U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

13.6.4 SECURITY ASSESSMENT - HIGH ASSURANCE EVALUATION

REVIEW RESPONSIBILITIES

Primary – Office of Nuclear Security and Incident Response

Secondary - None

I. AREAS OF REVIEW

For review of the high assurance evaluation of the voluntary security assessment the review involves the evaluation of the physical protection system of an applicant's reactor facility design. The review encompasses the applicant's physical security program during the pre-construction licensing phase, including identification of target sets, the analysis of specific threat (i.e., the design basis threat of radiological sabotage) scenarios, the use of a risk methodology to evaluate the reactor facility design to meet the general performance objectives as described in 10 CFR 73.55(a), and the identification of security design features which enable security functions to be accomplished without undue reliance upon operational security programs.

The scope of the assessment performed by an applicant would depend upon the specific type of the application and would determine the security design features and/or security functions 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 address the design of the facility or site within the scope of a previously completed assessment for the referenced permit, certification, or license. If a

combined license (COL) applicant references a certified design, the assessment would not be intended to identify enhancements to the portions of the design that have been certified [1].

The completed high assurance evaluation should provide a description of the process used to develop and identify target sets, including methodologies used to determine and group the targets (i.e., set equipment and/or operator actions), methodologies used to perform the assessment, a list of security functions, the security design features incorporated into the design, and the security assessment parameters to be considered at future design and construction stages, as appropriate.

Specific information to be reviewed, referenced to the applicable subsections of 10 CFR 73.55, 10 CFR 73.70, 10 CFR 73.1 and Appendix C to 10 CFR Part 73, include the following:

1. The specific performance criteria and methods used by the applicant for the determination of high assurance as to whether the physical protection system (PPS) is capable of protecting all target sets with adequate margin.

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 and peer reviews that have been performed.

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

5. Clear diagrams (where appropriate) and detailed descriptions displaying the following:

    a. The facility/site characterization.
    b. Security assessment parameters.
    c. Target set analysis methods.
    d. Target set analysis results including a table with detailed information about each attractive target set.
    e. The location and integration of security design features into the reactor facility design, including detection, delay, and response elements of the PPS and systems, structures, and components with, if applicable, their associated security functions for the stage of design being evaluated.
    f. The interactions of the security design features with plant safety.
    g. Overall scenarios developed from the standard NRC scenarios and the adversary and protective force timelines and pathways for these scenarios.
    h. The demonstration of overall system effectiveness of the PPS through a combination of qualitative and quantitative means.

---

(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 the portions of the design that have been certified.

6. Insights gained from the security assessment high assurance evaluation 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).

Other voluntary SRP sections interface with this section as follows:

1. Standard Review Plan 0800, Section 13.6.5 Security Assessment - Mitigative Measures Evaluation.
2. Standard Review Plan 0800, Section 13.6.6 Security Assessment – Cyber Assurance Evaluation.

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

II. ACCEPTANCE CRITERIA

Requirements

Acceptance criteria are based on meeting the relevant requirements of the following Commission regulations:

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 73.1(a)(1) "Radiological Sabotage."

4. 10 CFR 73.55 "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," and Appendices B, C, G and H.

5. 10 CFR Part 74 "Material Control and Accounting of Special Nuclear Material."

6. 10 CFR 73.70(f) “Records and Reports.”

7. 10 CFR 100.21(f) “Non-Seismic Siting Criteria.”

Regulatory guidance documents that can be applied are as follows:

8. Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, November 1978.

9. Regulatory Guide 1.91, Evaluations of Explosions Postulated to Occur at Transportation Routes Near Nuclear Power Plants, February 1978.

10. Regulatory Guide 4.7, General Site Suitability Criteria for Nuclear Power Stations, April 1998.

11. Regulatory Guide 5.12, General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials, November 1973.

12. Regulatory Guide 5.65, Vital Area Access Controls, Protection of Physical Security Equipment and Key and Lock Controls, September 1986.

13. Regulatory Guide 5.7, Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas, Revision 1, May 1980.

14. Regulatory Guide 5.44, Perimeter Intrusion Alarm Systems, Revision 3, October 1997.

15. Information Notice No. 86-83: Underground Pathways into Protected Areas, Vital Areas, and Controlled Access Areas, September 19, 1986.

16. Regulatory Information Summary 2005-04, Guidance on the Protection of Unattended Openings that Intersect a Security Boundary or Area, April 14, 2005.

