



NUCLEAR ENERGY INSTITUTE

5/26/2010

75 FR 29588

1

Christopher E. Earls  
DIRECTOR  
SECURITY  
NUCLEAR GENERATION DIVISION

June 28, 2010

Ms. Cynthia K. Bladey  
Acting Chief  
Rulemaking and Directives Branch  
Office of Administration  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

RECEIVED

2010 JUN 28 PM 4:59

RULES AND DIRECTIVES  
BRANCH  
USNRC

**Subject:** NEI Comments on NRC Proposed NUREG-0800; Standard Review Plan Section 13.6.6, Draft Revision 0 on "Cyber Security Plan," *Federal Register (FR Vol. 75, No. 101)*, Docket ID NRC-2010-0184

**Project Number: 689**

Dear Ms. Bladey:

This cover letter and the attached comments on NRC Docket ID NRC-2010-0184 are being submitted by the Nuclear Energy Institute (NEI)<sup>1</sup> on behalf of the nuclear power industry. NEI appreciates the opportunity to comment on the NRC Proposed NUREG-0800; Standard Review Plan Section 13.6.6, Draft Revision 0 on "Cyber Security Plan." We trust you will find these comments useful as you work to finalize the proposed guidance.

The detailed comments in the attachment to this letter represent a substantive review of the proposed Standard Review Plan (SRP) and were developed by NEI in collaboration with nuclear industry stakeholders.

<sup>1</sup> NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, nuclear material licensees, and other organizations and individuals involved in the nuclear energy industry.

SUNSI Review Complete  
Template = ADM-013

E-REDS = ADM-03  
Add = B. Subbaratnam (RXS2)

The following overview highlights the particular aspects of NEI's comments that we wish to emphasize:

- For consistency sake, the Staff might consider the viability of following the format of SRP 13.6.1, "Physical Security-Combined License."
- As the NRC has, at present, two approved cyber security plan templates, the Staff is urged to consider caveat language in the "Acceptance Criteria" similar to the language on SRP page 13.6.1-3. For example, the following text may be added, "The security plan is considered acceptable if it conforms to Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," the most recent NRC-approved NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," or any other NRC approved set of guidelines."
- Neither RG 5.71 nor the proposed draft SRP provides guidance on the implementation schedule that, according to the requirements of 10 CFR 73.54, must be submitted for NRC review and approval. The staff should consider the viability of providing such guidance.

NEI welcomes the opportunity to coordinate a meeting between NRC and industry representatives to discuss the SRP. The topics for the meeting might include:

- The path forward for the SRP;
- Expectations for the format and content of the implementation schedule; and
- The method the NRC staff will use to review cyber security plans submitted by operating reactors to meet the requirements of 10 CFR 73.54. As 10 CFR 50.34(h) requires the use of an SRP in effect six months prior to the date of application, NEI recommends the staff review be limited to bracketed text if submitted plans conform to an NRC approved template.

NEI's detailed comments are presented in the following attachment:  
Attachment – NEI Comments on Draft NUREG–0654, Supplement 3

We would like to thank the NRC in advance for its careful consideration of the comments and concerns outlined in this letter and our detailed comments provided in the attachment.

If you have any questions, please contact William Gross at (202) 739-8123; [wrg@nei.org](mailto:wrg@nei.org).

