SUPPORTING STATEMENT FOR
"CYBER SECURITY EVENT NOTIFICATIONS"
FINAL RULE

10 CFR PART 73 AND NRC FORM 366

(3150-0002 and 3150-0104)

REVISION

Description of the Information Collection

The U.S.Nuclear Regulatory Commission (NRC) is amending Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73 to add new cyber security regulations that govern nuclear power reactor licensees under 10 CFR Parts 50 and 52. The NRC requires these additions because cyber security event notification requirements were not included in the NRC's final rule that added section 73.54, "Protection of Digital Computer and Communication Systems and Networks," 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 that shall provide high assurance that digital computers, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in section 73.1.

The cyber security event notification requirements were originally published for public comment as part of the "Proposed Rule: Enhanced Weapons, Firearms Background Checks and Security Event Notifications," (76 FR 6200) in February, 2011. In December 2013, the staff notified the Commission of its plan to bifurcate the cyber security event notifications requirements from the enhanced weapons rulemaking due to delays in completing the final enhanced weapons rule.

The final rule codifies the new requirements under section 73.77, "Cyber Security Event Notifications," and requires licensees subject to the provisions of section 73.54 to report certain cyber security events to the NRC within the timeliness requirements specified. Licensees are required to submit written security follow-up reports to the NRC on NRC Form 366, "Licensee Event Report," for certain notifications made under section 73.77.

The current submission includes the following changes from the proposed rule, made in response to public comments:

- In the proposed rule, under one-hour notifications, there were originally two notification requirements. One requirement reflected physical security notification rule language and one involved notification for "uncompensated" cyber security events. Based on public comments, the final rule was revised to require notification for events pertaining to adverse impacts to safety, security and emergency preparedness (SSEP) functions. This language aligns more closely with the existing 10 CFR 73.54, "Protection of digital computer and communication systems and networks."

- In the proposed rule, under four-hour notifications, there were originally two notification requirements pertaining to suspicious cyber security events. In the final rule, suspicious cyber security events were combined into one requirement and moved to eight-hour

notifications. In addition, a notification was added under four hours based on public comments pertaining to cyber attacks that could have caused an adverse impact to SSEP functions to align more closely with the existing 10 CFR 73.54, "Protection of digital computer and communication systems and networks."

- In the proposed rule, under eight-hour notifications there was one cyber security requirement pertaining to tampering or unauthorized access. Based on public comments, in the final rule this requirement was moved to four-hour notifications and clarified to capture attacks initiated by personnel with physical or electronic access (e.g., tampering, unauthorized access). In the final rule, the combined suspicious cyber security events was moved to eight-hour notifications and clarified as preoperational planning and intelligence gathering activities.

- In the final rule, twenty-four hour recordable events were revised based on public comments to be captured in the site corrective action program instead of a safeguards event log.

- The final 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 cyber security event notifications final rule will affect the following sites: 58 sites with currently operating reactors, two sites with projected new power reactors for which a combined license (COL) already has been issued under 10 CFR Part 52, one site with reactors under construction under a 10 CFR Part 50 license, and four sites with only reactors that currently are in decommissioning. This results in 65 affected power reactor sites.

A. JUSTIFICATION

1. Need for and Practical Utility of the Information

Notification of cyber security events 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. Reporting cyber-related activities and incidents also assists the NRC in meeting its obligations under the Department of Homeland Security (DHS), Nuclear Sector Annex to the National Cyber Incident Response Plan. Reporting certain 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.

The specific reporting and recordkeeping requirements being added under the cyber security event notifications final rule are identified below.
Section 73.77(a)(1) requires licensees subject to the provisions of 10 CFR 73.54 to make a telephonic notification of the cyber security events identified at 10 CFR 73.77(a)(1) to the NRC Headquarters Operations Center via the

Emergency Notification System within one hour after discovery. Notifications must be made according to 10 CFR 73.77(c).

Section 73.77(a)(2) requires licensees subject to the provisions of 10 CFR 73.54 to make a telephonic notification of the cyber security events identified at 10 CFR 73.77(a)(2)(i)-(iii) to the NRC Headquarters Operations Center via the Emergency Notification System within four hours after discovery. Notifications must be made according to 10 CFR 73.77(c).