SRP Acceptance Criteria

Specific SRP acceptance criteria to meet the relevant requirements of the NRC's regulations identified above are as follows for the review described in this SRP section. The high assurance evaluation of the security assessment is not a requirement, and submission of it is voluntary. If submitted, the NRC will review the evaluation against the applicable security requirements for NRC licensed nuclear power reactors. The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. However, 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 acceptable methods of compliance with the NRC regulations.

1. Section (a) of 10 CFR 73.55. - General performance objective and requirements. Describes the requirements for establishing a physical protection system that has as its objective to provide high assurance of protection against the design basis threat (DBT) of radiological sabotage as stated in 10 CFR 73.1(a)(1).

2. Section (c) of 10 CFR 73.55 - Physical Barriers. The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers as defined in 10 CFR 73.2. The physical barriers at the perimeter shall be

separated from any other barrier designated as a physical barrier for a vital area within the protected area. Isolation zones in outdoor areas adjacent to the physical barrier at the perimeter of the protected area permit observation. Intrusion detection system detects penetration or attempted penetration of the protected area (PA) barrier. All exterior areas within the protected area are illuminated. The external walls, doors, ceiling and floors in the main control room are bullet resistant. Vehicle control measures which include vehicle barrier systems protect against the use of land vehicle.

3. Section (d) of 10 CFR 73.55 - Access Requirements. The licensee shall control all points of personnel and vehicle access into a protected area, and provide detection equipment capable of detecting firearms, explosives and incendiary devices at those points. Unoccupied vital areas are locked and alarmed with activated intrusion detection systems that annunciate in both the central and secondary alarm stations upon intrusion into a vital area. The individual responsible for the last access control function (controlling admission to the protected area) must be isolated within a bullet-resisting structure.

4. Section (e) of 10 CFR 73.55 - Detection Aids. All alarms required pursuant to this part shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station, not necessarily onsite, such that a single act cannot remove the capabilities of calling for assistance or otherwise responding to an alarm. The central alarm station shall be considered a vital area, shall be bullet-resisting, the interior will not be visible from the protected area perimeter, and associated onsite secondary power supplies for alarm annunciators and non-portable communication equipment must be located within vital areas. Alarm devices and transmission lines must be tamper indicating and self checking. Alarm annunciation shall indicate type of alarm and location. All emergency exits from protected and vital areas shall be alarmed.

5. Section (f) of 10 CFR 73.55 - Communication Requirements. Each security officer, watchman or armed response individual shall be capable of maintaining continuous communications with an individual in each continuously manned alarm stations. Conventional telephone and radio or microwave transmitted two-way voice communications shall be established with local law enforcement authorities.

6. Section (g) of 10 CFR 73.55 - Testing and Maintenance. Each applicant shall develop test and maintenance provisions for intrusion alarms, emergency alarms, communication equipment, access control equipment, physical barriers, and other security-related devices or equipment

7. Section 73.70(f) – Records and Reports. Describes the required records and reports for the on-site alarm system.

Technical Rationale

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

1. 10 CFR 73.55 establishes the detailed requirements for development and implementation of a physical security program that maintains high assurance against the threat of radiological sabotage.

2. 10 CFR 100.21(f) establishes that site characteristics must be such that adequate security plans and measures can be developed.

3. 10 CFR Part 74 establishes material control and accounting requirements for nuclear power reactors.

4. 10 CFR 73.1(a)(1) establishes the description of the design basis threat for radiological sabotage.

5. 10 CFR 73.70(f) establishes the required records and reports of the site security alarm system.

III. REVIEW PROCEDURES

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.

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 emphasize material from the procedures described below, as may be appropriate for the applicant's particular stage in the design process. The scope for each stage is described below.

1. Construction Permit (10 CFR Part 50). At the construction permit stage, an applicant would have selected a design and the site on which to build the plant. The scope of the assessment must include a description of the applicant's plan for conducting a security assessment and describe the security design features incorporated into the final design of the site based on the design and site characteristics. Scenarios that necessitate evaluation of the operational security programs may be outside the scope of this assessment. Scenarios that necessitate evaluation of operational security programs may be evaluated by using a standard set of operational security characteristics (e.g., number and position of guards, location of protected area fence). Any security design issue identified but not addressed by a security design feature may be recorded as unresolved and addressed by a future applicant who uses the construction permit.

