UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 8, 2000

MEMORANDUM TO: Bruce A. Boger, Director
Division of Inspection Program Management

FROM: Harold O. Christensen, Acting Chief
Operator Licensing, Human Performance
and Plant Support Branch
Division of Inspection Program Management

SUBJECT: NRR/NEI PUBLIC MEETING SUMMARY

On December 2, 1999, NRR/NEI held a public meeting at NRC Headquarters in Rockville, MD with 35 stakeholders present (attendance list attached). The subject of the meeting was to discuss NEI's interim Safeguards Performance Assessment Program (which has been renamed the Self Assessment Program by NEI) and the NRC Baseline Inspection Program (which was not discussed). A copy of all handouts is attached.

After brief introductory remarks and discussions of the modified agenda by the NRR representatives, NEI began the discussions by describing the organizational structure they have established for dealing with the interim Self Assessment Program and the rewriting of 10 CFR Part 73 as it relates to power reactors. NEI has assembled four industry working groups to deal with the mentioned activities. Those groups are: Group A is the Self Assessment Program which will develop the interim program; Group B deals with issues related to the adversary characteristic document (ACD) and the definition of radiological sabotage; Group C is drafting a new version of 10 CFR Part 73; Group D is reviewing the current 10 CFR Part 73 to identify unnecessary and inconsistent regulations for immediate change.

Several general issues were discussed which included the possibility of having to establish an independent "public interest" group that would be cleared and have access to the ACD. To do this, it may also be necessary to clear additional industry personnel for access to generic safeguards information. The staff will attempt to prepare a "milestone" chart which would identify all the key components of all the different activities before the next meeting. It was suggested by NEI the NRC establish "focus" groups to deal with the individual issues. Jesse Arildsen will have the lead on issues related to the definition of radiological sabotage and Robert Skelton will have the lead on issues related to the ACD.

NEI started their briefing by explaining the function of Group A which is preparing the interim Self Assessment Program (SAP) (attached). They provided the staff a draft of a document that would be used by licensees to standardize the evaluation of drills and exercises used to determine a licensee's ability to protect identified target sets against radiological sabotage. The importance of resolving the issues of defining radiological sabotage and the ACD before too

CONTACT: Robert F. Skelton, NRR
415-3309

D103

Template NRR-111

much additional work can be conducted was discussed at length. The staff advised that it was working on its own definition of radiological sabotage, not necessarily based on 10 CFR Part 100 release criteria, but nevertheless consistent with existing NRC guidance. NEI suggested that the SAP pilot be conducted for three years to be consistent with the rulemaking schedule and to ensure that each plant would be assessed at leased once. It was agreed that target set development is critical to the self assessment process and noted that NEI is considering recommending that exercise and drill frequency should be driven by the quality of site performance and not necessarily by a specific schedule. Actual pilot data would be used as a determining factor for exercise and drill frequency.

Regarding the Group B function, NEI presented a one page white paper on the subject of a 10 CFR Part 100 release (attached).

There was no discussion of the Group C function, new 10 CFR Part 73 rule language, during this meeting.

The Group D discussion related to a matrix prepared by NEI based upon survey results from six questions that were sent to each licensee. This Special Security Survey and Screening Criteria Form (attached) was used to determine variances in regional and/or plant interpretation/execution of security guidance that have resulted in security plans with inconsistent commitments. The details regarding a number of examples from the matrix were presented by NEI. Issues listed on the matrix are the issues for which NEI wants immediate security plan relief.

Several members of the public were present. The Nuclear Control Institute (NCI) was asked about their policy on controlling sensitive information. They indicated that it was their policy to disclose as much information as possible and that they did not want access to sensitive information. They raised the question regarding the role of the "active" insider in the exercise and drill self assessment. Questions were also expressed regarding the perceived lack of NRC interaction with other government agencies in relation to terrorism information and activities. Concerns were raised regarding the possible increased threat at reactor sites that are expected to have mixed oxide fuel. The issue of theft of reactor fuel was also raised by NCI. A staff member of Congressmen Markey raised concerns about the proper definition of radiological sabotage and that there had not been any discussion regarding oversight of the self assessment program.

The next "working level" meeting is scheduled for December 22, 1999 to discuss the "milestone" chart noted earlier.

Attachments:

Attendance List
Self Assessment Document
Prevention of a Part 100 Release
Special Screening Criteria
Matrix
Screening Criteria Form
NEI Security Working Group

1 INTRODUCTION

The Nuclear Regulatory Commission is considering changes to the security requirements that would increase licensee responsibility in assessing nuclear plant contingency response strategies. An industry goal is a process that allows use of performance insights to better focus available resources in those areas that most directly support protection of public health and safety.

This interim guide provides an acceptable approach for licensee evaluation of the physical protection contingency response capability required by the criteria of Appendix C to 10 CFR Part 73. It provides a performance-based program that uses evaluated drills and exercises. Other features of the safeguards defense-in-depth program, such as access authorization, continual behavioral observation, fitness-for-duty, and perimeter intrusion detection systems are considered in other parts of the licensee program.