Section 73.77(a)(3) requires licensees subject to the provisions of 10 CFR 73.54 to make a telephonic notification of the cyber security events identified at 10 CFR 73.77(a)(3) to the NRC Headquarters Operations Center via the Emergency Notification System within eight hours after discovery. Notifications must be made according to 10 CFR 73.77(c).

Section 73.77(b) requires licensees subject to the provisions of 10 CFR 73.54 to record cyber security events identified at 10 CFR 73.77(b) in the site corrective action program within twenty-four hours after discovery.

Sections 73.77(c)(1)-(4) describes the notification process. Burden for these notifications is captured under 73.77(a) (1) – (3).

Section 73.77(c)(5) requires licensees desiring to retract a previous cyber security event report that has been determined to not meet the threshold of a reportable event to telephonically notify the NRC Headquarters Operations Center and indicate the report being retracted and basis for the retraction.

Section 73.77(d) requires 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)(iii) to also submit a written security follow-up report to the NRC within 60 days of the telephonic notification using NRC Form 366, Licensee Event Report. 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) and (a)(3).

Under section 73.77(d)(12), licensees and also must maintain a copy of the written security follow-up report of an event submitted under section 73.77 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.

In addition to the above requirements, licensees are expected read the final rule and develop/revise procedures and train personnel. Licensees may use different approaches to update their procedures (e.g., updating an existing procedure [such as security event notification procedure] or developing a stand-alone procedure). The NRC has captured the burden associated with implementation as a one-time recordkeeping burden on Table 1.

2. Agency Use of the Information

The information received during a cyber security event notification will be reviewed by the NRC staff to determine appropriate response actions. These actions may include one or more of the following actions: (1) notifying the 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 reports provided by licensees to effectively monitor ongoing licensee actions and inform other licensees in a timely manner of cyber security-significant events.

3. Reduction of Burden through Information Technology

There are no legal obstacles to reducing the burden associated with this information collection. The NRC encourages respondents to use information technology when it would be beneficial to them. The NRC issued a regulation on October 10, 2003 (68 *FR* 58791), consistent with the Government Paperwork Elimination Act, which allows its licensees, vendors, applicants, and members of the public the option to make submissions electronically via CD-ROM, e-mail, special Web-based interface, or other means. It is estimated that 50 percent of the potential responses from section 73.77 will be filed electronically.

4. Effort to Identify Duplication and Use Similar Information

No sources of similar information are available. Cyber security event notification records maintained by licensees are not available from any other Federal agency or department, and would not be available from any other source.

There is no duplication of requirements. The NRC has in place an on-going program to examine all information collections with the goal of eliminating all duplication and/or unnecessary information collections.

In addition, the final rule incorporates provisions to avoid duplication. Sections 73.77(a)(2)(iii) specifically eliminate the need for licensees to submit duplicate notifications reportable in accordance with section 73.77(a). Section 73.77(c)(7) eliminates the need for licensees to submit separate notifications and reports for cyber security events that also are reportable in accordance with sections 50.72 and 50.73. However, these notifications also should indicate the applicable section 73.77 reporting criteria.

5. Effort to Reduce Small Business Burden

The NRC has determined that the companies that own the sites affected by the final rule 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).

6. Consequences to Federal Program or Policy Activities if the Collection is Not Conducted or is Conducted Less Frequently

The NRC has a strategic mission to immediately communicate threats or attack information, which also includes the immediate communication of threat or attack information to other NRC licensees so that they can increase the security posture at their facilities. Without the new cyber security event notification requirements in section 73.77, the NRC would not be notified as quickly about a cyber attack or threat so the communication to other affected licensees and the National Response Framework would be delayed.

7. Circumstances Which Justify Variation from OMB Guidelines

Certain requirements in section 73.77 vary from the Office of Management and Budget (OMB) Guidelines in 5 CFR 1320.5(d)(2) by requiring that licensees make telephonic notifications of cyber security events to the NRC more often than quarterly. Sections 73.77(a)(1) – (3) require that licensees make a telephonic notification of certain cyber security events to the NRC within one, four, or eight hours after discovery. These notification requirements are needed to allow response forces, the NRC Headquarters Operations Center staff, and law enforcement authorities to determine whether an actual or imminent threat against NRC licensed facilities exists.

