info-finder/decommissioning/power-reactor/, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission, "Combined License Applications for New Reactors" Web page, www.nrc.gov. Data current as of July 1, 2014. Available at: http://www.nrc.gov/reactors/new-reactors/col.html, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission, "Operating Nuclear Power Reactors (by Location or Name)" Web page, www.nrc.gov. Data current as of March 19, 2014. Available at: http://www.nrc.gov/info-finder/reactor/, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission, Rulemaker@nrc.gov, "NRC Labor Rates for Use in Regulatory Analyses (as of October 2013)," January 2, 2014.

U.S. Nuclear Regulatory Commission, *2013-2014 Information Digest* (NUREG-1350, Volume 25), "Appendix A: U.S. Commercial Nuclear Power Reactors - Operating Reactors under Active Construction or Deferred Policy," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission, *2013-2014 Information Digest* (NUREG-1350, Volume 25), "Appendix H: U.S. Commercial Nuclear Power Reactor Operating Licenses - Expiration by Year, 2013–2049," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission; "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications, Proposed Rule;" 76 *Federal Register* 6200 (February 3, 2011) (amending 10 CFR Part 73). Available at: http://www.gpo.gov/fdsys/pkg/FR-2011-02-03/pdf/2011-1766.pdf, last accessed on July 7,2014.

U.S. Nuclear Regulatory Commission; "Power Reactor Security Requirements, Final Rule;" 74 *Federal Register* 13926 (March 27, 2009) (amending 10 CFR Parts 50, 52, 72, and 73). Available at: http://www.gpo.gov/fdsys/pkg/FR-2009-03-27/pdf/E9-6102.pdf, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission; "Power Reactor Security Requirements, Proposed Rule;" 71 *Federal Register* 62664 (October 26, 2006) (amending 10 CFR Parts 50, 72, and 73). Available at: http://www.gpo.gov/fdsys/pkg/FR-2006-10-26/pdf/06-8678.pdf, last accessed on July 7, 2014.

U.S. Nuclear Regulatory Commission; *Regulatory Analysis Technical Evaluation Handbook* (NUREG/BR-OI84); Section 5.7, “Quantification of Attributes;” January 1997. Available at: http://pbadupws.nrc.gov/docs/ML0501/ML050190193.pdf, last accessed on July 29, 2014.

[Page intentionally left blank.]

# Appendix A
# Backfit Analysis

[Page intentionally left blank.]

# Backfit Analysis

The U.S. Nuclear Regulatory Commission (NRC) is amending its regulations in Part 73 to add reporting and recordkeeping requirements related to certain cyber security events. The NRC is adding these requirements because cyber security event reporting and recordkeeping requirements were not included in the NRC's final rule that added section 73.54 to the NRC's regulations (74 *FR* 13925; March 27, 2009). Section 73.54 requires power reactor licensees to establish and maintain a cyber security program at their facilities 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 as described in section 73.1. These new requirements are being added to the security event notification provisions of Part 73 as section 73.77.

Revisions that amend existing information collection and reporting requirements or impose new information and collection and reporting requirements are not considered to be backfits, as presented in the charter for the NRC's Committee to Review Generic Requirements (CRGR). Therefore, a backfit analysis has not been completed for this final rule.

[Page intentionally left blank.]

# Appendix B
# U.S. Commercial Nuclear Power Reactor Sites Affected by the Final Rule

[Page intentionally left blank.]