This is an interim program to be utilized after the NRC has completed its Operational Safeguards Response Evaluation (OSRE) program in mid-2000 until a comprehensive review of requirements in 10 CFR Part 73 and anticipated rule changes are completed (reference Secy-99-241, rulemaking Plan, Physical Security Requirements for Exercising power Reactor Licensees' Capability to Respond to Safeguards Contingency Events, and the November 22, 1999 SRM.). The pilot program is expected to last three years.

2 PURPOSE AND SCOPE

This guide provides a pilot program and tools for licensee developed programs to assess the effectiveness of Contingency Response Plans. A standardized self-assessment approach to evaluated drills and exercises used to determine a licensee's ability to protect identified target sets against radiological sabotage is presented in this document.

This program provides a uniform basis for licensee developed target sets—those safety-significant structures, systems and components (SSCs) that if protected will prevent radiological sabotage. The program includes integration of licensee actions that mitigate the consequences of the event. Using these guidelines, licensees perform self-assessments to evaluate their ability to protect the plant against the Design Basis Threat described in 10 CFR § 73.1(a). In drill and exercise scenarios, postulated adversaries who are attempting to commit radiological sabotage should be credited with having equipment, capabilities and characteristics as defined in a safeguards classified Adversary Characteristics Description (ACD).

The program is designed to test each key element of the licensee's contingency response program over a three-year period, with the licensee conducting a fully integrated evaluated exercise once during the three year pilot program. The Nuclear Regulatory Commission (NRC) may observe all evaluated drills and will be invited to observe the evaluated exercise.

Training deficiencies will be corrected through the licensee's ongoing training program. Tracking deficiencies in key program elements that have not been satisfied or implemented will be accomplished through the licensee's Corrective Action Program (CAP).

This interim program guidance is not designed to incorporate all elements of the current rule. For example, target sets are used as evaluation tools, not vital areas as discussed in the 10 CFR 73.55. Licensees will continue to meet the rule requirements not covered by this program until comprehensive rule-making is completed.

3 DEFINITIONS

Adversary Force Capabilities—Specific equipment, capabilities, and characteristics of a malevolent team of adversaries defined in a safeguards classified Adversary Characteristics Description (ACD).

Contingency Response—The plan developed by a licensee that is used to implement the intended actions of the organization's members in response to a DBT event.

Corrective Action Program (CAP)—A process used to identify non-conformances, program weaknesses, ascertain causes and action necessary to correct and prevent recurrence.

Drill—Activity aimed at perfecting or evaluating the skill, knowledge, and capability of an individual or group.

Evaluated Drill—A structured drill that evaluates at least one key element of the contingency response plan.

Evaluated Exercise—A structured exercise that evaluates the integrated response to defend against the Design Basis Threat.

Exercise—An integrated response aimed at perfecting or demonstration the licensee's capability to defend against the Design Basis Threat (DBT) or components of the DBT. An exercise includes a mock adversary force and would normally demonstrate multiple scenarios.

Integrated Response—The planned, organized and controlled actions of plant employees, across disciplines to minimize or mitigate a threat and/or prevent adversarial actions that could result in a greater than 10 CFR Part 100 release. The plant response may be augmented by law enforcement, other government agencies having jurisdiction and off-site licensee resources.

Key Elements—Those elements of the plant protection program needed to protect against radiological sabotage.

Other Elements—Those elements of the plant protection program, other than key elements, that support protection against radiological sabotage.

Radiological Sabotage—Any deliberate act directed against a plant in which an activity licensed pursuant to the regulations in 10 CFR 73 is conducted, or against a component of such plant which could directly endanger the public health and safety by exposure to radiation in excess of the release limits described in 10 CFR 100.

Tabletop Drill—A drill conducted using appropriate training aids such as site structure models or drawings aimed at perfecting skills and knowledge.

Target Set—A licensee defined grouping of structures, systems and components (SSCs) to be protected from radiological sabotage. It should be noted that other equipment outside the Target Set may be used by the licensee to prevent exceeding part 100 release criteria.

Timeline—A mechanism for marking elapsed time from initiation of an event through one or more points or activities, For example, the time ticks for an adversary's progress from perimeter alarm until neutralized or to a specific target destruction. Timelines are also used for the armed response force to ensure interdiction is possible.

Weapons Proficiency—Successful completion of licensee 10 CFR 73 Appendix B weapons qualification courses or approved plan courses of fire{Need relief for pilot plants from the Appendix B requirement}.

4. SELF ASSESSMENT PROGRAM

A clear set of performance objectives must be identified for use in evaluating a licensee's contingency response strategy. These should be the same objectives used by a licensee in developing its security program. Two overarching criteria are provided in 10 CFR 73.55(a), Design Basis Threat and protection of public health and safety by protecting against exposure to radiation in excess of the release limits described in 10 CFR 100.

Public health and safety can be protected by preventing a radiological sabotage. This is consistent with the approach used for other design basis accidents. Analysis identifies target sets that, if all targets within a target set are destroyed, could lead to a radiological release that exceeds design criteria. This provides a basis for evaluating the success of a contingency response using the same evaluation criteria used by the other cornerstone areas in assessing the significance of the risk involved.

