Standard Review Plan Comment Disposition

NEI Comment:

> For consistency sake, the Staff might consider the viability of following the format of SRP 13.6.1, “Physical Security-Combined License.”

Staff Response:

Not incorporated. This commend will be considered when Regulatory Guide (RG) 5.71 and this Standard Review Plan (SRP) are revised.

NEI Comment:

> 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.”

Staff Response:

Incorporated.

NEI Comment:

> 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.

Staff Response:

Implementation schedule guidance is slated to be put into the first revision of RG 5.71. Note that guidance was provided to licensees via numerous other methods. For example, see Agencywide Documents Access and Management System (ADAMS) Accession No.ML093080517.

NEI Comment:

> 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)

Staff Response:

Incorporated.

NEI Comment:

> 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.

Staff Response:

Section I of the SRP contains verification that the implementation milestone is included in the final safety analysis report table of operational programs. Section II of the SRP contains the criterion for an acceptable implementation milestone.

NEI Comment:

> Operational Program Description and Implementation
> This section should clearly state that this review is not applicable to operating plant necessary for cyber security plans submitted by licensees.

Staff Response:

This section of the SRP contains at the beginning, “For a combined license (COL) application …,” which makes it very clear it is applicable only to a new reactor application.

NEI Comment:

> Review Interfaces
> This section should not be applicable to operating plant licensees.

Staff Response:

The operational programs section of review interfaces points to COL reviews making it clear, it is applicable only to a new reactor application.

NEI Comment:

> 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.

Staff Response:

Change made as described in response to second comment above.

NEI Comment:

> 2nd 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 73.55(m)(2) [effectiveness reviews].

Staff Response:

The second sentence has been deleted.

NEI Comment:

> Incomplete quote of regulation which expands requirements.

Staff Response:

Revised as proposed.

NEI Comment:

> 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.

Staff Response:

10 CFR Part 73 is Reference 1 of RG 5.71. 10 CFR 73.58 is a section in 10 CFR Part 73. The process for security control implementation in RG 5.71, Appendix A, Section A.3.1.1 states, "[Licensee/Applicant] did not apply a security control when it was determined that the control would adversely impact SSEP functions." This conforms with the 10 CFR 73.58 requirements.

NEI Comment:

> Operational Programs
> As stated, this statement applies to COL reviews. It does not mention anything about review of licensee submitted plans.

Staff Response:

The paragraph was added following the guidance in Office Instruction NRO-REG-300.

NEI Comment:

> Technical Rationale
> Item 2 incorrectly cites 10 CFR 73.55 as codifying the cyber security requirements for NRC licensed power reactors. The correct citation is 10 CFR 73.54.

Staff Response:

This paragraph of the SRP discusses sections of 10 CFR Part 73 that are pertinent to cyber security.

NEI Comment:

> 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.
>
> 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.

Staff Response:

The SRP was written to correlate to RG 5.71. The review of cyber security plans for licenses and applicants is very similar not substantially different. In a letter dated May 5, 2010, (ADAMS Accession No. ML101190371). The NRC staff found that use of the template in NEI 08-09, Revision 6 would result in an acceptable cyber security plan. The staff's review of NEI 08-09 was based on using RG 5.71 guidance as the acceptance criteria. Therefore, no change is needed. This comment will be considered in future revision of the SRP.

NEI Comment:

> 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 use to comply with 10 CFR 73.54.
>
> 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, Revision 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."
>
> Similarly, the NRCs 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."
>
> 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.

The NRC review and acceptance criteria in Section III of 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.

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.

Clearly, Section III does not apply to cyber security plan submitted using the NRC approved plan template contained in NEI 08-09, Revision 6.

Staff Response:

The NRC staff must verify that each submitted cyber security plan that utilized one of the two approved templates, incorporated the template wording in the submitted plan. No change is required.

NEI Comment:

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 it 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 submitted using 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.

Staff Response:

The NRC staff review of cyber security plans does focus on deviations from the templates used. However, NRC guidance documents should still correlate, in other words the SRP should reflect RG 5.71.

NEI Comment:

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. (A.2.1)

Staff Response:

SRP clarified to reflect Regulatory Positions C.3.3 and C.4.

NEI Comment:

The first paragraph includes text not found in RG 5.71. (A.3.1.2)

Staff Response:

The text in the first paragraph was taken from different parts of RG 5.71, Section A.3 and was combined for efficiency.

NEI Comment:

> 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.” (A.3.1.3)

Staff Response:

The SRP text is the same as the corresponding of RG 5.71 text.