## Table B-1. U.S. Commercial Nuclear Power Reactor Sites Subject to the Cyber Security Event Notifications Rule

| No. | Site Name | Location | Reactors at Site | | | | | | Type of Site for Purposes of Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | | | Operating Reactor 1 Unit | Operating Reactors 2 Units | Operating Reactors 3 Units | Projected New Reactor Issued Combined License under Part 52 | Reactors under Active Construction under Part 50 License | Reactors Undergoing Decommissioning | |
| 1 | Arkansas Nuclear One | London, AR | | X | | | | | Site with only reactors that are currently in commercial operation |
| 2 | Beaver Valley Power Station | Shippingport, PA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 3 | Braidwood Station | Braceville, IL | | X | | | | | Site with only reactors that are currently in commercial operation |
| 4 | Browns Ferry Nuclear Plant | Athens, IL | | | X | | | | Site with only reactors that are currently in commercial operation |
| 5 | Brunswick Steam Electric Plant | Southport, NC | | X | | | | | Site with only reactors that are currently in commercial operation |
| 6 | Byron Station | Byron, IL | | X | | | | | Site with only reactors that are currently in commercial operation |
| 7 | Callaway Plant | Fulton, MO | X | | | | | | Site with only reactors that are currently in commercial operation |
| 8 | Calvert Cliffs Nuclear Power Plant | Lusby, MD | | X | | | | | Site with only reactors that are currently in commercial operation |
| 9 | Catawba Nuclear Station | York, SC | | X | | | | | Site with only reactors that are currently in commercial operation |
| 10 | Clinton Power Station | Clinton, IL | X | | | | | | Site with only reactors that are currently in commercial operation |
| 11 | Columbia Generating Station | Benton County, WA | X | | | | | | Site with only reactors that are currently in commercial operation |
| 12 | Comanche Peak Nuclear Power Plant | Glen Rose, TX | | X | | | | | Site with only reactors that are currently in commercial operation |
| 13 | Cooper Nuclear Station | Brownville, NE | X | | | | | | Site with only reactors that are currently in commercial operation |
| 14 | Crystal River | Crystal River, FL | | | | | | X | Site with only reactors that currently are in decommissioning |
| 15 | Davis Besse Nuclear Power Station | Oak Harbor, OH | X | | | | | | Site with only reactors that are currently in commercial operation |

## Table B-1. U.S. Commercial Nuclear Power Reactor Sites Subject to the Cyber Security Event Notifications Rule

| No. | Site Name | Location | Reactors at Site | | | | | | Type of Site for Purposes of Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | | | Operating Reactor 1 Unit | Operating Reactors 2 Units | Operating Reactors 3 Units | Projected New Reactor Issued Combined License under Part 52 | Reactors under Active Construction under Part 50 License | Reactors Undergoing Decommissioning | |
| 16 | Diablo Canyon Nuclear Power Plant | Avila Beach, CA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 17 | Donald C. Cook Nuclear Plant | Bridgman, MI | | X | | | | | Site with only reactors that are currently in commercial operation |
| 18 | Dresden Nuclear Power Station | Morris, IL | | X | | | | X | Site with only reactors that are currently in commercial operation [a] |
| 19 | Duane Arnold Energy Center | Palo, IA | X | | | | | | Site with only reactors that are currently in commercial operation |
| 20 | Edwin I. Hatch Nuclear Plant | Baxley, GA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 21 | Fermi | Newport, MI | X | | | | | X | Site with only reactors that are currently in commercial operation [a] |
| 22 | Fort Calhoun Station | Ft. Calhoun, NE | X | | | | | | Site with only reactors that are currently in commercial operation |
| 23 | Grand Gulf Nuclear Station | Port Gibson, MS | X | | | | | | Site with only reactors that are currently in commercial operation |
| 24 | H.B. Robinson Steam Electric Plant | Hartsville, SC | X | | | | | | Site with only reactors that are currently in commercial operation |
| 25 | Hope Creek Generating Station | Hancocks Bridge, NJ | X | | | | | | Site with only reactors that are currently in commercial operation |
| 26 | Indian Point Nuclear Power Plant | Buchanan, NY | | X | | | | X | Site with only reactors that are currently in commercial operation [a] |
| 27 | James A. FitzPatrick Nuclear Power Plant | Scriba, NY | X | | | | | | Site with only reactors that are currently in commercial operation |
| 28 | Joseph M. Farley Nuclear Plant | Columbia, AL | | X | | | | | Site with only reactors that are currently in commercial operation |
| 29 | Kewaunee | Kewaunee, WI | | | | | | X | Site with only reactors that currently are in decommissioning |
| 30 | LaSalle County Station | Marseilles, IL | | X | | | | | Site with only reactors that are currently in commercial operation |