8. Consultations Outside the NRC

On February 3, 2011, the NRC published the proposed regulations that would implement the new cyber security event notification requirements as part of a larger proposed rule entitled "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications" (76 *FR* 6200). The public comment period closed on August 4, 2011.

The NRC received a total of 14 submittals relating to enhanced weapons, firearms background checks, and security event notifications (which included cyber security event notifications) on the proposed rule and draft guidance document. From the 14 submittals received, 26 comments (from four separate commenters) from the proposed rule specific to cyber security event notifications were bifurcated and addressed in this final rulemaking. In addition, certain event notifications that were applicable to both cyber security events and physical security events (e.g., suspicious events) were bifurcated and addressed in this final rulemaking as well. The following are the comments and the NRC responses from the proposed rule specific to cyber security event notifications:
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, therefore eliminating the four-hour notification events. One commenter specifically recommended that suspicious events be moved from four-hour to eight-hour notifications. [NEI-17, 161, Hardin-2]

Response: The NRC agrees in part, with this comment. The NRC agrees that suspicious cyber security events (i.e., activities that may indicate intelligence gathering or pre-operational planning related to a cyber attack) should be moved from four-hour notifications to eight-hour notifications. However, notifications with a local, State, or other Federal agency is consistent with existing NRC regulations at 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 have been clarified to address suspected or actual cyber attacks initiated by personnel with physical or electronic access and were moved in the final rule to four-hour notifications due to the implications of an internal threat. Accordingly, the NRC has revised the rule language and associated guidance consistent with this approach to address the broader recommendation of aligning more closely with 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 of 10 CFR part 73 regarding the recording of events in a safeguards event log. The commenter suggested licensees use the corrective action program instead of using a separate log. [NEI-18, 194, 202]

Response: The NRC agrees with this comment. The cyber security plan for each licensee describes the use of the corrective action program to track, trend, correct, and prevent recurrence of cyber security failures and deficiencies.

Therefore, the cyber security event notification rule text (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. Regulatory Guide 5.83 has also been revised to reflect this change.

Comment 6: The NRC received a comment regarding the use of the term "compensatory" in the context of cyber security, stating that the term is unclear, and is not defined in the two cyber security plan (CSP) templates, Appendix A of RG 5.71, and Appendix A of NEI 08-09. [NEI-153, 165]

Response: The NRC agrees with this comment. The term "compensatory" is not defined in either CSP template or in other NRC guidance related to cyber security. Based on public comments, the NRC has developed a different approach for determining cyber security event notifications, one that is based on whether the cyber attack caused an adverse impact (or not) to SSEP functions. The final rule and RG 5.83 have been revised to reflect this new approach.

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

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

Comment 8: One commenter proposed changes to the rule language, paragraph I.(h)(1) of appendix G I of 10 CFR part 73, adding the terms "credible", "malicious" and "radiological sabotage" to add clarity. The commenter recommended rewriting the event to add in part, "a credible threat to commit or cause a malicious act to modify, destroy, or compromise any systems, networks, or equipment that falls within the scope of 10 CFR 73.54 of this part where a compromise of these systems has resulted or could result in radiological sabotage." [NEI-157, 206]

Response: The NRC disagrees with this comment. Based on public comments, the NRC developed a different approach for determining cyber security event notifications, one that is based on whether a cyber attack caused an adverse impact (or not) to SSEP functions. This approach aligns more closely with § 73.54 and the terms "credible," "malicious," and "radiological sabotage" are not needed to provide clarity under this approach. Regulatory Guide 5.83 has been revised to reflect this new approach.

Comment 9: One commenter proposed revising the proposed rule language in paragraph I.(h)(2) in appendix G I of 10 CFR part 73 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. Regulatory Guide 5.83 has been revised to reflect this approach.