The self-assessment program incorporates a plant-wide approach in response to attempts at radiological sabotage. Success is achieved if the adversary is unable to disable all targets within the target set necessary to cause a release in excess of 10 CFR Part 100 release criteria. Full plant capability and personnel response may be included in this success evaluation. For example, if a target set contains six components that must be compromised and an adversary was successful in eliminating five of those components before they were contained or neutralized, then the response strategy would be considered successful. If an entire target set is compromised, integrated licensee response may be considered in determining if a part 100 release would result. If an entire target set is lost and the licensee demonstrates that contingency measures were successful in preventing a release in excess of part 100, then the response strategy would also be considered successful.

Periodic evaluated drills and exercises are used to determine the effectiveness of the contingency response program. To be effective, it must be clear what program elements are being evaluated

in each drill or exercise. The following key elements will be used in developing evaluated drills or evaluated exercises:

- Contingency Response Strategy
- Timelines
- Target Set Protection
- Integrated Plant Response

Other program elements, which may contribute to the successful demonstration of a key element, should be evaluated over the three-year review cycle. These include:

- Coordination and Planning
- Command and Control
- Communications
- Alarm Station Operations
- Individual Responder Tactics
- Team Response Tactics
- Use of Deadly Force
- Alarm Assessment and Intrusion Detection Equipment
- Weapons Handling and Proficiency
- Controller Participation
- Post Drill/Exercise Briefing/Critiques
- Defensive positions
- Deployment of responders and equipment
- Training

Licensees should develop a program of evaluated drills and exercises that provide for review of program elements over a three-year period. The program of integrated security drills and exercises may include table-top drills, limited scope (using no shadow force) shift drills, or exercises.

The adversary characteristics of the Design Basis Threat are used to develop scenarios for the drills and exercises. A range of adversary force capabilities should be used in developing scenarios. Although not required in every evaluated drill, the capabilities described in the Adversary Characteristics Description should be exercised when considering the entire set of evaluated drills and exercises conducted during a three-year cycle.

For each evaluated drill or exercise, the licensee shall develop a scenario that tests some portion of the licensee's capability to defend against radiological sabotage. Each scenario must clearly identify those key elements of the contingency response program being evaluated.

Each licensee shall provide for an evaluation of the plant's response during the drills and exercises and ensure that appropriate actions are taken to address areas where key or other program elements are not met. Assessment of the actions needed and follow up should be through use of the CAP.

Drills conducted for other purposes, such as initial training or familiarization, need not be included as part of the self-assessment program.

5 TARGET SET DEVELOPMENT

Clearly defined target sets are key to the evaluation process, providing a basis for determining the effectiveness of contingency response strategies. The target set development process is included here as a basic step in the evaluation process.

Target sets are developed based on a safety-focused approach considering design, operational, and security characteristics of the plant. Target set development is independent of the threats that could lead to radiological sabotage. Each target set is developed to provide reasonable assurance that, if any element is protected, public health and safety will not be endangered by radiological sabotage.

Appendix A provides examples of several processes used for developing target sets.

6 ADVERSARY CHARACTERISTICS

The Design Basis Threat described in 10 CFR 73.1 covers a spectrum of adversary capabilities. To develop and evaluate contingency response strategies, precise definition of key factors such as the adversaries' physical capabilities and skills, armament, and understanding of plant systems and operations is needed. These characteristics are defined in the Safeguards Information Adversary Characteristics Description (ACD).

Scenarios are developed to test up to the full capabilities of the adversaries defined in the ACD. Adversary capability for some scenarios may be less than the full capabilities, depending on the program elements being tested. A variety of scenarios should be used to ensure that the full range of adversary characteristics is periodically tested. A combination of the target sets and adversary characteristics provides the basis for evaluating the effectiveness of program elements.

7 CONTINGENCY RESPONSE STRATEGY

Because each nuclear plant is unique, it is not possible to develop a generic contingency response strategy. The licensee will develop target sets based on plant design and physical layout. The ACD provides specific adversary characteristics serving as the basis for determining adversary timelines. Using this information, licensees will develop a strategy to defend target sets by ensuring that response timelines place an adequate number of responders in position to defend target sets. The primary goal of this guide is to develop a standardized effectiveness evaluation. To do this certain elements of the response strategy must have been defined and must be available for evaluation. These include:

- Define a timeline for adversaries carrying their required weapons, explosives and equipment to reach and destroy each of the targets in a target set. The composite time line should consider times to:

- breach various points along the Protected Area (PA) perimeter to entrances to buildings and structures that contain parts of the assemblage of SSCs that make up a target set,
- defeat the barrier at that entrance,
- destroy that equipment, and
- reach the next component of a target set.
- Determine the timelines for armed responders from deployment points to response positions where they can engage adversaries during the attack. If responders were required to obtain equipment or complete other activities prior to responding, this would be factored into the timelines.