## Table B-1. U.S. Commercial Nuclear Power Reactor Sites Subject to the Cyber Security Event Notifications Rule

| No. | Site Name | Location | Reactors at Site | | | | | | Type of Site for Purposes of Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | | | Operating Reactor 1 Unit | Operating Reactors 2 Units | Operating Reactors 3 Units | Projected New Reactor Issued Combined License under Part 52 | Reactors under Active Construction under Part 50 License | Reactors Undergoing Decommissioning | |
| 31 | Limerick Generating Station | Limerick, PA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 32 | McGuire Nuclear Station | Huntersville, NC | | X | | | | | Site with only reactors that are currently in commercial operation |
| 33 | Millstone Power Station | Waterford, CT | | X | | | | X | Site with only reactors that are currently in commercial operation [a] |
| 34 | Monticello Nuclear Generating Plant | Monticello, MN | X | | | | | | Site with only reactors that are currently in commercial operation |
| 35 | Nine Mile Point Nuclear Station | Scriba, NY | | X | | | | | Site with only reactors that are currently in commercial operation |
| 36 | North Anna Power Station | Mineral, VA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 37 | Oconee Nuclear Station | Seneca, SC | | | X | | | | Site with only reactors that are currently in commercial operation |
| 38 | Oyster Creek Nuclear Generating Station [c] | Forked River, NJ | X | | | | | | Site with only reactors that are currently in commercial operation |
| 39 | Palisades Nuclear Plant | Covert, MI | X | | | | | | Site with only reactors that are currently in commercial operation |
| 40 | Palo Verde Nuclear Generating Station | Wintersburg, AZ | | | X | | | | Site with only reactors that are currently in commercial operation |
| 41 | Peach Bottom Atomic Power Station | Delta, PA | | X | | | | X | Site with only reactors that are currently in commercial operation [a] |
| 42 | Perry Nuclear Power Plant | Perry, OH | X | | | | | | Site with only reactors that are currently in commercial operation |
| 43 | Pilgrim Nuclear Power Station | Plymouth, MA | X | | | | | | Site with only reactors that are currently in commercial operation |
| 44 | Point Beach Nuclear Plant | Two Rivers, WI | | X | | | | | Site with only reactors that are currently in commercial operation |
| 45 | Prairie Island Nuclear Generating Plant | Welch, MN | | X | | | | | Site with only reactors that are currently in commercial operation |

## Table B-1. U.S. Commercial Nuclear Power Reactor Sites Subject to the Cyber Security Event Notifications Rule

| No. | Site Name | Location | Reactors at Site | | | | | | Type of Site for Purposes of Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | | | Operating Reactor 1 Unit | Operating Reactors 2 Units | Operating Reactors 3 Units | Projected New Reactor Issued Combined License under Part 52 | Reactors under Active Construction under Part 50 License | Reactors Undergoing Decommissioning | |
| 46 | Quad Cities Nuclear Power Station | Cordova, IL | | X | | | | | Site with only reactors that are currently in commercial operation |
| 47 | R.E. Ginna Nuclear Power Plant | Ontario, NY | X | | | | | | Site with only reactors that are currently in commercial operation |
| 48 | River Bend Station | St. Francisville, LA | X | | | | | | Site with only reactors that are currently in commercial operation |
| 49 | Salem Nuclear Generating Station | Hancocks Bridge, NJ | | X | | | | | Site with only reactors that are currently in commercial operation |
| 50 | San Onofre Nuclear Generating Station | San Clemente, CA | | | | | | X | Site with only reactors that currently are in decommissioning |
| 51 | Seabrook Station | Seabrook, NH | X | | | | | | Site with only reactors that are currently in commercial operation |
| 52 | Sequoyah Nuclear Plant | Soddy-Daisy, TN | | X | | | | | Site with only reactors that are currently in commercial operation |
| 53 | Shearon Harris Nuclear Power Plant | New Hill, NC | X | | | | | | Site with only reactors that are currently in commercial operation |
| 54 | South Texas Project | Bay City, TX | | X | | | | | Site with only reactors that are currently in commercial operation |
| 55 | St. Lucie Plant | Jensen Beach, FL | | X | | | | | Site with only reactors that are currently in commercial operation |
| 56 | Surry Power Station | Surry, VA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 57 | Susquehanna Steam Electric Station | Berwick, PA | | X | | | | | Site with only reactors that are currently in commercial operation |
| 58 | Three Mile Island Nuclear Station | Middletown, PA | X | | | | | X | Site with only reactors that are currently in commercial operation [a] |
| 59 | Turkey Point Nuclear Generating | Homestead, FL | | X | | | | | Site with only reactors that are currently in commercial operation |
| 60 | Vermont Yankee Nuclear Power Station | Vernon, VT | | | | | | X | Site with only reactors that currently are in decommissioning [b] |