Sincerely,



Christopher E. Earls

c: NRC Document Control Desk

Attachment

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
13.6.6-01	I	SRP 13.6.6 incorrectly defines "defense-in-depth" as D3. Numerous other NRC documents and general industry practice is that D3 means "diversity and defense-in-depth."	Delete D3 throughout the SRP (Pages 1, 2,17 and others)
13.6.6-01-05	I, II	Sections I and II do not reflect the fact that 73.54 requires the submittal of a proposed implementation schedule along with the proposed cyber security plan. The first mention of the implementation schedule is in Section III.  These sections do not mention the staff's December 14, 2009 letter to NEI which provided staff guidance for these implementation schedules.	SRP 13.6.6 should be revised to describe the background and acceptance criteria for the proposed implementation schedule that is required to be submitted by licensees.
13.6.6-03	I	<u>Operational Program Description and Implementation</u> This section should not be applicable to operating plant licensees.	This section should clearly state that this review is not necessary for cyber security plans submitted by licensees.
13.6.6-03	I	<u>Review Interfaces</u> This section should not be applicable to operating plant licensees. Licensees have approved physical security plans and operational programs	This section should clearly state that this review is not necessary for cyber security plans submitted by licensees.
13.6.6-04	Acceptable Criteria	The SRP states that "The security plan is considered acceptable if it conforms to Regulatory Guide (RG) 5.71, 'Cyber Security Programs for Nuclear Facilities.'" The NRC has also approved NEI 08-09 as an acceptable guideline, so it (or any other NRC approved document) should be included with RG 5.71.	The security plan is considered acceptable if it conforms to Regulatory Guide (RG) 5.71 "Cyber Security Programs for Nuclear Facilities," the most recent NRC-approved NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors", or any other NRC approved set of guidelines."

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
			<p>-----</p> <p>Section III, Review Procedures should be modified. A new sentence should be added:</p> <p>If an applicant commits to a template approved by the NRC, the NRC review should be limited to validating that the application conforms to the approved template. Additional technical reviews should only occur if the applicant has departed from the approved text. In such case, the review should be limited to the proposed departure.</p> <p>-----</p> <p>Additionally, Table 1 should be modified by inserting a new row:</p> <p>The "Requirement" column should state: 10 CFR 73.54.</p> <p>The "Acceptance Criteria" column should note: NRC approved CSP template.</p> <p>It should also note that the NRC review should stop in this step if the plan fully conforms to the approved template.</p>
13.6.6-04	II.3	2 <sup>nd</sup> sentence – "Applicants' physical security plans should address the other cyber requirements found in 10 CFR 73.55, Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." – This sentence does not pertain to 10 CFR	<ul style="list-style-type: none"> <li>• Delete sentence</li> </ul>

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan

Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
		73.55(m)(2) [effectiveness reviews]	
13.6.6-04	II.4.B	Incomplete quote of regulation which expands requirements	<ul style="list-style-type: none"> <li>Should read "...or vital area for which compensatory measures have not been employed."</li> </ul>
13.6.6-05	II.5	Expectations regarding content of cyber security plan in implementing 10 CFR 73.58 are unclear. Reg Guide 5.71, which the SRP states is acceptable, has no reference to §73.58.	<ul style="list-style-type: none"> <li>Reg Guide 5.71 and SRP should be revised to conform with each other. NRC expectations on location of implementation details for §73.58 should be described in SRP. Since §73.58 deals with multiple security plans and non-security processes, it should be acceptable for implementation to be described in the FSAR, rather than the Cyber Security Plan itself. SRP acceptance criteria should specifically state what is required to be in Cyber Security Plan.</li> </ul>
13.6.6-05	II	<u>Operational Programs</u> As stated, this statement applies to COL reviews. It does not mention anything about review of licensee submitted plans.	This section should clearly state that this review is not necessary for cyber security plans submitted by licensees.
13.6.6-05	II	<u>Technical Rationale</u> Item 2 incorrectly cites 10 CFR 73.55 as codifying the cyber security requirements for NRC licensed power reactors. The correct citations is 10 CFR 73.54.	Revise the SRP to refer to 10 CFR 73.54.
13.6.6-06-35	III	The overall process to review Cyber Security Plans submitted by licensees versus applicants would appear to be substantially different. There are some sections of the SRP which appear to have been initially written for COL applicants but may be interpreted to apply also to operating plant licensees.	Section III, Table 1 should be revised such that the Acceptance Criteria column references the specific sections of RG 5.71, Appendix and NEI 08-09, Revision 6. The sections in these templates have already been approved by the NRC and thus need not be reviewed again.