Comment 10: One commenter proposed language to paragraph I.(c)(1) in appendix G of 10 CFR part 73 to report only instances of suspicious or surveillance activity or attempts to access systems, networks, or equipment that is within the scope of 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 paragraph I.(c)(1) in appendix of 10 CFR part 73 appears to be misquoted. The changes proposed by the commenter would amend paragraph II.(c)(1) in appendix G. The NRC believes that surveillance activities are captured within activities that indicate intelligence gathering or pre-operational planning and should be reported, and has made appropriate changes to this final rule. The NRC has clarified and relocated this requirement to the eight-hour notifications, now designated as 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 paragraph I.(c)(2) in appendix G of 10 CFR part 73 in the proposed rule text should be completely removed because it duplicates other proposed rule text. [NEI-160]

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

Comment 12: One commenter proposed changes to paragraph III in appendix G of 10 CFR part 73 to clarify the language under eight-hour reportable events to be consistent with 10 CFR 73.54(c)(1), which implements security controls to protect CDAs and critical systems from cyber attacks. [NEI-162]

Response: The NRC agrees in part, with this comment. Based on public comments, the NRC developed an approach that aligns more closely with 10 CFR 73.54. The implementation of security controls to protect CDAs from

cyber attacks as described in 10 CFR 73.54(c)(1) is designed to prevent adverse impacts to SSEP functions. Therefore, in the final rule, a cyber attack that adversely impacted SSEP functions requires notification within one hour after discovery, and cyber attacks that could have caused an adverse impact to SSEP functions requires notification within four hours after discovery due to the potential consequences of these events. Regulatory Guide 5.83 has been revised to reflect this new approach.

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

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

The commenter stated that this re-worded provision would better align with another proposed provision in paragraph I.(h)(2) in appendix G of 10 CFR part 73. [NEI-163]

Response: The NRC disagrees with this comment. Adding the words, "that would" to the rule text changes the context of the type of events that are required to be recorded. However, based on other public comments, the NRC re-evaluated the 24-hour recordable events for cyber security event notifications and developed an approach that aligns more closely with the CSP requirements. Under this approach, as reflected in the new 10 CFR 73.77(b)(1) provision being added as part of this final rule, licensees will be required to use their corrective action program to record vulnerabilities, weaknesses, failures, and deficiencies in their cyber security program within twenty-four hours of their discovery. Regulatory Guide 5.83 has been updated to reflect this change.

Comment 14: One commenter recommended revising the proposed rule language to align exactly with the rule language in 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 paragraph II.(c)(2) in appendix G of 10 CFR part 73 because the commenter believes it is duplicated in paragraph I.(h)(2) in appendix G. [NEI-169]

Response: The NRC agrees that the proposed paragraph II.(c)(2) in appendix G of 10 CFR part 73 is similar to paragraph I.(h)(2) in appendix G.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. Regulatory Guide 5.83 has been revised to reflect this new approach.

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

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

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

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

Comment 18: One commenter recommended clarification on cyber security event notification requirements regarding exclusion of licensees not subject to 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-31, 48]

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

Comment 21: One commenter recommended clarifying requirements regarding law enforcement interactions. The commenter recommended that notifications that could result in public or media inquiries should not duplicate notifications made under other NRC regulations such as 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. Regulatory Guide 5.83 has been revised to reflect this change.

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

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

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

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

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

Response: The NRC agrees with this comment. The final rule reflects an approach that aligns more closely with 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). Regulatory Guide 5.83 has also been revised to reflect this new approach.

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

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

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

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

9. Payment or Gift to Respondents

Not applicable.

10. Confidentiality of Information

Certain information is designated as Classified National Security Information or as Safeguards Information. Classified National Security Information is prohibited

from disclosure in accordance with Executive Order 12958. The NRC's regulations in 10 CFR Part 95 address the protection of Classified National Security Information.

Safeguards Information is prohibited from disclosure under Section 147 of the Atomic Energy Act of 1954, as amended (AEA). The NRC's regulations in 10 CFR 73.21 and 73.22 address the protection of Safeguards Information.

Confidential and proprietary information is protected in accordance with NRC regulations in 10 CFR 9.17(a) and 10 CFR 2.390(b).

11. Justification for Sensitive Questions

Not applicable.

