U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

13.6.6 SECURITY ASSESSMENT - CYBER ASSURANCE EVALUATION

REVIEW RESPONSIBILITIES

Primary - Office of Nuclear Security and Incident Response

Secondary - None

I. AREAS OF REVIEW

For the cyber assurance evaluation of the voluntary security assessment, the review involves the evaluation of the applicant's cyber assurance program, for critical digital assets (CDAs) that could adversely impact safety, security, and emergency preparedness. The review encompasses parts of the applicant's security program during the licensing phase, including consideration of the effects of cyber attacks on individual components of each target set, as stated in 10 CFR 73.55. Furthermore, as stated in 10 CFR 73.55, the security program also includes implementation of a cyber-security program that provides high assurance that applicable computer systems are protected from cyber attacks, and that applicants implement a cyber-security assessment program to systematically assess and manage cyber risks.

DRAFT - August 2007

The scope of the assessment performed by an applicant would depend upon the particular stage of the application process and would determine the security design features to be incorporated into the facility design, site, and security operational programs (as applicable). A license application that incorporates by reference a construction permit, design certification, or manufacturing license, would not be required to address the design of the facility or site within the scope of the previously completed assessment for the referenced permit, certification, or license. If an applicant references a certified design, the assessment would not be intended to require enhancements to the portions of the design that has been certified [1].

Specific information to be reviewed, referenced to applicable sections of 10 CFR Part 73, §73.55, include the following:

1. The purpose and objectives of the applicant's cyber assurance evaluation

2. The scope of the assessment for the applicant in a particular licensing phase.

3. The conduct of the analysis, including quality assurance controls, staff participation, peer reviews that have been performed, and training programs.

4. Validity of resources (engineering publications) for the input data to the cyber security assessment.

5. Clear diagrams, tables and/or detailed descriptions displaying the following:

    a. The defensive model, methods and approach, with a level of detail similar to that of the example defensive model presented in NEI 04-04, Revision 1.
    b. The methodology used to evaluate cyber security risk.
    c. Risk reduction techniques to be applied to the defensive model.
    d. The initial and periodic assessments of the cyber security program, as described in NEI 04-04 Revision 1, Section 5 and NUREG/CR-6847.
    e. The initial cyber assessment results.
    f. Procedures to manage, prevent and mitigate incidents caused by a cyber attack.
    g. Continuing activities required to maintain an effective defensive strategy.

6. Insights gained from the cyber assurance process.

Review Interfaces

Other required SRP sections interface with this section as follows:

1. Standard Review Plan 0800, Section 13.6.2 Physical Security - Design Certification.

2. Standard Review Plan 0800, Section 14.3.12 Physical Security Hardware Inspections, Tests, Analyses, and Acceptance Criteria (PS-ITAAC).

---

(1) While the Tier 1 portion of the design-related information requires a rulemaking to be modified, the unmodified Tier 2 and Tier 2* portions do not have this requirement. However, this assessment is not intended to require enhancements to any of these portions of the design that has been certified.

The listed voluntary SRP sections interface with this voluntary section as follows:

1. Review of the adequacy of the high assurance evaluation of the physical protection system as part of the security assessment submittal is performed under SRP 13.6.4.

2. Review of the adequacy of the establishment of mitigative measures as a part of the security assessment submittal is performed under SRP 13.6.5.

The specific acceptance criteria and review procedures are contained in the referenced SRP sections.

II. ACCEPTANCE CRITERIA

The cyber security assessment for the reactor facility is acceptable if the cyber assurance program meets the relevant requirements of the following Commission regulations:

A. 10 CFR Part 73, §73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," as it relates to establishing the a cyber security program to protect any system that, if compromised, can adversely impact safety, security or emergency preparedness. (proposed rule)

Specific criteria acceptable to meet[2] the relevant requirements of the Commission's regulations identified above are as follows for each review described in subsection I of this SRP section:

1. 10 CFR Part 73, proposed rule §73.55 requires that an applicant develop a cyber security program which provides high assurance that computer systems, which if compromised would likely adversely impact safety, security, and emergency preparedness, are protected against cyber attacks. Application of 10 CFR Part 73, §73.55 provides assurance that the cyber assurance program will be effective and in compliance with NEI 04-04, Revision 1.