8 EVALUATED DRILLS AND EXERCISES

The purpose of the evaluated drill and exercise program is to demonstrate and evaluate the licensee's ability to meet the key elements of its contingency response program. This is done by providing a standardized approach to developing, planning, conducting, and assessing drills and exercises.

Personnel and plant safety must be the top priority throughout the planning and execution phase of a drill or exercise. Detailed planning is required to ensure that there is no inadvertent use of live weapons, and that drill participants are made aware of licensee safety requirements and the existence of any unsafe conditions.

One acceptable methodology for conducting a drill or exercise is provided in Appendix B.

8.1 SCENARIO DEVELOPMENT

Each licensee shall develop scenarios for each evaluated drill or exercise that evaluates key elements of the licensee's contingency response strategy. These scenarios should be credible and realistic to be representative of the ACD. These scenarios should challenge the licensee's contingency response strategy by simulating various adversary assaults to include proper response equipment and integrated licensee response, as appropriate. The scenarios will clearly identify the key elements that are being challenged and the performance criteria for successful demonstration of the key elements.

Some examples of scenario development can be found in Appendix B.

8.2 PLANNING

Proper planning and coordination of drills and exercises is required to ensure adequate resources and personnel are available to safely conduct drills or exercises. The first step in planning and coordinating is to determine the objective of the drill or exercise. Is the purpose of the drill to provide training, evaluation or testing, validation of a new strategy or is it a required or prescheduled drill or exercise.

Planning elements that should be considered are included in Appendix B:

8.3 CONDUCT OF DRILLS AND EXERCISES

Prior to initiation of a drill or exercise, briefings must be conducted in the following areas:

- Safety plan briefings will be conducted prior to all drills or exercises. Ensure that all safety equipment as necessary is issued. Conduct walk-downs of drill area if necessary. Identify conditions under which the drill may be terminated due to safety concerns
- Verify that all drill participants are briefed on their responsibilities prior to conducting drills or exercises.
- Communicate with plant operations and control room prior to initiating drill.
- If a Shadow Force is used during a drill or exercise, ensure that all participants understand their responsibilities for drill participation.

8.4 ASSESSMENT OF A DRILL OR EXERCISE

Critiques should be used both as a tool for training and as a means of program assessment. The critiques should evaluate and document the licensee's performance in each of the key or other elements identified in the scenario.

Post drill or exercise critiques should normally include input from each evaluator, controller, and player to ensure all lessons learned can be incorporated into the final drill report. The Controller will normally facilitate the post drill/exercise critiques.

Examples of information normally found on Critique Forms are located in Appendix B

Post drill/exercise critiques should be formally documented using the standard sites format so that each element of performance is measured and appropriately assessed.

The initial draft report should be reviewed by the principles participating in the drill and comments gathered through a cross review process. Consideration will be given to comments for inclusion into the report. The final drill/exercise reports will be retained for three years.

8.5 FREQUENCY

Drills should be performed regularly enough to demonstrate proficiency for key security personnel. One evaluated drill shall be conducted annually for each shift. An evaluated exercise shall be conducted triennially. An extension of the time interval of evaluated drills and exercises up to 25% is acceptable.

Appendix C provides a method for two new performance indicators that could be used after the self-assessment program had been well established at a facility. The proposal does not specifically address minimum drill and exercise frequency beyond the triennial exercise requirement. Frequency will be determined at each site based on the following factors:

- The number of evaluated drills and exercises needed to meet drill participation goals,
- The number of evaluated drills and exercises needed to establish proficiency in the key elements, and

- Actual performance measured against drill and exercise performance goals.

9 CORRECTIVE ACTION

Deficiencies identified during an evaluated drill or exercise should be handled consistent with the site's corrective action, self-assessment or training program. Training deficiencies are normally addressed as part of the training program. Key element deficiencies should be considered for inclusion in a corrective action program.

APPENDIX A

Target Set Development Process

There are several acceptable approaches to target set development. There are four general areas that must be considered, as listed below. Tabs to this appendix provide several more detailed procedures that may be used.

1. SOURCE

Determine the radiological sources that have the potential to create a release in excess of 10CFR Part 100 limits. Other sources may be eliminated on a plant specific basis using an engineering evaluation of source term to determine if a release in excess of 10CFR Part 100 limits is possible or if sufficient design characteristics exist to mitigate any radiological release to less than 10CFR Part 100 limits.

Examples are:

- Reactor
- Spent Fuel Storage Pool

2 BARRIERS

Determine the barriers that must be protected to prevent a radiological release in excess of 10CFR Part 100 limits.

Examples are:

- Fuel cladding
- RCS piping and pressure boundary
- Containment Integrity

3 SYSTEMS, STRUCTURES, AND COMPONENTS (SSCs)

Determine SSCs that must be protected to prevent radiological sabotage:

Examples are:

- Reactor Coolant inventory sources (tanks, pools, etc)
- Power sources (electrical, steam, etc)
- Physical barriers (containment, system piping, etc)
- Equipment (Pumps, fans, etc)

Credit for personnel action per normal and emergency procedures or guidelines is assumed for any radiological sabotage event. If protection of SSCs does not provide adequate protection to prevent barrier breech, additional plant personnel action may be considered.