## Table B-1. U.S. Commercial Nuclear Power Reactor Sites Subject to the Cyber Security Event Notifications Rule

| No. | Site Name | Location | Reactors at Site | | | | | | Type of Site for Purposes of Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | | | Operating Reactor 1 Unit | Operating Reactors 2 Units | Operating Reactors 3 Units | Projected New Reactor Issued Combined License under Part 52 | Reactors under Active Construction under Part 50 License | Reactors Undergoing Decommissioning | |
| 61 | Virgil C. Summer Nuclear Station | Jenkinsville, SC | X | | | X | | | Site with both operating reactors and projected new reactors under a Part 52 license |
| 62 | Vogtle Electric Generating Plant | Waynesboro, GA | | X | | X | | | Site with both operating reactors and projected new reactors under a Part 52 license |
| 63 | Waterford Steam Electric Station | Killona, LA | X | | | | | | Site with only reactors that are currently in commercial operation |
| 64 | Watts Bar Nuclear Plant | Spring City, TN | X | | | | X | | Site with both operating reactors and reactors under active construction under a Part 50 license |
| 65 | Wolf Creek Generating Station | Burlington, KS | X | | | | | | Site with only reactors that are currently in commercial operation |

[a] Site has operating reactor(s) and decommissioning reactor(s). Because the final rule applicability period for an operating reactor exceeds the period for a reactor that already is decommissioning, the site is categorized as a "site with only reactors that are currently in commercial operation" for purposes of this analysis.

[b] The Vermont Yankee Nuclear Power Station is assumed to be in decommissioning on the effective date of the final rule (i.e., in 2015) and thus, is categorized as "site with only reactors that currently are in decommissioning." The Vermont Yankee Nuclear Power Station plans to terminate commercial operation in December 2014. The operating license renewal applications for Indian Point Nuclear Generating Units 2 and 3 are currently under NRC consideration and it was assumed that these license renewals will be granted.

[c] Oyster Creek Nuclear Generating Station plans to terminate commercial operation in 2019.

**Sources:**


(1) NRC, "Operating Nuclear Power Reactors (by Location or Name)" Web page, www.nrc.gov. Data current as of March 19, 2014. Available at: http://www.nrc.gov/info-finder/reactor/, last accessed on May 26, 2014.

(2) NRC, "Locations of Power Reactor Sites Undergoing Decommissioning" Web page, www.nrc.gov. Data current as of April 24, 2014. Available at: http://www.nrc.gov/info-finder/decommissioning/power-reactor/, last accessed on May 26, 2014.

(3) NRC, 2013-2014 Information Digest (NUREG-1350, Volume 25), "Appendix A: U.S. Commercial Nuclear Power Reactors - Operating Reactors under Active Construction or Deferred Policy," August 2013. Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1350/#pubinfo, last accessed on May 26, 2014.

(4) NRC, "Combined License Applications for New Reactors" Web page, www.nrc.gov. Data current as of April 17, 2014. Available at: http://www.nrc.gov/reactors/new-reactors/col.html, last accessed on May 26, 2014

[Page intentionally left blank.]

# Appendix C
# Estimation of Overall Costs of the Final Rule Based on the Sensitivity Analysis

[Page intentionally left blank.]