2. 10 CFR Part 73, proposed rule §73.55(f)(2) requires that an applicant consider the effects of cyber attacks on individual components of each target set. Application of 10 CFR Part 73, §73.55(f)(2) ensures that a target set analysis, performed for the high assurance evaluation of the security assessment, as described in the "Nuclear Power Plant Security Assessment Format and Content Guide," will be comprehensive and complete for targets that have potential cyber vulnerabilities.

(2) Note: The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. However, pursuant to 50.34(h), an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

Technical Rationale

The technical rationale for application of these acceptance criteria to reviewing this SRP section is discussed in the following paragraphs:

1. 10 CFR 73.55 contains physical security program requirements for power reactor licensees. The current security regulations do not contain requirements related to cyber security. Subsequent to the events of September 11, 2001, the NRC issued orders to require power reactor licensees to implement measures to enhance cyber security. These security measures require an assessment of cyber systems and the implementation of corrective measures sufficient to provide protection against the cyber threats at the time the orders were issued. The requirements maintain the intent of the security order by establishing the requirement for a cyber security program to protect any system that, if compromised, can adversely impact safety, security or emergency preparedness.

   Recently 10 CFR 73.55 has been revised (as a proposed rule) to codify the cyber security requirements for NRC-licensed power reactors. The proposed rule is expected to become final in the time frame of July 2008. Specifically, paragraph (f) of § 73.55 requires that the security assessment process consider the effects that cyber attacks may have upon individual components of each target set grouping. Paragraph (m) of § 73.55 requires that the applicant implement a cyber-security program that provides high assurance that computer systems, which if compromised, would adversely impact safety, security, and emergency preparedness, are protected from cyber attacks. Paragraph (n) of § 73.55 requires that the cyber security program is included in an applicant's security program reviews and audits.

III. REVIEW PROCEDURES

The scope of the security assessment varies depending on the particular stage of the application process in 10 CFR Parts 50 and 52. Therefore, the reviewer will select and utilize material from the procedures described below, as may be appropriate for the applicant's particular stage in the design process. See the Standard Review Plan for the associated High Assurance Evaluation (SRP 13.6.4) for further discussion of the scope for each stage.

In conducting the reviews for the various licensing stages described above, the reviewer will select and utilize material from the following procedures, as may be appropriate for a particular case. For each area of review specified in subsection I of this SRP section, the review procedure is identified below. These review procedures are based on the identified SRP acceptance criteria. For deviations from these specific acceptance criteria, the staff should review the applicant's evaluation of how the proposed alternatives to the SRP criteria provide an acceptable method of complying with the relevant NRC requirements identified in subsection II.

The NRC staff will conduct the acceptance review using a checklist, based on the cyber assurance evaluation guidance outlined in the "Nuclear Power Plant Security Assessment Format and Content Guide," dated August 2007. Section 4 of the format and content guide provides guidance for the cyber assurance program and Section 5.4 provides format and content guidelines for the applicant's cyber assurance submittal as part of the security assessment. To conduct the acceptance review, NRC staff will specifically compare the contents of the cyber assurance submittal with the requirements in 10 CFR 73.55. The staff

uses a simple scale of acceptability to help the reviewers document their results: (1) Acceptable, (2) Acceptable, but Request for Additional Information Prepared, and (3) Rejected, Inadequate to Support Detailed Review. The reviewer should use the review checklist provided in Table 1 to determine whether the submittal is reasonably complete and conforms to the requirements outlined in 10 CFR Part 73.55.