A loss of off-site power would normally be assumed to occur at the onset or during the radiological sabotage event. It is also assumed that personnel action to shutdown the plant by a scram will be effective. No single failure of redundant components is assumed since this is not a design basis event.

4 TARGET SETS

A Target Set is defined as a group of SSCs whose failure would lead to a radiological release in excess of 10CFR100 limits. Target Sets are identified by determining the minimum group(s) of targets from the SSCs, based on input from plant personnel experienced in Security, Operations, Engineering, Probabilistic Risk Assessment, etc., that will prevent a radiological release in excess of 10CFR100 limits. This grouping of targets will define an individual Target Set. All targets within any given Target Set must be damaged to the extent they will not function before a radiological sabotage event could be postulated to occur.

APPENDIX A TAB 1

Risk Informed Target Set Development

The following six-step process describes one approach to using a risk informed process to develop target sets for a physical security response strategy.

(TO BE DEVELOPED)

APPENDIX A TAB 2

Sample Target Set Development

EXPERT PANEL APPROACH

(TO BE DEVELOPED)

APPENDIX A TAB 3

Sample Target Set Development

LOGIC FLOW PATH APPROACH

(TO BE DEVELOPED)

APPENDIX B

EXAMPLES EVALUATED DRILL AND EXERCISE

SCENARIO DEVELOPMENT

Scenarios can be developed for a variety of environmental conditions such as inclement weather or darkness. Plant conditions may range from operating at power to refueling or other major maintenance activities. Drills can also be conducted during various conditions of security readiness such as day, night or, backshifts. Some scenarios should be run involving less than full adversary characteristics. Some examples include:

- unarmed intruder with ecological or media exposure goals,
- a single individual with no special adversary skills and simple tools, weapons and improvised explosive devices,
- threats of adversary actions such as bomb threats or attack. or
- a disgruntled employee who may attempt workplace violence.

Each scenario should be evaluated to validate both the safety of the scenario and ability to assess the desired key elements of the contingency response strategy.

1. PLANNING ELEMENTS THAT SHOULD BE CONSIDERED:

The following are Planning Elements that must be considered

- Safety and development of a safety plan
- Adequate simulation equipment
- Communications support for drill participants
- Ensuring security plan commitments are met during the drill
- Drill participant roles defined
- Advance notifications of required personnel

During the planning phase of a specific drill or exercise, key elements to be evaluated must be identified, as well as the success criteria. Planning details will be dictated by whether the purpose is to provide training, evaluation or testing.

In planning the evaluated drill or exercise, personnel must be specifically identified to fill each of the following roles.

- **Lead Controller** - The drill or exercise leader with overall knowledge of security shift operations. This individual may be selected from the security staff or other organization as appropriate.

- **Controllers**--Individuals with required knowledge of his/her assigned area whose responsibility is to assist the Lead Controller in drill safety and operation. May be selected from the Security Staff or other organization as appropriate.
- **Evaluators**—An individual with knowledge of his assigned area who observes and documents drill participant performance and reports his/her observations to the Lead Controller. May be selected from the Security Staff or other organization as appropriate
- **Adversaries**—Appropriately equipped and trained mock attackers with the required physical abilities to engage the licensee drill players in an armed attack to test their ability to defend against the DBT.
- **Players**
  - **CAS/SAS Players**--Security force members stationed in the alarm stations that will perform CAS/SAS duties as drill players during the drills and exercises. They will be briefed on drill conditions and respond security force players to drill contingency events.
  - **Security Force Players**—Security responders equipped with exercise response gear or equipment that respond to the Security contingency event.
  - **Security Shadow Force**—Non-drill players who are used during a force on force exercise to ensure that all requirements identified in site specific Physical Security Plan and Training and Qualification Plans are met during an exercise.
  - **Plant Operations Personnel**--Single SRO who would normally be assigned to a command and control function.

2. EXAMPLES OF INFORMATION NORMALLY ON CRITIQUE FORMS

The following are examples of information normally found on Critique Forms:

- Name of controller/evaluator
- Players evaluated
- Date of drill or exercise
- Quantified evaluation standards for each element
  - Strengths
  - Element demonstrated
  - Demonstrated with conditions
  - Not Demonstrated needs improvement
  - Not observed
  - Contain all performance areas i.e., command and control, communications
- Have a comments or lessons learned section in the document so enhancements or weaknesses can be tracked and documented for further evaluation

3. EXAMPLES OF TYPES OF EVALUATED DRILLS

The following are examples of types of evaluated drills:

- Timeline Drills - Conducted for individuals or portions of shift to ensure that responders are knowledgeable of their response strategy and are capable of meeting their response timelines.
- Table Top Drills - Conducted at least annually for each CAS Officer. This is the most valuable planning drill and will be used as an evaluation tool for development and changes to contingency response plans.
- Limited Scope Shift Drills - Conducted as needed for each individual, group or shift to validate/test contingency response plans.