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
		<p>Of concern is whether this can realistically be accomplished with a single SRP 13.6.6 or whether there needs to be two separate but similar processes.</p>	
13.6.6-06-35	III	<p>The overall review process described in Section III of the SRP is excessive and unnecessary given the existence of two NRC approved cyber security plan templates that most, if not all, licensees and applicants will be using to comply with 10 CFR 73.54.</p> <p>As background, NRC by letter date May 5, 2010, approved the use of NEI 08-09, Revision 6, the staff concluded that "submission of a cyber security plan using the template provided in NEI 08-09, Rev. 6 dated April 2010, would be acceptable for use by licensees to comply with the requirements of 10 CFR 73.54 with the exception of the definition of "cyber attack."</p> <p>Similarly, the NRC states in RG 5.71 that "Appendix A to RG 5.71 provides a template for a generic cyber security plan which licensees and applicants may use to comply with the licensing requirements of 10 CFR 73.54."</p> <p>In both cases, the use of NRC approved cyber security plan templates by licensee and applicants is intended to simplify and expedite the NRC review and approval process of the submitted cyber security plans. The review procedures provided in Section III are a re-review of material and text that have already been approved by the staff.</p> <p>The NRC review and acceptance criteria in Section III of</p>	<p>Revise SRP 13.6.6 to use the review process as conceived in SRP 13.6.1, Section III, which states in part:</p> <p>These review procedures are based on the identified SRP acceptance criteria. For deviations from these acceptance criteria, the staff should review the applicant's evaluation of how the proposed alternatives provide an acceptable method of complying with the relevant NRC requirements identified in Subsection II.</p> <ol style="list-style-type: none"> <li>1. Determine if the Security Plan conforms with the most recent NRC-endorsed revision of the generic security plan, NEI 03-12 (template), regulations, the information requirements of subsection I above, and the acceptance criteria of subsection II above.</li> </ol> <p>Thus, rather than referring to the Security plan and NEI 03-12, SRP 13.6.6 would refer to the Cyber Security Plan and RG 5.71 and NEI 08-09 Revision 6.</p> <p>Determine if the Cyber Security Plan conforms with the most recent NRC-endorsed revision of the generic cyber security plan, NEI 08-09, Revision 6 or RG 5.71 (templates).</p>

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
		<p>the SRP should be focused on the bracketed text within each template and any deviations that the licensee or applicant may take to the template in its own cyber security plan.</p> <p>Bracketed text is text that must be completed by the license or applicant. In RG 5.71, bracketed text is primarily the choice between 'licensee' and 'applicant'. In NEI 08-09, this bracketed text is provided along with bracketed text for the "defensive strategy."</p> <p>As written, SRP 13.6.6 Section III unnecessarily requires a review of all sections of the RG 5.71 based cyber security plan when the content of the plan has already been established by the approved RG 5.71 template.</p> <p>Given the two NRC approved templates, the reviews of the as written Section III would only be necessary if a cyber security plan was submitted that was not based on either approved template.</p> <p>Clearly, Section III does not apply to cyber security plan submitted using the NRC approved plan template contained in NEI 08-09, Revision 6.</p>	<p>Section III of SRP 13.6.6 needs to be revised to focus the staff cyber security plan review on:</p> <ol style="list-style-type: none"> <li>1. Bracketed text from RG 5.71 and NEI 08-09, Rev 6</li> <li>2. Deviations from the approved templates, if any, that may be proposed and justified by either the applicant or licensee</li> </ol>
13.6.6-06	III	<p>SRP 13.6.6 does not acknowledge the NRC approved template contained in NEI 08-09, Rev 6. By letter dated May 5, 2010, NRC approved its use by licensee and applicants. The format of NEI 08-09 and level of detail is significantly different than contained in RG 5.71. Accordingly, the use of SRP 13.6.6 as written would be an inappropriate review process for cyber security plans</p>	<p>SRP 13.6.6 needs to be revised to focus the staff cyber security plan review on:</p> <ol style="list-style-type: none"> <li>1. Bracketed text from RG 5.71 and NEI 08-09, Rev 6, and</li> <li>2. Deviations from the approved templates, if any, that may be proposed and justified by either the applicant or licensee</li> </ol>