The completed cyber security assessment should provide a description of the cyber security program management roles and responsibilities, a description of the methodology used to assess overall cyber security risk, a detailed defensive strategy to be used by the cyber security program that apply to the specific cyber risks for that reactor facility, and a description of continuing activities to maintain the cyber security program's defensive strategy.

Table 1. Acceptance Review Checklist for Cyber Assurance Evaluation

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	The submittal provides:				
4.1	Introduction				
	A detailed account of the program organization roles and responsibilities, including:				
	Description of senior nuclear management (vice president or officer level)	NEI 04-04 Rev.1 4.1 Roles and Responsibilities Review Criteria: Program adequately defines responsibilities of senior management as follows: Senior nuclear management—vice president or officer level—shall sponsor the cyber security program with accountability assigned to appropriate level of management to ensure that the program meets the needs of the site and receives appropriate attention, support and compliance.			
	An individual who has been designated as the Cyber Security Program Owner	NEI 04-04 Rev.1 4.1 Roles and Responsibilities Review Criteria: Program adequately defines responsibilities of senior management as follows: An individual shall be designated as the Cyber Security Program Owner. This individual shall be given full responsibility and accountability for the program and function as the Single Point of Contact (SPOC) for any and all issues related to site cyber security.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	Those who design, own and maintain process and plant systems	NEI 04-04 Rev.1 4.1 Roles and Responsibilities Review Criteria: Program adequately defines responsibilities of process and plant system owner/designers as follows: Process and plant system designers, owners and maintainers shall be responsible for implementation of applicable components and corrective actions of the program.			
	The roles, responsibilities and accountabilities of each department and the responsible individual for that department	NEI 04-04 Rev.1 4.1 Roles and Responsibilities Review Criteria: Program adequately defines roles, responsibilities, and accountabilities as follows: The roles, responsibilities and accountabilities of each department and the responsible individual shall be identified and documented.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
4.2	Site Cyber Security Policy and Procedures				
	The site cyber security program, including policies and associated procedures, is provided to identify a hierarchical listing of implementing procedures mapped to policy in accordance with NEI 04-04, Revision 1.	NEI 04-04 Rev.1, Section 4.4 Review Criteria: Program adequately defines the hierarchical listing of implementing procedures to support the cyber security policy as well as a traceability matrix that maps established policy to implementing procedures.			
4.3	Overview of Plant Network Architecture				
	A description of the network architecture and connectivity of the plant digital systems	NEI 04-04 Rev.1 5.2 Examine Plant-Wide Cyber Security Practices Review Criteria: Documents and comprehensive I&C Drawings “D” Size exist to adequately describe Defensive Strategy Program AND physical network architecture and connectivity of the plant digital systems. Should include topological diagrams that identify networks involving CS and CDA and any related networks to which CS and CDA connect.			
4.4	Cyber Security Defensive Strategy and Risk Mitigation				
	A description of the defensive strategy with the following components:				