12. Estimate of Industry Burden and Cost

The reporting and recordkeeping burden associated with the cyber security event notification requirements are given in Tables 1-8. There is no 3rd party annual reporting burden under the final rule.

Based on the NRC staff's best estimate, the incremental industry burden to comply with the cyber security event notification requirements of the final rule is estimated to total 15,919.98 hours at an annualized cost of $4,441,675 (15,919.98 hours x $279/hr[1]). Of this burden, 8,551.98 hours are associated with the implementation of the rule and ongoing requirements under 10 CFR Part 73 (OMB clearance number 3150-0002), while 7,368 hours are associated with reporting and recordkeeping on NRC Form 366, "Licensee Event Report" to report cyber security events under 73.77(d) (OMB clearance number 3150-0104). The burden estimate for reporting cyber security events on NRC Form 366 is 80 hours (64 hours reporting plus 16 hours recordkeeping), which is consistent with other events reported on NRC Form 366.

Total Cyber Event Notification Final Rule Burden

	Responses	Hours	Cost @$279/hr
Reporting	338.70	6033.05	$1,683,221
Recordkeeping (One-time and Annual)	65.00	9886.93	$2,758,454
TOTAL	403.70	15919.98	$4,441,675

13. Estimate of Other Additional Costs

The NRC has determined that the quantity of records to be maintained is roughly proportional to the recordkeeping burden and, therefore, can be used to calculate approximate records storage costs. Based on the number of pages maintained for a typical clearance, the records storage cost has been determined to be equal to 0.0004 x the recordkeeping burden cost. Therefore, the incremental records

1 10 CFR 170.20, "Average cost per professional staff-hour." Available online at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part170/part170-0020.html, last accessed on July 18,2014.

storage cost for the cyber security event notification records is estimated to be $1,104 (0.0004 x 9,886.9 recordkeeping hours x $279 per hour[2]). Of this, $164 is associated with NRC Form 366 (.0004 x 1,473.6 hrs x $279/hr) and $939 is associated with Part 73 (.0004 x 8,413.3 hours x $279/hr).

14. Estimated Annualized Cost to Federal Government

Based on the NRC staff's best estimate, the estimated annual burden to the NRC under the final rule is estimated to total 1,876 hours (458 hours for one-time implementation activities and 1,418 hours for annual activities), with an annualized cost estimate to the NRC of $523,404 (1,876 hours x $279 per hour[3]). The cost is fully recovered through fee assessments to NRC licensees pursuant to 10 CFR Parts 170 and/or 171.

NRC Action	Annualized Burden Hours	Cost at $279/hr
One-Time Implementation Activities		
Develop final rule and regulatory guide	458	$127,782
Subtotal	*458*	*$127,782*
Annual Activities		
Respond to telephonic notifications made under sections 73.77(a)(1), (a)(2), and (a)(3)	1,233	$344,007
Review written follow-up reports submitted under section 73.77(d)	185	$51,615
Subtotal	*1,418*	*$395,622*
Total	**1,876**	**$523,404**

15. Reasons for Change in Burden or Cost

The estimated incremental burden of the final rule is 15,919.9 hours. This estimate is composed of one-time and annual requirements of the final rule.

The increase in burden is associated with the addition of new cyber security event notification requirements to Part 73, which require licensees subject to the provisions of section 73.54 to: (1) report certain cyber security events to the NRC within the timeliness requirements specified; (2) use their site corrective action program to record information on cyber security events; and (3) submit written security follow-up reports to the NRC for certain notifications made under section 73.77.

2 10 CFR 170.20, "Average cost per professional staff-hour." Available online at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part170/part170-0020.html, last accessed on July 18,2014.

3 10 CFR 170.20, "Average cost per professional staff-hour." Available online at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part170/part170-0020.html, last accessed on July 18,2014.

16. Publication for Statistical Use

This information will not be published for statistical use.

17. Reason for Not Displaying the Expiration Date

The expiration date is displayed on NRC Form 366, “Licensee Event Report.”

The remaining recordkeeping and reporting requirements for this information collection are associated with regulations and are not submitted on instruments such as forms or surveys. For this reason, there are no data instruments on which to display an OMB expiration date. Further, amending the regulatory text of the CFR to display information that, in an annual publication, could become obsolete would be unduly burdensome and too difficult to keep current.