Triennial evaluated exercise will be announced in advance and used to demonstrate the on-site response capability of the licensee against the DBT. This will involve use of a shadow force and involve multiple shifts. Each shift will be involved in an evaluated drill during the three-year cycle.

4. DETAILED EVALUATION CRITERIA

Immediately following the drill or exercise, a formal evaluation including the controllers, participants, supervision, and others will occur. The following are measures to be used in determining if overall performance is adequate.

- Adequate Personnel: The required number of licensee personnel necessary to adequately implement the response strategy. This number will vary from plant to plant based on plant design and characteristics.
- Appropriately Equipped: Do licensee personnel implementing the security contingency response plan have the weapons and equipment necessary to execute their responsibilities.
- Responding in a timely manner: Do licensee response personnel have adequate time in their response timelines to get to their response positions in advance of the adversary timelines.
- Does the response plan provide protection for target sets such that the plant is protected against exceeding a Part 100 release?

The post drill/exercise critiques should begin with an overview or re-statement of the drill/exercise scenario describing the purpose, objectives, general observations, and specific results. The Controller should conduct the overview so that the critique is meaningful and orderly. Each evaluator and controller should review their individual observations describing in detail each element of the performance observed and quantify the results.

Each player or participant should be allowed to add clarification for actions demonstrated and be encouraged to asked questions. If safety issues are identified, the lead evaluator should document these findings in the sites corrective actions program. Post drill/exercise critique forms should be collected and combined with the drill package for retention and review. These results constitute the basis for the final drill/exercise report.

A formal post drill critique discussion made up of the evaluators and controllers should take place to thoroughly sift through the drill performance. This review should ensure that the

objectives were met or not met, identify if any key elements were missed that could require immediate actions, review all supporting elements for enhancements or strengths and quantify a consensus overall score. The group should then prepare the initial draft report.

The initial draft report should be reviewed by the principles participating in the drill and comments gathered through a cross review process. Consideration will be given to comments for inclusion into the report. The final drill/exercise reports will be retained for three years.

Licensee Evaluation/Critique Process will involve standards for supervisors and drill controllers to ensure results of tests, drills and exercises are factored into the training process. Controllers and supervisors will provide feedback to individuals, shifts, and management using objective critique criteria for all elements of the exercise from adversary detection through drill completion. Controller critique information will be made a part of the drill and exercise records and be available for NRC review.

Evaluation Process is against defined performance criteria, will be objective and cover the following as a minimum: CAS Officers, Armed Responders, Command and Control Personnel, Operations Personnel (if involved), and Simulated Adversary Personnel.

- CAS Officers will be evaluated to ensure that they can adequately acknowledge, access and dispatch responders to the threat.
- Armed Responders will be evaluated to ensure that adequate responders are available to respond to protect the required elements of the target sets, with weapons and equipment capable of meeting its intended function and that they are trained to use that equipment under conditions encountered in the plant, and that they have individual response plans for all developed scenarios to include knowledge of target set components.
- Command and Control Personnel will be evaluated to ensure that they can execute and direct a contingency response force.
- Operations Personnel will be evaluated to ensure that they are familiar with security contingency plans and are capable of taking mitigating actions should a direct armed assault occur and/or elements of target sets are destroyed.
- Adversary Personnel will be evaluated to ensure that they are creating a realistic challenge for the response force by simulating the adversary characteristics outlined in the ACD.

APPENDIX B TAB 1

Drill Evaluation Considerations

The following guidelines provide factors that should be considered when developing performance assessment checklists for drills and exercises.

1 EXERCISE CONTROL

a. Security personnel participation meets expectations?
b. Controllers participation meet expectations?
c. Adversaries participation meet expectations?
d. Pre-exercise briefings meet expectations?
e. Control during drill/exercise meet expectations?
f. De-briefing and evaluation of drill/exercise meet expectations?
g. Overall exercise control and evaluation meet expectations?

2 EXERCISE ADMINISTRATION

a. Written scenarios demonstrate key elements?
b. Written drill/exercise plans meet expectations?
c. Drill/exercise guidelines meet expectations?
d. Safety plan meets expectations?
e. Controller checklists meet expectations?
f. Post-exercise documentation meets expectations?
g. De-briefs meet expectations?

3 PLANNING

a. Were response plans in place for the security force to deal with this type of scenario?
b. Were these plans demonstrated?
c. Did all personnel understand the plans?
d. Was plant vulnerability properly assessed?
e. Were defensive positions established to meet the plant vulnerability?
f. Were plans and procedures made for defense-in-depth?
g. Were necessary improvised plans rapidly developed?
h. Did CAS/SAS utilize available contingency plans and checklists?
i. Were plans developed to notify/use LLEA?
j. Did adversaries develop plans to challenge the response plans?
k. Did overall plans contribute or detract from the resolution of this scenario?

4 COORDINATION, COMMAND, AND CONTROL

a. Were affected portions of the plant notified prior to initiation of the drill/exercise?
b. Was coordination and command within the security force demonstrated?
c. Was coordination between security and LLEA demonstrated?

d. Were security personnel knowledgeable of lines of authority?
e. Did overall command and control contribute or detract from the resolution of this scenario?