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	Description of a defensive model, methods and approach	NEI 04-04 Rev.1 4.2 Cyber Security Defensive Strategy Review Criteria: Strategy adequately detailed to effectively implement site level cyber security program as follows: A detailed defensive strategy is necessary to implement an effective site level cyber security program.			
	Identification of the systems/assets to be protected.	NEI 04-04 Rev.1 5.3 Identify Critical Digital Assets (CDAs) Review Criteria: CDAs adequately identified for the assessment as follows: In this stage the assessment team identifies digital assets that warrant further investigation because they perform a “critical” function at the site. It is important to consider all systems within the scope of the assessment since this step will ultimately define the level of cyber security coverage by the site’s defensive strategy. The team should take full advantage of insights from existing plant analysis such as Probabilistic Safety Assessments (PSA), the Maintenance Rule and the Safety Analysis Report.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	Identification of postulated asset threats	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Postulated threats have been adequately identified for identification of the postulated asset threats.			
	Identification of allowed and disallowed protocols between interconnected systems and/or networks.	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Identification of allowed and disallowed protocols between interconnected systems and/or networks have been adequately described.			
	Acceptable methods of data transfer between networks and systems of varying defensive levels.	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Acceptable methods of data transfer between networks and systems of varying defensive levels have been adequately described.			
	Protection mechanisms employed to counteract postulated threats	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Protection mechanisms employed to counteract postulated threats have been adequately described.			
	Defined vulnerability assessment and patch management program	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Defined vulnerability assessment and patch management program has been adequately described.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	Defined actions to be taken when a postulated threat is encountered	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Defined actions to be taken when a postulated threat is encountered have been adequately described.			
	Incident handling and escalation of cyber security event	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Incident handling and escalation of cyber security event have been adequately described.			
	Defined defensive strategy objectives	NEI 04-04 Rev.1 6.2 Defensive Strategy Review Criteria: Defined defensive strategy objectives have been adequately described.			
	A description of the defensive model with appropriate level of detail in accordance with Appendix B of NEI 04-04	NEI 04-04 Rev.1 Appendix B 2 The Defensive Model Review Criteria: The essential ingredients of the model have adequately demonstrated to contain 1. The presence of multiple levels. 2. The characteristics of the interface boundary between any two levels.			
	A description of risk reduction techniques to be applied to the defensive strategy	NEI 04-04 Rev.1 6.3 Risk Reduction Review Criteria: Defined risk reduction techniques to be applied have been adequately described.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	The methodology used to evaluate cyber security risk.	NEI 04-04 Rev.1 6.3 Risk Reduction Review Criteria: Risk adequately determined through a six-step evaluation process that included: 1. Examination of current cyber security practices. 2. Identification of Critical Digital Assets. 3. Detailed review and validation of CDA configuration. 4. Assessment of susceptibility of each CDA. 5. Assessment of the consequence on the risk level of each CDA. 6. Determination of the overall risk.			
4.5	Assessments				
	A description of the initial assessment of the cyber security program in accordance with NEI 04-04 Revision 1, Section 5, including but not limited to: the makeup of the assessment team, identification and detailed review of critical digital assets (CDAs), susceptibility assessment, detailed consequence analysis and risk assessment process	NEI 04-04 Rev.1 5.1 Assessment Team Review Criteria: The initial assessment has been adequately performed as follows: 1. Resources beyond those available for the normal management of a cyber security program have been used. 2. A plan has been developed to address management awareness, sponsorship, project leadership, objectives, team training and support functions.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	Identification of documentation including baseline assessment data, periodic reviews or self-assessments and reviews prompted by design changes	NEI 04-04 Rev.1 5.9 Assessment Records Review Criteria: The assessment process generated documentation that has been retained to provide data for the future, including the baseline assessment data.			
4.5.1	Initial Assessment Results				
	A description of the initial cyber assessment results including the susceptibility assessment, consequence analysis, resulting risk of CDAs and acceptability of risk for these CDAs, as delineated in NEI 04-04, Revision 1, Section 5	NEI 04-04 Rev.1 5 Program Assessment Review Criteria: Risk adequately determined through a six-step evaluation process that included: 1. Examination of current cyber security practices. 2. Identification of Critical Digital Assets. 3. Detailed review and validation of CDA configuration. 4. Assessment of susceptibility of each CDA. 5. Assessment of the consequence on the risk level of each CDA. 6. Determination of the overall risk.			
	If a bounding analysis is used, justification for the grouping strategy of similar CDAs	NEI 04-04 Rev.1 5.3 Identifying Critical Digital Assets (CDAs) Review Criteria: Adequate documentation exists describing the benefit and critical thought process if CDAs were classified or grouped into a single CDA.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
4.6	Training and Software Quality Assurance				
	A description of the cyber security training program in accordance with Section 6.5 of NEI 04-04, Revision 1, including:				
	Awareness program and training	NEI 04-04 Rev.1 6.5 Training Program Review Criteria: Adequate awareness program and training that increases the sensitivity to the threats and vulnerabilities and the recognition of the need to protect data, information and the means of processing them exists.			
	Technical Training	NEI 04-04 Rev.1 6.5 Training Program Review Criteria: Adequate technical training for system administrators, design engineers and network administrators responsible for the support and maintenance of the critical digital infrastructure exists.			
	Specialized Cyber Security Training	NEI 04-04 Rev.1 6.5 Training Program Review Criteria: Adequate specialized cyber security training for providing risk management and incident response personnel with the skills to design, execute and manage the cyber defensive strategy exist.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
	A description of how cyber security considerations are incorporated into software quality assurance	NEI 04-04 Rev.1 6.6 Software Quality Assurance Review Criteria: Adequate cyber security considerations are incorporated into the software quality assurance program to ensure that application security is appropriate for the environment.			
4.7	Incident Handling and Response				
	A description of the process for responding to incidents that may be caused by a cyber attack, including handling procedures, capabilities to contain and repair damage from incidents and processes to prevent and mitigate further incidents	NEI 04-04 Rev.1 6.7 Incident Handling and Response Review Criteria: Each site adequately has, as part of the defensive strategy, a process for responding to incidents that may or may not have been caused by a cyber attack.			