2. Operating License (10 CFR Part 50). Generally, the applicants for a construction permit and an operating license are the same entity. At the operating license stage, the applicant would have developed the operational security programs. The scope of the assessment should include (1) reference to the security assessment for the construction permit, (2) a description of how security design features left unresolved at the construction permit stage were resolved, and (3) scenarios that necessitate evaluation of the operational security programs. Ultimately, any security design issue identified by the assessment that is not resolved by a security design feature may be identified by a security assessment parameter and would be resolved by the operational security programs.

3. Design Certification (10 CFR Part 52). At the design certification stage, the applicant would know the design but not the site or the operational security programs. The scope of the security assessment should include a description of the applicant's plan for conducting a security assessment and describe the security design features incorporated into the design based on the scenarios evaluated by the assessment. Scenarios that necessitate evaluation of site characteristics and the operational security programs may be outside the scope of this assessment. However, the applicant may decide to assess the effectiveness of the plant's security design features at a hypothetical site or sites having characteristics that fall within a set of postulated site parameters (e.g., the location of transportation routes, heat sink, water access ways, and vehicle pathways). In addition, operational security programs may be assessed by using a standard set of operational security characteristics (e.g., number and location of armed responders, protected area fence type and location). Any security design issue identified but not addressed by a security design feature may be recorded as unresolved and addressed by a future applicant who references the design certification.

4. Manufacturing License. An applicant for a manufacturing license who references a design certification for which a security assessment was done would know the design but not the site or the operational security programs. However, because the manufacturing license applicant would not change the information in the design certification, a security assessment may not be conducted at the manufacturing license stage. Any security design issue identified but not addressed by a security design feature at the design certification stage would continue to be recorded as unresolved and addressed by a future applicant who references the manufacturing license. If the applicant for a manufacturing license proposes to use a custom design (i.e., not reference a design certification), then the scope of the assessment would be to perform a comprehensive security assessment of the entire custom design. Scenarios that necessitate evaluation of site characteristics and the operational security programs may be outside the scope of this assessment. However, the applicant may decide to assess the effectiveness of the plant's security design features at a hypothetical site or sites having characteristics that fall within a set of postulated site parameters (e.g., the location of transportation routes, heat sink, water access ways, and vehicle pathways). In addition, operational security programs may be assessed by using a standard set of operational security characteristics (e.g., number and location of armed responders, protected area fence type and location). Any security design issue identified but not addressed by a security design feature may be recorded as unresolved and addressed by a future applicant who references the manufacturing license.

5. Standard Design Approval. At the standard design approval stage, the applicant would know the design but not the site or the operational security programs. The application may include a description of the applicant's plan for conducting a security assessment and describe the security design features incorporated into the design based on the scenarios evaluated by the assessment. Scenarios that necessitate evaluation of site characteristics and the operational security programs could be outside the scope of this assessment. However, the applicant may decide to assess the effectiveness of the plant's security design features at a hypothetical site or sites having characteristics that fall within a set of postulated security assessment parameters (e.g., the location of transportation routes, heat sink, water access ways, and vehicle pathways). In addition, operational security programs may be assessed by using a standard set of operational security characteristics (e.g., number and location of armed responders, protected area fence type and location). Any security design issue identified but not addressed by a security design feature would be recorded as unresolved and addressed by

a future applicant who uses the standard design approval, in developing its operational security program.

6. Combined License (10 CFR Part 52). An applicant for a combined license who selects a plant design by referencing either a design certification or manufacturing license for which a security assessment was done, would know the design, the site, and the operational security program. The scope of the assessment, if performed, should include (1) reference to the security assessment for either the design certification or manufacturing license, (2) a description of how security design features left unresolved by the design certification or manufacturing license were addressed, and (3) scenarios that necessitate consideration of the site characteristics and the operational security programs. Ultimately, security design issues identified by this or a previous assessment which are not resolved by a security design feature may be identified by a security assessment parameter and must be resolved by the operational security programs.

If the combined license application proposes to use a custom design, then the scope of the security assessment should include a comprehensive security assessment, including what would otherwise have been performed at the design certification stage, as described above. A combined license applicant referencing an already-certified design would not be able to make enhancements to the plant design on physical security issues already resolved. However there may be enhancements such as adding an alarmed door to a building that does not violate the seismic design certification that could be made at this licensing stage.