5 EVALUATE DEFENSIVE STRATEGY

The following are methods to use in evaluating defensive strategy in setting the plant's initial strategy and in response to changing plant conditions or increases in threat levels.

a. Ensure that barriers and perimeter intrusion detection systems, and assessment systems are adequate to delay, detect, and provide capability to assess the adversary.
b. Ensure that communication plans and equipment exist to facilitate a contingency response plan.
c. Ensure that a command and control plan exists to direct a contingency response plan.
d. Ensure that CAS/SAS Officers can acknowledge, assess and dispatch responders to the threat.
e. Ensure that responders are available to respond to protect the required elements of the target sets.
f. Ensure that responders have weapons and equipment capable of meeting its intended function and that they are trained to use that equipment under conditions encountered in the plant.
g. Ensure that responders have response plans for all developed scenarios to include knowledge of target set components.
h. Ensure that Operations personnel are capable of taking mitigating actions should elements of target sets be destroyed.
i. Ensure that response plans contain both initial and follow up plans.
j. Ensure that there is a continuous communications loop between responders in the field, CAS/SAS, Command personnel and Operations.

6 COMMUNICATIONS

a. Was alarm acknowledged and information relayed to security force?
b. Was the adversary target identified?
c. Were communications between CAS/SAS and security force demonstrated?
d. Were communications between supervisors and the security force demonstrated?
e. Were communications between security force members demonstrated?
f. Did security force members relay information/intelligence to CAS/SAS?
g. Were communications between adversaries demonstrated?
h. Were communications between CAS/SAS and Operations demonstrated or simulated?
i. Were communications between the site and LLEA demonstrated or simulated?
j. Were radio communications relied on too heavily?
k. Were alternate means of communications used?
l. Was communication security discipline maintained?
m. Were communications understandable?

7 ALARM STATION RESPONSE

a. Did station operators assess the number of Intruders?
b. Were intruders described?
c. Did station operators track intruders?
d. Did station operators identify zone of penetration?
e. Did station operators identify armament or equipment?
f. Were plant notifications made?
g. Did station operators use contingency plans, procedures?
h. Was information gathered from cameras?
i. Was information gathered from response officers?
j. Did station operators utilize station equipment to fullest advantage?

8 INDIVIDUAL TACTICS

a. Did the officer respond to the initial alarm tactically?
b. Did the officer notify CAS/SAS of engagement or sighting?
c. Did the officers appropriately defend their positions?
d. Was available cover and concealment used?
e. Were selected firing positions tactically sound?
f. Was minimum exposure maintained?
g. Were danger areas crossed tactically?
h. Did the officer simulate firing the weapon? Reloading?
i. Did the officer shoot properly through smoke?
j. Did the officer respond to adversary tactics/weapons?
k. Did the officer relay adversary intelligence to CAS/SAS?
l. Were terrain and/or the physical plant utilized for cover and concealment or movement?
m. Overall, did individual tactics contribute to or detract from the resolution of this scenario?
n. Did the officers interpose between targets and the adversary force with adequate presence and effective fire/counterforce (situation dependent)?

9 TEAM TACTICS

a. Did the security force work together as a team?
b. Did the security force work with operations as a team?
c. Were tactical deployment techniques used? (cover and concealment)
d. Were alternate response routes planned or available?
e. Were correct defensive positions achieved in a timely manner based upon the adversary target and plant vulnerability?
f. Was supporting fire used?
g. Did the security force take action to protect critical plant safety systems?
h. Did the security force maintain control of key targets?
i. Overall, did team tactics contribute to or detract from the resolution of this scenario?
j. Were team tactics effective in denying or otherwise neutralizing the adversary force?

10 USE OF DEADLY FORCE /APPLICATION OF FORCE

a. Was the necessary level of force used to prevent radiological sabotage?
b. Was the use of excessive force avoided?
c. Did the force applied minimize danger to security force and plant personnel/equipment?
d. Did security force personnel maintain fire control and discipline, tactics, target acquisition and selective fire?

11 RESPONSE TO INTRUDERS WITHOUT IDENTIFIED WEAPONS

a. Did the response team interpose between the intruder and target sets?
b. Did the response team control of the situation?
c. Was a proper distance between the responders and the intruder maintained?
d. Did response team members cover the intruder?
e. Was the intruder contained?
f. Did the response team employ use of handcuffs and non-lethal controls?

12 PHYSICAL SECURITY AND EQUIPMENT

a. Did the security force use physical security systems to their advantage?
b. Was security force response sufficient to meet alarm system detection?
c. Did assessment systems provide information about adversaries for security force interdiction?
d. Were communications systems adequate?
e. Were the correct security force weapons used in this scenario?
f. Did barriers provide denial or delay to allow security force interdiction?
g. Did response positions provide protection for security force personnel?
h. Were alternate routes to response positions available?
i. Did overall physical plant and security equipment provide an opportunity for the security force to accomplish its mission?