Format and Content Guide Section	Requirement	Basis and Acceptance Criteria	Accept	Accept with RAI	Rej.
4.8	Continuing Cyber Security Program Areas				
	A description of continuing activities to maintain an effective defensive strategy	NEI 04-04 Rev.1 7 Continuing Programs Review Criteria: The cyber security program is effective in maintaining the defensive strategy for the site and continuing activities adequately address areas of 1. Training effectiveness 2. Self-assessments 3. Configuration control 4. Evaluating new CDAs 5. Evaluating upgrades 6. Incident response 7. Program effectiveness reviews 8. Contingency plans 9. Disaster recovery plans 10. Periodic threat reviews			
5	References for all documents are listed in a Reference section of the security assessment	NEI 04-04 Rev.1 Appendix A General References Review Criteria: References and definitions have been adequately documented and utilized.			

Additional guidance for the reviewer is provided below:

1. The reviewer should verify that the scope of the security assessment is appropriate for the design stage of the reactor facility being reviewed.

2. The reviewer should verify that the cyber security assessment has been accurately and satisfactorily conducted. The analysis should be performed by a knowledgeable team of experts that together cover the entire expertise scope of the cyber security assessment. A one page resume of each team member should be provided to verify their expertise. Additionally, the reviewer should confirm that a proper quality assurance program is in place and independent and peer reviews have been performed. Documentation should be available of the protective measures taken for sensitive information used during the analysis.

3. The reviewer should confirm the validity of resources (engineering publications) that were used as input data to the cyber security assessment.

4. The reviewer should verify that insights gained from the cyber assurance process were acceptably documented.

IV. EVALUATION FINDINGS

The reviewer should verify that the applicant has provided sufficient information and that the review and calculations support conclusions of the following type to be included in the staff's safety evaluation report. The reviewer should also state the bases for those conclusions.

The evaluation finding for a Cyber Assurance Evaluation review should be substantially equivalent to the following statement:

> The applicant submitted a Security Assessment to address the cyber measures Required by 10 CFR 73, §73.55(f), to mitigate the effects that cyber attacks may have upon individual equipment or elements of each target set or grouping, and §73.55(m), to implement a cyber security program that provides high assurance that computer systems, which could adversely impact safety, security, and emergency preparedness, are protected from cyber attacks. Parts of the Security Assessment have been withheld from public disclosure pursuant to 10 CFR 2.390(d).
>
> The applicant has provided a reasonable evaluation of the reactor facility's cyber security program, in accordance with the requirements of 10 CFR 73.55. The applicant, in their cyber security assessment, described the process they will use to manage cyber security for digital systems whose function is safety related, important to safety, site security, digital systems necessary for emergency response, or for any directly connected interfacing systems that may have an adverse impact on these digital systems. Additionally, the applicant has shown that the security assessment process considers the effects of cyber attacks on individual components of each target set and that implementation of a cyber-security assessment program will systematically assess and manage cyber risks.
>
> The staff reviewed the security assessment cyber assurance section for format and content using Section 4 of the "Nuclear Power Plant Security Assessment Format and Content Guide," and found that the applicant adequately addressed cyber risks and cyber security for the applicant's stage in the licensing process in accordance with 10 CFR 73, §73.55(f) and (m).