If the combined license application proposes to use a standard design approval, then the scope of the security assessment could include a complete security assessment, including what would otherwise have been performed at the design certification stage, as described above. A combined license applicant referencing an already-certified design would not be able to make enhancements to the plant design within the scope of the design certification.

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 the 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 "Nuclear Power Plant Security Assessment Format and Content Guide," dated August 2007, provides guidance on the methodology and format and content of a security assessment. The format and content guide described the process for evaluating an applicant's physical protection system (physical protection system requirements for nuclear power plants are defined in 10 CFR 73.55) against the design basis threat of radiological sabotage (as described in 10 CFR 73.1(a)(1)) and plans for mitigative measures for loss of large areas of the plant due to explosions or fires (as required as described in Appendix C to 10 CFR Part 73). Section 2.0 of the format and content guide provides guidance for conducting the high assurance evaluation and Section 5.0 provides format and content guidance for the applicant's high assurance evaluation submittal as part of the security assessment.

The reviewer should refer to the Review Procedures section of SRP 13.6.2 for technical guidance that may be applied to the review procedures described 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 confirm that the specific performance criteria used by the applicant for the determination of high assurance are clearly defined. The criteria should conform to the objectives as described in 10 CFR 73.55 with respect to prevention of significant core damage, sabotage of spent fuel and theft and diversion of special nuclear material. Furthermore, the reviewer should verify that the applicant-defined high assurance criteria are complete and sufficient such that satisfying the criteria ensures that the PPS is capable of protecting all target sets, identified for the evaluation, with adequate margin.

3. The reviewer should verify that the security assessment has been accurately and satisfactorily conducted. The analysis should have been performed by a knowledgeable team of experts that together cover the entire expertise scope of the 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.

4. The reviewer should verify that the facility and site characterization is complete and focuses on the characteristics to be used in the target set analysis. The characterization should include facility drawings important to the security assessment (including buildings, room locations, equipment locations, etc.) important operational data, operational and maintenance configurations, the physical environmental setting of the facility (site and property boundaries, adjacent facilities, etc.) entry control points, types and numbers of employees and response time of local law enforcement. The reviewer should confirm that a top view figure (D-size) of the site is included that depicts the site and facility physical security characteristics. Finally, the reviewer should verify that the design information reflects the most advanced state of the design at the time of submission.

5. The reviewer should verify that any security design issue identified by the security assessment but not addressed by a security design feature is identified in the applicant's security assessment as a security assessment parameter.

6. The reviewer should confirm that a valid method is described for the development and identification of target sets, and the analyses and methodologies used to determine and group the target set equipment or elements. The method should include risk-informed target identification, grouping of target set equipment, achievable target set screening, target set generation, attractive target set characterization and screening, analysis team qualifications, a listing of target set analysis input documents, consideration of cyber attacks and, if applicable, a process description for alternative approaches such as prevention set analysis. An acceptable method for determining target sets for the security assessment - high assurance evaluation is described in Appendix B of the "Nuclear Power Plant Security Assessment Format and Content Guide."

7. The reviewer should verify that the results of the target set analysis are the set of attractive target sets. This set should use the most current set of achievable targets.

The reviewer should confirm that a table is supplied which lists each attractive target set, using a unique target set identification method, and includes the following information for each target set listed: target set objective, initiating event, all target set equipment and locations, adversary actions necessary to neutralize target, target resiliency, credited operator actions and damage control measures, estimated time to core damage/spent fuel sabotage and theft nuclear material (as appropriate), anticipated results and its bases, likelihood of exceeding Part 100 radioactive material release and any additional pertinent considerations.

8. The reviewer should confirm, if applicable, that the prevention set analysis results are documented in a similar manner to those listed previously for target set analysis results.

9. The reviewer should verify that the applicant performed an iterative evaluation of the addition of PPS elements to the reactor facility design and that insights gained during the process were documented and implemented, as necessary. The review should also confirm that a thorough description of the physical protection system for the reactor facility design is provided, which includes the people, procedures and detect, delay, and response characteristics that are proposed for the protection of assets or facilities against theft, radiological sabotage, or other malevolent human attacks. This description should detail, through figures (D-size drawing) and text, how and where security design features have been integrated, as a result of the security assessment. It should also list the security functions of the plant. Furthermore, the reviewer should confirm that each PPS feature has an associated explanation for how that feature provides or enhances the capability of the facility to protect target sets and related elements (i.e., the physical protection system's ability to provide high assurance (e.g., central alarm station functions and responders)) against an adversary possessing the DBT characteristics. Further guidance for reviewing each type of PPS element is described below.