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
		submitted that use the Appendix A template of NEI 08-09, Revision 6.  The review of submitted cyber security plans that are based on approved templates should be focused on bracketed text and deviations from the approved template.	
13.6.6-07	A.2.1	The first and second bullets reference Section C.3.3 and Section C.4 of RG 5.71, respectively. RG 5.71 contains two sections named C.3.3 and C.4. Clarification is needed as to which sections are actually being referenced.	Add : Part C: Regulatory Position  Add: Part C: Regulatory Position
13.6.6-10	A.3.1.2	The first paragraph includes text not found in RG 5.71.	Modify the first paragraph to read: "The CST conducts objective security assessments, and resolves issues using the process described in Section 3.1.6 of this plan."
13.6.6-14	A.3.1.3	The fifth bullet on this page requires "identification of the digital devices having direct or indirect roles in CS function." RG 5.71 has this same requirement except that "CS" is "CDA."	identification of the digital devices having direct or indirect roles in CDA function
13.6.6-15	A.3.1.4	The following is misstated from RG 5.71: "The submitted CSP identifies and documents the following for each CDA"	The language should be clarified to read: "The submitted CSP reviews and validates the following for each CDA" to bring the SRP into alignment with Appendix A to RG 5.71, Page A-4
13.6.6-16	A.3.1.4	The last bullet contains a requirement not found in RG 5.71. It is recommended that this bullet be deleted.	Delete last bullet.
13.6.6-17	A.3.1.5	The first bullet references "Section C.3.2 of RG 5.71." RG 5.71 contains two sections named C.3.2. Clarification is needed as to which sections are actually being	Add: Part C: Regulatory Position

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan

Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
		referenced.	
13.6.6-21	A.3.2	The fifth bullet is missing a comma between "training" and "devices"	coordination of the acquisition of physical or cyber security services, training, devices, and equipment
13.6.6-23	A.4.1.1	The second bullet states that "The licensee must verify..." RG 5.71 states that "The CST verifies..."	Modify to read: The CST must...
13.6.6-23	A.4.1.1, 2 <sup>nd</sup> bullet	"Annual" status verification is bracketed in RG 5.71. SRP states it is a requirement. §73.54 does not contain an annual requirement.	<ul style="list-style-type: none"> <li>SRP should state criteria for other-than-annual since RG 5.71 allows a different frequency ('annual' is bracketed).</li> </ul>
13.6.6-24	A.4.1.2, 5 <sup>th</sup> bullet	§73.55(m) requires effectiveness reviews every two years, not annually	<ul style="list-style-type: none"> <li>Change to 'every two years' or provide regulatory basis</li> </ul>
13.6.6-26	A.4.1.3	The first bullet contains a requirement that is not found in RG 5.71. The CST may not be appropriate group that resolves the deficiencies. The corrective action program should drive the responsibility.	The licensee will conduct vulnerability scans or assessments and identify deficiencies. The frequency of the scans and assessments is at least once each quarter. Refer to RG 5.71, Appendices B and C, for frequency for specific controls.
13.6.6-27	A.4.1.3	The last bullet uses "CST" while the RG 5.71 uses "Licensee/Applicant."	Modify to read "Licensee/Applicant"
13.6.6-28	A.4.2	The first bullet uses "CST" while the RG 5.71 uses "Licensee/Applicant."	Modify to read "Licensee/Applicant"
13.6.6-30	A.4.2.2	The second bullet contains a typo.	Modify to read: the CST will evaluate, document, and incorporate...
13.6.6-30	A.4.2.2	The phrase "infrastructure interdependencies" needs a "-" beside it.	<ul style="list-style-type: none"> <li>– connectivity pathways</li> <li>– infrastructure interdependencies</li> <li>– application of defensive strategies including:</li> </ul>
13.6.6-32	A.4.2.4	The first paragraph contains a typo.	The CST must review... controls, network architecture, security devices...