V. IMPLEMENTATION

The following is intended to provide guidance to applicants and licensees regarding the NRC staff's plans for using this SRP section.

This SRP section will be used by the staff when reviewing the cyber assurance evaluation section of the security assessment submittals by applicants pursuant to 10 CFR 50 and 10 CFR

52. Except in those cases in which the applicant proposed an acceptable alternative method for complying with specified portions of the Commission's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with Commission regulations.

The provisions of this SRP section apply to reviews of applications immediately to accommodate design certification and COL application schedules.

VI. REFERENCES

1. 10 CFR Part 50 “Domestic Licensing of Production and Utilization Facilities.”

2. 10 CFR Part 52 “Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants.”

3. 10 CFR Part 73 “Physical Protection of Plants and Materials,” (Proposed Section §73.55).

4. “Nuclear Power Plant Security Assessment Format and Content Guide,” Information Systems Laboratories, Rockville MD, August 2007. Safeguards Information.

5. NEI 04-04, Revision 1 “Cyber Security Program for Power Reactors.”

6. NUREG/CR-6847 “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants,” Pacific Northwest National Laboratory, Richland WA, October 2004. Official Use Only.

7. NUREG/CR -6852 “An Examination of Cyber Security at Several Nuclear Power Plants,” Pacific Northwest National Laboratory, Richland WA, September 2004. Official Use Only.

8. Regulatory Guide 1.152, Rev 2 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 2006.

9. U.S. Nuclear Regulatory Commission Standard Review Plan NUREG-0800, Branch Technical Position 7-14, Rev 5 "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," March 2007.

10. U.S. Nuclear Regulatory Commission Standard Review Plan NUREG-0800, Appendix 7.1-D, Guidance for Evaluation of the Application of IEEE STD 7-4.3.2.

11. IEEE Standard 603-1998, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, July 1, 1998.

12. IEEE Standard 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, December 19, 2003.

13. EA-02-026 Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants, February 2002. Safeguards Information.

14. EA-03-086 Design Basis Threat for Radiological Sabotage, April 2003. Safeguards Information.

15. 72 Federal Register 12705 Final Rule on the Design Basis Threat (DBT), published March 19, 2007.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the draft Standard Review Plan are covered by the requirements of 10 CFR Part 50.54, which were approved by the Office of Management and Budget, approval number 3150 - 0011.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

SRP Section 13.6.6
Description of Changes

Section 13.6.6 is a new SRP section not previously included in NUREG-0800 and was developed to provide guidance for the review of Security Assessments.

In addition this SRP section was administratively updated in accordance with NRR Office Instruction, LIC-200, Revision 1, "Standard Review Plan (SRP) Process." The revision also adds standard paragraphs to extend application of the updated SRP section to prospective submittals by applicants pursuant to 10 CFR Part 52.

The technical changes are incorporated in Revision 0, dated [Month] 2007:

REVIEW RESPONSIBILITIES - Reflects changes in review branches resulting from reorganization and branch consolidation. Change is reflected throughout the SRP.

I. AREAS OF REVIEW

None.

II. ACCEPTANCE CRITERIA

None.

III. REVIEW PROCEDURES

None.

IV. EVALUATION FINDINGS

None.

V. IMPLEMENTATION

None.

VI. REFERENCES

None.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu