SUPPORTING STATEMENT FOR
10 CFR PART 73
"CYBER SECURITY EVENT NOTIFICATIONS"
FINAL RULE

(3150-0002 and 3150-0104)

REVISION

Description of the Information Collection

The U. S. Nuclear Regulatory Commission (NRC) is amending 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. Based on public comment, the NRC has revised the final rule to require licensees to record cyber security events in their site corrective action program, rather than recording them in a safeguards event log as specified in the proposed rule. Finally, 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 cyber security event notifications final rule will affect the following sites: 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. 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 The U.S. Nuclear Regulatory Commission (NRC) management. Reporting cyber-related suspicious 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 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.

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 of 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 of 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 of discovery. Notifications must be made according to 10 CFR 73.77(c).

Section 73.77(b) requires licensees to use the site corrective action program to record vulnerabilities, weaknesses, failures and deficiencies in their 10 CFR 73.54 cyber security program (section 73.77(b)(1)). Licensees and also must use the site corrective action program to record notifications made under sections 73.77(a)(1) - (3) (section 73.77(b)(2)).

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 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)(ii) 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. 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 the Office of Management and Budget 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 of 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.

Section 73.77(d) also varies from the OMB Guidelines in 5 CFR 1320.5(d)(2) by requiring that licensees retain records for more than three years. These records are required for inspection or for reconstruction of events in the event of a safeguards incident.

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). From the 14 submittals received, 6 comments 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:

Comment 1: 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.

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 safety, security, and emergency preparedness 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 2: 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.

Response: The NRC agrees with this comment. The cyber security plan for each licensee describes the use of the corrective action program to record 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 3: One commenter recommended four and eight-hour notifications be consolidated into "within 24-hours" to mitigate event reporting violations.

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 4: 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).

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 notifications.

Comment 5: One commenter recommended deleting the requirements and guidance for written follow-up reports on several reporting events (four and eight-hour notifications).

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 6: One commenter recommended that the final rule require licensees to notify their local Federal Bureau of Investigations (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.

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. 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 8,952.88 hours at an annualized cost of $2,435,185 (8,952.88 hours x $272/hr[1]). Of this burden, 8,551.98 hours is associated with the implementation of the rule and ongoing requirements

[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.

under 10 CFR Part 73, while 400.9 hours is associated with reporting and recordkeeping on NRC Form 366, "Licensee Event Report" to report cyber security events under 73.77(d). The burden estimate for reporting cyber security events on NRC Form 366 is 4 hours reporting and 0.5 hours recordkeeping, or 4.5 hours total.[2]

Total Cyber Event Notification Final Rule Burden

	Responses	Hours	Cost @$272/hr
Reporting	403.70	507.05	$137,918
Recordkeeping (One-time and Annual)	65.00	8,445.83	$2,297,267
TOTAL	**468.70**	**8,952.88**	**$2,435,185**

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 storage cost for the cyber security event notification records is estimated to be $919 (0.0004 x 8,446 recordkeeping hours x $272 per hour[3]).

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 $510,272 (1,876 hours x $272 per hour[4]). The cost is fully recovered through fee assessments to NRC licensees pursuant to 10 CFR Parts 170 and/or 171.

[2] Cyber security events are estimated to required 4 hours to report and 0.5 hours for recordkeeping, compared to other events reported on NRC Form 366, which are estimated to take 64 hours to report and 16 hours for recordkeeping. Cyber security events are estimated to take significantly less time because they will not require the types of complex engineering analysis that may be required for other types of reportable events at operating power reactors.

[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.

[4] 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.

NRC Action	Annualized Burden Hours	Cost
One-Time Implementation Activities		
Develop final rule and regulatory guide	458	$124,576
Subtotal	*458*	*$124,576*
Annual Activities		
Respond to telephonic notifications made under sections 73.77(a)(1), (a)(2), and (a)(3)	1,233	$335,376
Review written follow-up reports submitted under section 73.77(d)	185	$50,320
Subtotal	*1,418*	*$385,696*
Total	**1,876**	**$510,272**

15. Reasons for Change in Burden or Cost

The estimated incremental burden of the final rule is 8,952.88 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.

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.

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	1.00	65.00	374.0	24,310.00
TOTAL			65.00		24,310.00
ANNUALIZED TOTAL			**22.00**		**8,103.00**

TABLE 2
ANNUAL REPORTING BURDEN FOR PART 73 [a]

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	30.70	1.0	30.70
73.77(a)(2)	65	0.94	61.40	0.5	30.70
73.77(a)(3)	65	2.38	154.50	0.5	77.25
73.77(c)(1)-(4)	Burden covered under sections 73.77(a)(1), (a)(2), and (a)(3)				
73.77(c)(5)	Burden covered under sections 73.77(a)(1), (a)(2), and (a)(3)				
TOTAL			**311.60**		**138.65**

TABLE 3
ANNUAL RECORDKEEPING BURDEN FOR PART 73 [a]

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

TABLE 4
TOTAL BURDEN FOR PART 73

	Responses	Hours	Cost @$272/hr
One-Time Recordkeeping	--	8,103.33	$2,204,107
Annual Reporting	311.60	138.65	$37,713
Annual Recordkeeping	65.00	310.00	$84,320
TOTAL	**376.60**	**8,551.98**	**$2,326,139**

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	4.0	368.40
TOTAL			**92.10**		**368.40**

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

Section	No. of Recordkeepers	Burden Hours per Recordkeeper	Total Burden Hours
73.77(d)(12)	65	0.50	32.5
TOTAL			**32.5**

TABLE 7
TOTAL BURDEN FOR NRC FORM 366

	Responses	Hours	Cost @$272/hr
Annual Reporting	92.10	368.40	$100,205
Annual Recordkeeping	65.00	32.50	$8,840
TOTAL	**157.10**	**400.90**	**$109,045**

[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.

TABLE 8
TOTAL BURDEN FOR CYBER EVENT NOTIFICATION FINAL RULE

	Responses	Hours	Cost @$272/hr
One-Time Recordkeeping[5]	--	8,103.33	$2,204,107
Annual Reporting	403.70	507.05	$137,918
Annual Recordkeeping	65.00	342.50	$93,160
TOTAL	**468.70**	**8,952.88**	**$2,435,185**

Respondents: 65 (58 sites with currently operating reactors, 2 sites with projected new power reactors for which a 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).

[5] This rule affects a total of 65 recordkeepers. Each recordkeeper has been counted one time in the total number of responses.