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC–2010–0184

Page	Section	Comment	Proposed New Language
13.6.6-33	A.4.2.5	The first bullet references "Section C.3.1.4 of RG 5.71. RG 5.71 contains two sections named C.3.1.4. Clarification is needed as to which sections are actually being referenced.	Modify to read: Part C: Regulatory Position.
13.6.6-33	A.4.2.6	In the first three bullets, sections are referenced that are either ambiguous or do not match RG 5.71.	<ul style="list-style-type: none"> <li>• deploys the CDA in the appropriate level of the defensive model described in Section C.3.2 of RG 5.71 Part C: Regulatory Position</li> <li>• performs a security impact analysis, as described in Section C.4.2.2 of RG 5.71 Part C: Regulatory Position</li> <li>• verifies that the technical controls identified in Appendix B to RG 5.71 are implemented as described in Sections 3.1.6 of the CSP</li> </ul>
13.6.6-36-38	III	<p>Table 2, RG 5.71, Appendix B Technical Security Controls.</p> <p>For licensees and applicants who choose to submit cyber security plans based on NEI 08-09, Revision 6, Technical Security controls are not within the plan itself. Rather, the Technical Security Controls contained in NEI 08-09 Revision 6 are references to the Plan and the applicable implementing directives and procedures.</p> <p>Therefore, Table 2 is not applicable to those plans submitted for review that are based on NEI 08-09, Revision 6.</p> <p>Staff review of implemented Technical Security Controls for cyber security plans submitted using the template of NEI 08-09, Revision 6 should occur during onsite</p>	Revise SRP to state that Table 2 is only applicable to those Cyber Security Plans submitted using the template of RG 5.71 and not applicable to those cyber security plans submitted using the template of NEI 08-09, Revision 6.

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
13.6.6-39-43	III	<p>inspections.</p> <p>Table 3, RG 5.71, Appendix C, Management and Operations Security Controls</p> <p>In RG 5.71 Appendix C the title is: "Operational and Management Security Controls"</p> <p>For licensees and applicants who choose to submit cyber security plans based on NEI 08-09, Revision 6, Operational and Management Security Controls are not within the cyber security plan itself. Rather, the Operational and Management Security Controls contained in NEI 08-09 Revision 6 are references to the Plan and are reflected in the applicable implementing directives and procedures.</p> <p>Therefore, Table 3 is not applicable to those cyber security plans submitted for review that are based on NEI 08-09, Revision 6.</p> <p>Staffs review of implemented Operational and Management Security Controls for cyber security plans submitted using the template of NEI 08-09, Revision 6 should occur during onsite inspections.</p>	<p>Revise SRP to state that Table 3 is only applicable to those Cyber Security Plans submitted using the template of RG 5.71 and not applicable to those cyber security plans submitted using the template of NEI 08-09, Revision 6.</p> <p>Correct the title to be consistent with RG 5.71</p>
13.6.6.40	C.8.4	<p>Though an accurate quote from RG 5.71, there is no regulatory basis for the following 2-hour requirement: "In the event of an unplanned incident that reduces the number of required cyber security personnel, the licensee must compensate by using other trained and qualified onsite cyber security personnel or calling in off-</p>	<ul style="list-style-type: none"> <li>The requirement should be struck from both RG 5.71 and the SRP.</li> </ul>

Proposed NUREG-0800 – Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber  
Security Plan  
Docket ID: NRC-2010-0184

Page	Section	Comment	Proposed New Language
		duty personnel within 2 hours from the time of discovery."	
13.6.6-43	III	<p>The SRP states that "For reviews of CSPs for an operating reactor, the implementation schedule must consider refueling outages."</p> <p>This statement does not provide adequate acceptance criteria for staff review of proposed implementation schedules.</p>	SRP 13.6.6 should be revised to describe the complete review procedures for the proposed implementation schedule that is required to be submitted by licensees.
13.6.6-43	IV	<p>The SRP does not provide any evaluation finding for the staff's review of the proposed implementation schedule.</p> <p>NRC letter dated December 14, 2009 provides statements of the staff expectations for implementation schedules.</p>	SRP 13.6.6 should be revised to describe the evaluation findings for the proposed implementation schedule that is required to be submitted by licensees.
13.6.6-44	V	<p><u>IMPLEMENTATION</u></p> <p>The SRP inappropriately states the submittals of license amendment applications and license applications as being from applicants. The more appropriate terms commonly used by the NRC (including usage in RG 5.71) are licensees submit license amendments and COL applicants submit license applications.</p>	Revise to appropriately include licensees and applicants throughout the SRP