18. Exceptions to the Certification Statement

There are no exceptions.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

Statistical methods are not used in this collection of information.

BURDEN ESTIMATES FOR PART 73 (3150-0002)

TABLE 1
ONE-TIME IMPLEMENTATION RECORDKEEPING BURDEN FOR PART 73[a]

Section	No. of Respondents	Responses per Respondent	Number of Responses	Burden Hours per Response	Total Burden Hours
73.77	65	1	65	374	24,310.00
TOTAL			65		24,310.00
ANNUALIZED TOTAL			**21.67**		**8103.33**

TABLE 2
ANNUAL RECORDKEEPING BURDEN FOR PART 73

Section	No. of Recordkeepers	Burden Hours per Recordkeeper	Total Burden Hours
73.77(d)	65	4.77	310.00
TOTAL			**310.00**

TABLE 3
ANNUAL REPORTING BURDEN FOR PART 73

Section	No. of Respondents	Responses per Respondent	Number of Responses	Burden Hours per Response	Total Annual Burden Hours
73.77(a)(1)	65	0.47	30.7	1	30.7
73.77(a)(2)	65	0.94	61.4	0.5	30.7
73.77(a)(3)	65	2.38	154.5	0.5	77.25
73.77(e)(1)-(4)	Burden covered under sections 73.77(a), (b), and (c)				
73.77(e)(5)	Burden covered under sections 73.77(a), (b), and (c)				
TOTAL			**246.6**		**138.65**

TABLE 4
TOTAL BURDEN FOR PART 73

	Responses	Hours	Cost @$279/hr
One-Time Recordkeeping	21.67	8103.33	$2,260,830
Annual Reporting	246.6	138.65	$38,683
Annual Recordkeeping	65	310.00	$86,490
TOTAL	311.60	8551.98	$2,386,003

(all one-time recordkeepers are also annual recordkeepers, therefore, the 65 recordkeepers are each only counted once)

BURDEN ESTIMATES FOR NRC FORM 366 (3150-0104)[4]

TABLE 5
ANNUAL REPORTING BURDEN FOR NRC FORM 366 [a]

Section	No. of Respondents	Responses per Respondent	Number of Responses	Burden Hours per Response	Total Annual Burden Hours
73.77(d)	65	1.42	92.10	64	5894.40
TOTAL			**92.10**		**5894.40**

TABLE 6
ANNUAL RECORDKEEPING BURDEN FOR NRC FORM 366 [a]

Section	No. of Respondents	Responses per Respondent	Number of Responses	Burden Hours per Recordkeeper	Total Burden Hours
73.77(d) (12)	65	1.42	92.10	16	1473.6
TOTAL					1473.6

TABLE 7
TOTAL BURDEN FOR NRC FORM 366

	Responses	Hours	Cost @$279/hr
Annual Reporting	92.10	5894.40	$1,644,538
Annual Recordkeeping	65	1473.6	$411,134
TOTAL	157.10	7368.00	$2,055,672

[a] NOTE: The number of responses per respondent and burden hours per recordkeeper was calculated based on the estimated number of responses and respondents or burden hours, resulting in apparent rounding errors.

4 NOTE: Burden reporting on NRC Form 366 was included in Part 73 (3150-0002) totals when the proposed rules was submitted to OMB in 2011. For the final rule, the NRC staff have broken out the hours separately for reporting and recordkeeping associated with NRC Form 366 (3150-0104).

TABLE 8
TOTAL BURDEN FOR CYBER EVENT NOTIFICATION FINAL RULE

	Responses	Hours	Cost @$279/hr
Reporting	338.70	6033.05	$1,683,221
Recordkeeping (One-time and Annual)	65.00	9886.93	$2,758,454
TOTAL	403.70	15919.98	$4,441,675

Respondents: 65 (58 sites with currently operating reactors, 2 sites with projected new power reactors for which a combined license (COL) already has been issued under 10 CFR Part 52, 1 site with reactors under construction under a 10 CFR Part 50 license, and 4 sites with only reactors that currently are in decommissioning).