## Table C-1. Industry Implementation (One-Time Costs): Develop Procedures

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $11,000 | $638,000 | $638,000 | $638,000 | $46,387 | $29,312 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $11,000 | $22,000 | $22,000 | $22,000 | $1,466 | $777 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $11,000 | $11,000 | $11,000 | $11,000 | $737 | $399 |
| Sites with only reactors that currently are in decommissioning | $11,000 | $44,000 | $44,000 | $44,000 | $4,515 | $3,578 |
| **Total for all sites** | | **$715,000** | **$715,000** | **$715,000** | **$53,106** | **$34,066** |

## Table C-2. Industry Implementation (One-Time Costs): Revise and Deliver Initial Notification Training to Designated Personnel

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $35,750 | $2,073,500 | $2,073,500 | $2,073,500 | $150,758 | $95,264 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $35,750 | $71,500 | $71,500 | $71,500 | $4,766 | $2,524 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $35,750 | $35,750 | $35,750 | $35,750 | $2,397 | $1,296 |
| Sites with only reactors that currently are in decommissioning | $17,000 | $68,000 | $68,000 | $68,000 | $6,978 | $5,530 |
| **Total for all sites** | | **$2,248,750** | **$2,248,750** | **$2,248,750** | **$164,898** | **$104,614** |

## Table C-3. Industry Operation (Annual Costs): Make One-Hour Notifications (10 CFR 73.77(a)(1) and (c))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $625 | $36,250 | $498,575 | $789,010 | $36,250 | $36,250 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $625 | $1,250 | $18,754 | $35,414 | $1,250 | $1,250 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $625 | $625 | $9,322 | $17,236 | $625 | $625 |
| Sites with only reactors that currently are in decommissioning | $125 | $500 | $4,873 | $6,148 | $500 | $500 |
| **Total for all sites** | | **$38,625** | **$531,524** | **$847,808** | **$38,625** | **$38,625** |

## Table C-4. Industry Operation (Annual Costs): Make Four-Hour Notifications (10 CFR 73.77(a)(2) and (c))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $625 | $36,250 | $498,575 | $789,010 | $36,250 | $36,250 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $625 | $1,250 | $18,754 | $35,414 | $1,250 | $1,250 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $625 | $625 | $9,322 | $17,236 | $625 | $625 |
| Sites with only reactors that currently are in decommissioning | $125 | $500 | $4,873 | $6,148 | $500 | $500 |
| **Total for all sites** | | **$38,625** | **$531,524** | **$847,808** | **$38,625** | **$38,625** |

## Table C-5. Industry Operation (Annual Costs): Make Eight-Hour Notifications (10 CFR 73.77(a)(3) and (c))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $938 | $54,404 | $748,261 | $1,184,146 | $54,404 | $54,404 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $938 | $1,876 | $28,146 | $53,149 | $1,876 | $1,876 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $938 | $938 | $13,991 | $25,868 | $938 | $938 |
| Sites with only reactors that currently are in decommissioning | $219 | $876 | $8,537 | $10,771 | $876 | $876 |
| **Total for all sites** | | **$58,094** | **$798,936** | **$1,273,934** | **$58,094** | **$58,094** |

## Table C-6. Industry Operation (Annual Costs): Record Events in Site Corrective Action Program (10 CFR 73.77(b))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $1,875 | $108,750 | $1,495,725 | $2,367,030 | $108,750 | $108,750 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $1,875 | $3,750 | $56,263 | $106,241 | $3,750 | $3,750 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $1,875 | $1,875 | $27,967 | $51,708 | $1,875 | $1,875 |
| Sites with only reactors that currently are in decommissioning | $313 | $1,252 | $12,201 | $15,395 | $1,252 | $1,252 |
| **Total for all sites** | | **$115,627** | **$1,592,156** | **$2,540,374** | **$115,627** | **$115,627** |

## Table C-7. Industry Operation (Annual Costs): Prepare and Submit Written Security Follow-Up Reports (10 CFR 73.77(d))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $200,000 | $11,600,000 | $159,543,964 | $252,483,185 | $11,600,000 | $11,600,000 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $200,000 | $400,000 | $6,001,383 | $11,332,402 | $400,000 | $400,000 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $200,000 | $200,000 | $2,983,147 | $5,515,532 | $200,000 | $200,000 |
| Sites with only reactors that currently are in decommissioning | $45,000 | $180,000 | $1,754,184 | $2,213,293 | $180,000 | $180,000 |
| **Total for all sites** | | **$12,380,000** | **$170,282,679** | **$271,544,412** | **$12,380,000** | **$12,380,000** |

## Table C-8. Industry Operation (Annual Costs): Update and Deliver Recurring Notification Training to Designated Personnel (10 CFR 73.77)