   Detection Elements: The reviewer should confirm that a list of intrusion sensors (internal and external) used in the final PPS design is provided. This list should include alarm assessment subsystems, access control subsystems and the alarm communication and display system. Additionally, the list should include details of the placement and protection of the central alarm station (CAS) and secondary alarm station (SAS).

   Delay Elements: The reviewer should confirm that a list is provided of passive and active barriers used in the final PPS design for access delay. Guidance for delay times may be found in SAND2001-2168, "Technology Transfer Manual - Access Delay Technology, Volume 1," Regulatory Information Summary (RIS) 2003-06, and (RIS) 2005-09.

   Response Elements: The reviewer should confirm that a discussion of the response capability and strategy used in the final PPS design is provided. Locations and types of automated denial capabilities should be listed. This discussion should include how response communications were integrated as a part of the response strategies.

Communication
Sub-element: The reviewer should confirm that a list and description of the on-site and off-site communication systems, for the final PPS design, is provided.

10. The reviewer should confirm that, as appropriate, security design features are referenced to the associated security plans and appendices, required by 10 CFR 73.55. Design applicants should identify those features that are to be included by future applicants that reference that design.

11. The reviewer should verify that the applicant demonstrates that the role of safety (i.e., safety/security interface) was considered when adding the PPS elements during the iterative PPS design process.

12. The reviewer should confirm that a standard set of NRC adversary attack scenarios was utilized or that the scenarios used include the pertinent characteristics and attributes of the radiological sabotage DBT. A description of the method used to identify overall scenarios for each standard scenario is provided. Scenarios to prevent the theft of mixed-oxide fuel assemblies are provided or there is an explanation provided with respect to why those scenarios do not apply. Adversary pathways, target access points, detection devices, traversal distances, protective features and anticipated protection force routes should be identified. Ensure that the delay associated with the security system (i.e., the time from sensor detection to time of dispatch) is included in the timeline analyses provided. A description of the method to determine the most vulnerable pathways should also be verified by the reviewer. Each scenario should be depicted in a D-size drawing that displays: adversary pathways, responder pathways, responder positions with fields of fire, and location of targets specific to that scenario.

13. For each DBT scenario, the reviewer should confirm that the adversary timeline depictions with the smallest margins and a description of the method used to assess the protective force timelines are provided. For the protective force timelines, the location of each critical interruption point (CIP), the minimum safe (or required) standoff distance (from NUREG 6190 and if applicable (within the scope) for the analysis provided), milestones in the timeline (e.g., critical point of detection, point of communication, point in which the CIP is reached and point at which weapons are readied), and time elapsed between these milestones should be provided. The reviewer should verify that any assumptions used in either timeline, that are not from one of the acceptable for use engineering publications identified by the NRC, are justified and sensitivity studies for these assumptions are provided.

14. The reviewer should verify the analysis method used to determine overall physical protection system effectiveness. If table-top methods were used, detailed descriptions of the methodologies should be included. If other modeling and simulation analysis tools were used, input variables and their sources should be verified. The reviewer should verify that any assumptions used in the analysis, that are not from one of the engineering publications identified as acceptable for use by the NRC, are justified and sensitivity studies for these assumptions are provided.

    The reviewer should confirm that adequate overall system effectiveness is demonstrated, qualitatively or quantitatively or a combination thereof, for an acceptable

set of the possible overall scenarios. The results should include a list of the most advantageous overall scenarios for the adversary (those with the lowest overall system effectiveness or timelines demonstrating the least margin). The reviewer should verify that this list contains at least the 25 worst overall scenarios, or as a minimum, the worst overall scenario corresponding to each standard NRC DBT scenario. If the results are shown in a combination or bounding fashion, adequate bases for the selected scenarios chosen should be provided.

Modeling and Simulation Analysis Method
Quantitative results should be provided in a tabular format such that the worst (i.e., lowest physical protection system effectiveness) overall scenarios are assigned with probabilities of physical protection system effectiveness that are a function of the probability of interruption and neutralization.