NEI Comment:

> The following is misstated from RG5.71: “The submitted CSP identifies and documents the following for each CDA.” (A.3.1.4)

Staff Response:

SRP modified to correspond with RG 5.71.

NEI Comment:

> The last bullet contains a requirement not found in RG 5.71. It is recommended that this bullet be deleted. (A.3.1.4)

Staff Response:

SRP modified to correspond with RG 5.71.

NEI Comment:

> 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 referenced. (A.3.1.5)

Staff Response:

Clarification added to SRP.

NEI Comment:

> The fifth bullet is missing a comma between “training” and “devices.” (A.3.2)

Staff Response:

Comma inserted as recommended.

NEI Comment:

> The second bullet states that "The licensee must verify …" RG 5.71 states that "The CST verifies…" (A.4.1.1)

Staff Response:

The word "licensee" changed to "CST."

NEI Comment:

> "Annual" status verification is bracketed in RG 5.71. SRP states it is a requirement. §73.54 does not contain an annual requirement. (A.4.1.1)

Staff Response:

The SRP is aligned with RG 5.71. No change is required.

NEI Comment:

> §73.55(m) requires effectiveness reviews every two years, not annually. (A.4.1.2)

Staff Response:

The SRP is aligned with RG 5.71. No change is required.

NEI Comment:

> 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. (A.4.1.3)

Staff Response:

The SRP has the licensee responsible to resolve deficiencies.

NEI Comment:

> The last bullet uses "CST" while the RG 5.71 uses "Licensee/Applicant." (A.4.1.3)

Staff Response:

Replaced "CST" with "Licensee/Applicant."

NEI Comment:

The first bullet uses “CST” while the RG 5.71 uses “Licensee/Applicant.” (A.4.2)

Staff Response:

Replaced “CST” with “Licensee/Applicant.”

NEI Comment:

The second bullet contains a typo. (A.4.2.2)

Staff Response:

The typographical error was corrected.

NEI Comment:

The phrase “infrastructure interdependencies” needs a "-“ beside it. (A.4.2.2)

Staff Response:

A dash was inserted as recommended.

NEI Comment:

The first paragraph contains a typo. (A.4.2.4)

Staff Response:

A comma was inserted to correct the typographical error.

NEI Comment:

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. (A.4.2.5)

Staff Response:

Clarified as Regulatory Position C.3.1.4 of RG 5.71.

NEI Comment:

In the first three bullets, sections are referenced that are either ambiguous or do not match RG 5.71. (A.4.2.6)

Staff Response:

The SRP was modified to agree with RG 5.71.

NEI Comment:

> Table 2, RG 5.71, Appendix B Technical Security Controls.
>
> 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.
>
> Therefore, Table 2 is not applicable to those plans submitted for review that are based on NEI 08-09, Revision 6.
>
> 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 inspections.

Staff Response:

Not incorporated. The plans must be evaluated well before they are implemented and the program is inspected.

NEI Comment:

> Table 3, RG 5.71, Appendix C, Management and Operations Security Controls.
>
> In RG 5.71 the title is: “Operational and management Controls.”
>
> 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 the applicable implementing directives and procedures.
>
> Therefore, Table 3 is not applicable to those plans submitted for review that are based on NEI 08-09, Revision 6.
>
> 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.

Staff Response:

Not incorporated. The plans must be evaluated well before they are implemented and the program is inspected.

NEI Comment:

> Though an accurate quote from RG 5.71, there is no regulatory basis for the following 2-hour requirement: "In the event of 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-duty personnel within 2 hours from the time of discovery." (C.8.4)

Staff Response:

The statement was removed from the SRP as there is no regulatory basis.

NEI Comment:

> The SRP states that "For reviews of CSPs for an operating reactor, the implementation schedule must consider refueling outages."
>
> This statement does not provide adequate acceptance criteria for staff review of proposed implementation schedules.

Staff Response:

The staff provided guidance to the industry under ADAMS Accession No. ML093080517. The SRP will be revised after RG 5.71 is revised to provide further implementation schedule guidance.

NEI Comment:

> The SRP does not provide any evaluation finding for the staff's review of the proposed implementation schedule.
>
> NRC letter dated December 14, 2009 provides statements of the staff expectations for implementation schedules.

Staff Response:

The staff provided guidance to the industry under ADAMS Accession No. ML093080517. The SRP will be revised after RG 5.71 is revised to provide further implementation schedule guidance.

NEI Comment:

> <u>IMPLEMENTATION</u>
> 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.

Staff Response:

The SRP was revised to address the comment.