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $10,500 | $609,000 | $8,376,058 | $13,255,367 | $609,000 | $609,000 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $10,500 | $21,000 | $315,073 | $594,951 | $21,000 | $21,000 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $10,500 | $10,500 | $156,615 | $289,565 | $10,500 | $10,500 |
| Sites with only reactors that currently are in decommissioning | $10,500 | $17,000 | $165,673 | $209,033 | $17,000 | $17,000 |
| **Total for all sites** | | **$657,500** | **$9,013,419** | **$14,348,917** | **$657,500** | **$657,500** |

## Table C-9. NRC Implementation (One-Time Costs): Perform Rulemaking Activities

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| All Sites | Not Applicable | $166,375 | $166,375 | $166,375 | $11,089 | $5,873 |
| **Total for all sites** | | **$166,375** | **$166,375** | **$166,375** | **$11,089** | **$5,873** |

## Table C-10. NRC Operation (Annual Costs): Respond to One-Hour Notifications (10 CFR 73.77(a)(1) and (c))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $3,025 | $175,450 | $2,413,102 | $3,818,808 | $175,450 | $175,450 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $3,025 | $6,050 | $90,771 | $171,403 | $6,050 | $6,050 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $3,025 | $3,025 | $45,120 | $83,422 | $3,025 | $3,025 |
| Sites with only reactors that currently are in decommissioning | $605 | $2,420 | $23,584 | $29,756 | $2,420 | $2,420 |
| **Total for all sites** | | **$186,945** | **$2,572,578** | **$4,103,390** | **$186,945** | **$186,945** |

## Table C-11. NRC Operation (Annual Costs): Respond to Four-Hour Notifications (10 CFR 73.77(a)(2) and (c))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $6,050 | $350,900 | $4,826,205 | $7,637,616 | $350,900 | $350,900 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $6,050 | $12,100 | $181,542 | $342,805 | $12,100 | $12,100 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $6,050 | $6,050 | $90,240 | $166,845 | $6,050 | $6,050 |
| Sites with only reactors that currently are in decommissioning | $1,210 | $4,840 | $47,168 | $59,513 | $4,840 | $4,840 |
| **Total for all sites** | | **$373,890** | **$5,145,155** | **$8,206,779** | **$373,890** | **$373,890** |

## Table C-12. NRC Operation (Annual Costs): Respond to Eight-Hour Notifications (10 CFR 73.77(a)(3) and (c))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $9,075 | $526,350 | $7,239,307 | $11,456,425 | $526,350 | $526,350 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $9,075 | $18,150 | $272,313 | $514,208 | $18,150 | $18,150 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $9,075 | $9,075 | $135,360 | $250,267 | $9,075 | $9,075 |
| Sites with only reactors that currently are in decommissioning | $2,118 | $8,472 | $82,564 | $104,172 | $8,472 | $8,472 |
| **Total for all sites** | | **$562,047** | **$7,729,544** | **$12,325,072** | **$562,047** | **$562,047** |

## Table C-13. NRC Operation (Annual Costs): Review Written Security Follow-Up Reports (10 CFR 73.77(d))

| Type of Site | Cost per Site | Cost for All Sites | For All Sites | | | |
|---|---|---|---|---|---|---|
| | | | Present Value 7% Discount Rate | Present Value 3% Discount Rate | Annualized Value 7% Discount Rate | Annualized Value 3% Discount Rate |
| Sites with only reactors that are currently in commercial operation | $2,420 | $140,360 | $1,930,482 | $3,055,047 | $140,360 | $140,360 |
| Sites with both operating reactors and projected new reactors under a Part 52 license | $2,420 | $4,840 | $72,617 | $137,122 | $4,840 | $4,840 |
| Sites with both operating reactors and reactors under active construction under a Part 50 license | $2,420 | $2,420 | $36,096 | $66,738 | $2,420 | $2,420 |
| Sites with only reactors that currently are in decommissioning | $545 | $2,180 | $21,245 | $26,805 | $2,180 | $2,180 |
| **Total for all sites** | | **$149,800** | **$2,060,440** | **$3,285,712** | **$149,800** | **$149,800** |