Table-Top or Hand-Calculation Method
Qualitative results should display key pieces of the quantitative (i.e., assigned probability of detection, assigned delay time to traverse distance/barriers, charge weights required for breaching/destruction of target set equipment) results and should include timeline depictions that combine adversary and protective force timelines in such a manner that the critical detection point (CDP), CIP and adequate margin (on the order of one standard deviation from the mean, if applicable) are displayed. Guidance for breaching analyses can be found in Regulatory Information Summary (RIS) 2003-06, (RIS) 2005-09 and NUREG 6190.

15. The reviewer should confirm that a description of the process to select, assess and evaluate the candidate security design features is provided. Candidate security features should consist of advanced security system concepts (e.g., multi-level bullet resisting enclosures built into buildings, gabion walls) and advanced security systems (e.g., remotely operated weapons, munitions based access denial systems, sticky foam, and silent defender). Chapters 4 and 5 of the “Nuclear Power Plant Security Assessment Technical Manual,” contain candidate concepts and systems. The results of the evaluation should also be verified. Those concepts/systems to be implemented are listed and displayed in accordance with element 9 above.

16. The reviewer should verify that the discussion and conclusions provided for in the high assurance evaluation are consistent with what is presented in the methods and results of the high assurance sections. The reviewer should confirm that a discussion involving the insights gained by the applicant during the security assessment process is provided.

17. The reviewer should verify that references used throughout the assessment are itemized in a reference(s) section.

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 the review of the High Assurance Evaluation of the Security Assessment should be substantially equivalent to the following statement:

> The applicant submitted a Security Assessment to address the high assurance evaluation of the physical protection system required by 10 CFR 73.55. Parts of the Security Assessment have been withheld from public disclosure pursuant to 10 CFR 2.390(d) and 10 CFR 73.21.
>
> The applicant has provided an adequate evaluation of the physical protection system of the reactor facility design. The applicant provided, in a completed security assessment, a description of the process to develop and identify target sets, including methodologies used to determine and group the target set components, methodologies used to perform the assessment, a list of security functions, the security design features incorporated into the design, the security assessment parameters, and the security assessment parameters to be considered at future design and construction stages, as applicable.
>
> The staff finds that the applicant's assessment demonstrates that the reactor facility design meets the general performance objectives of 10 CFR 73.55(a) and safeguards contingency plan described in 10 CFR Part 73, Appendix C, and provides high assurance that security functions can be accomplished without undue reliance upon operational security programs when the facility is operating. The staff also finds that the security assessment provides high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The NRC staff concludes that the applicant's physical protection system design for protection of the reactor facility against acts of radiological sabotage and theft and diversion of special nuclear material are adequate for the applicant's stage in the licensing process.

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 high assurance evaluation of the security assessment submittals of license applications submitted 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. Conventional Weapons Effects (CONWEP) software and manual, U.S. Army Corps of Engineers, Omaha, NE. Restricted to government agencies and their contractors.

2. Single Degree of Freedom Blast Design Spreadsheet (SBEDS) Version 3.1 software and Methodology Manual, U.S. Army Corps of Engineers, Omaha, Nebraska. Unclassified.

3. Waterborne Sub-Surface Blast Effects to the Design Basis Threat, D. Sulfredge, Oak Ridge National Laboratory, Oak Ridge, TN. Safeguards Information.

4. Waterborne Surface Blast Effects to the Design Basis Threat, D. Sulfredge, Oak Ridge National Laboratory, Oak Ridge, TN. Safeguards Information.

5. Guidance for Using Underwater Explosion (UNDEX) Data for Estimating Loads on Submerged Targets, D. Sulfredge, Oak Ridge National Laboratory, Oak Ridge, TN, and B. Tegeler, U.S. Nuclear Regulatory Commission, Washington, DC. Unclassified.

6. NUREG/CR-4250 "Vehicle Barriers: Emphasis on Natural Features," Sandia National Laboratory, Albuquerque, NM. Unclassified.

7. Regulatory Information Summary 2003-06 "High Security Protected and Vital Area Barrier/Equipment Penetration Manual," U.S. Nuclear Regulatory Commission, Washington, DC. Safeguards Information.

8. FM 5-250 "Explosives and Demolitions," Department of the Army, Washington, DC. Restricted to government agencies and their contractors. Export controlled.

9. DOETIC-11268 "Manual for the Prediction of Blast and Fragment Loading for Structures," U.S. Department of Energy, Washington DC. Unclassified.

10. SD-STD-02.01 "Certification Standard, Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates," U.S. State Department, Washington, DC. Unclassified.

11. Department of Defense and Department of State certified vehicle barrier list, (updated periodically by the U.S. Army Corps of Engineers, Omaha, NE, available at https://pdc.usace.army.mil/library/BarrierCertification/. Unclassified.

12. TM 5-1300 "Structures to Resist the Effects of Accidental Explosions," Department of Defense, Washington, DC. Unclassified. (Also designated as Air Force AFR 08-22 and Navy NAVFAC P-3897).

13. SAND2001-2168 "Technology Transfer Manual - Access Delay Technology, Volume 1," Sandia National Laboratory, Albuquerque, NM. In addition, all manuals in the Technology Transfer series: SAND99-2390, SAND2000-2142, SAND2004-2815P, SAND99-391, SAND99-2388, SAND99-2392 and SAND99-2389. Unclassified Controlled Nuclear Information.

14. Air Force Manual (AFMAN) 91-201 "Explosive Safety Standard," U.S. Air Force, Washington, DC. Unclassified.

15. NUREG/CR-6190 “Protection Against Malevolent Use of Vehicles at Nuclear Power Plants,” U.S. Army Corps of Engineers, Omaha, NE. Safeguards Information.

16. WINGARD (Window Glazing Analysis Response and Design) software, U.S. General Services Administration (GSA), Washington, DC. Restricted. (Available at www.oca.gsa.gov).

17. Regulatory Information Summary 2005-09, "High Security Protected and Vital Area Barrier Breaching Analysis," U.S. Nuclear Regulatory Commission, Washington, DC. Safeguards Information.

18. PDC-TR-01-01 "Structural Assessment of Spent Fuel Pools Attacked with a Sophisticated Sabotage Threat," U.S. Army Corps of Engineers, Omaha, NE. Safeguards Information.

19. PDC-TR-01-02 "Structural Assessment of Spent Fuel Pools Attacked with an Unsophisticated Sabotage Threat," U.S. Army Corps of Engineers, Omaha, NE. Safeguards Information.

20. NIJ Standard 0108.01 Ballistic Resistant Protective Materials, National Institute of Justice, Washington, DC. Unclassified.

21. Underwriters Laboratories (UL) Standard for Bullet Resisting Equipment, UL 752. Unclassified.

22. Federal Register 50 FR 32138 10 CFR 50 "Policy Statement on Severe Reactor Accidents in Regarding Future Designs and Existing Plants."

23. NUREG-1226 "Development and Utilization of the NRC Policy Statement on the Regulation of Advanced Nuclear Power Plants."

24. NUREG /CR-1345 "Nuclear Power Plant Design Concepts for Sabotage Protection," Sandia National Laboratories, Albuquerque, NM., 1981. Unclassified.

25. EA-02-026, "Interim Compensatory Measures (ICM) Order."

26. EA-03-086 "Design Basis Threat Order.”

27. NRC Guidance on Implementation of the April 2003 Revised Design Basis Threat. U.S. Nuclear Regulatory Commission, Washington, DC. Safeguards Information.

28. NUREG-1267 "Technical Resolution of Generic Safety Issue A-29, "U.S. Nuclear Regulatory Commission, Washington, DC. Unclassified.

29. NUREG/CR-1381 "A Methodology for Evaluating Safeguards Capabilities for Licensed

Nuclear Facilities," Sandia National Laboratories, Albuquerque, NM. Unclassified.

30. NUREG/CR-1198 "Design Guidance and Evaluation Methodology for Fixed-Site Physical Protection Systems," Sandia National Laboratories, Albuquerque, NM. Unclassified.

31. NUREG/CR-2643 "A Review of Selected Methods for Protecting Against Sabotage by an Insider," Sandia National Laboratory, Albuquerque, NM. Unclassified.

32. NUREG/CR-2585 "Nuclear Power Plant Damage Control Measures and Design Changes for Sabotage Protection," Sandia National Laboratories, Albuquerque, NM. Unclassified.

33. NRC Letter to Mr. Stephen D. Floyd, Vice President, Regulatory Affairs, Nuclear Generation Division, NEI. NRC Staff Review of NEI 03-12: Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program] ADAMS ML033640038.

34. Nuclear Power Plant Security Assessment Format and Content Guide, Information Systems Laboratories, August 2007. Safeguards information

35. Nuclear Power Plant Security Assessment Technical Manual, Sandia National Laboratories, August 2007. Unclassified.

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 13.6.4
Description of Changes

Section 13.6.4 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.