13 CONTROLLER PARTICIPATION

a. Were controllers trained and/or briefed on responsibilities for drill/exercise?
b. Were controllers trained and/or briefed on rules of engagement?
c. Did controllers ensure drill/exercise participants were equipped with appropriate simulated weapons and perform safety inspections and briefings?
d. Were controllers prepared to stop actions for any safety hazards?
e. Did controllers coach or advise drill/exercise participants?
f. Did controllers resolve questionable shots by drill/exercise participants?
g. Did controllers provide objective critique at post-drill/exercise briefing?
h. Did controllers provide feedback to assigned participant?
i. Did controllers evaluate individual and team tactics?

14 POST DRILL/EXERCISE BRIEFING

a. Were drill/exercise participants present for briefing?
b. Were notifications made to plant personnel at conclusion of drill/exercises?

c. Were scenarios and expectations explained?
d. Did drill/exercise participants relay their participation and responses?
e. Were drill/exercise deficiencies reviewed in briefing?
f. Were participants responsive in briefing?
g. Was briefing conducted in a professional manner?
h. Did exercise participants maintain a professional attitude?
i. Did overall briefing contribute to or detract from the overall resolution of this scenario?
j. Did the drill/exercise sufficiently evaluate the site's ability to prevent radiological sabotage from occurring during this scenario?

APPENDIX C

Physical Protection Effectiveness

The objective of this evaluation tool is to ensure that the licensee is capable of implementing adequate measures to protect the public health and safety during a physical protection emergency. Licensees routinely assess and refine their physical protection plans through Integrated Site Security Organization (ISSO) participation in drills, exercises, actual events, training, and subsequent problem identification and resolution. Employees are trained to ensure that the plan can be effectively implemented during an emergency. Drills, exercises, ISSO participation and reliability of the perimeter detection system all contribute to reasonable assurance that the licensee has an effective physical protection program.

{The term ISSO needs to be clearly defined in this section.}

The protection of public health and safety is assured by a defense in depth philosophy that relies on: safe reactor design and operation, the operation of mitigation features and systems, a multi-layered barrier system to prevent fission product release, and a defensive strategy.

The onsite performance indicators monitored by this section are:

- Drill/Exercise performance
- ISSO Drill Participation
- Perimeter Detection System Reliability

The performance indicators do not specifically address minimum drill and exercise frequency beyond the triennial requirement. It is assumed that some drill and/or exercise activity will be conducted quarterly. Actual frequency will be determined at each site based on the following factors:

- The number of drills and exercises needed to meet key ISSO drill participation goals,
- The number of drills and exercises needed to establish proficiency in the key elements, and
- Actual performance measured against drill and exercise performance goals.

1 DRILL/EXERCISE PERFORMANCE

1.1 PURPOSE

This indicator monitors timely and accurate licensee performance in drills and exercises when presented with opportunities to demonstrate the defensive strategy, implementation of timelines, target set denial and/or firearms proficiency.

1.2 INDICATOR DEFINITION

The percentage of all drills and exercises that were performed successfully during the previous twelve quarters.

1.3 DATA COLLECTION ELEMENTS

The following data is required to calculate this indicator:

- The number of drills and exercises during the previous quarter.
- The number of drills and exercises performed successfully during the previous quarter.

The indicator is calculated quarterly

1.4 CALCULATION

The site average values for this indicator are calculated as follows:

(# of successful drills and exercises during the previous12 quarters) times 100
(Total number of drills and exercises during previous 12 quarters)

1.5 DEFINITION OF TERMS

Opportunities should include multiple or singular events during a single drill or exercise as follows:

- Demonstration of the appropriate defensive strategy
- Implementation of a time line for the appropriate defensive strategy
- Demonstration that a target set has been denied to an adversary
- Firearms proficiency during a course of fire

Successful means the pre-established criteria has been met for an opportunity during a drill, exercise or actual event.

2 PHYSICAL PROTECTION ORGANIZATION DRILL PARTICIPATION

2.1 PURPOSE

This indicator measures the percentage of key Physical Protection Program (ISSO) members who have participated in drills, exercises, or training opportunities.

2.2 INDICATOR DEFINITION

The percentage of key ISSO members that have participated in a drill, exercise, or actual event during the previous twelve quarters, as measured on the last calendar day of the quarter.

2.3 DATA COLLECTION ELEMENTS

The following data are required to calculate this indicator:

- Total number of key ISSO members
- Total key ISSO members that have participated in a drill or exercise, in the previous twelve quarters

The indicator is calculated, based on participation over the previous twelve quarters.

2.4 CALCULATION

The site indicator is calculated as follows:

$$\frac{\text{(\# of Key ISSO Members that have participated in a drill or exercise, during the previous 12 quarters) times 100}}{\text{Total number of Key ISSO Members}}$$

2.5 DEFINITION OF TERMS

Key ISSO members are those who fulfill the following functions:

- Control Room
  - Shift Manager—Supervision of reactor operation, responsible for plant operational response to physical threats
- Security
  - Response Force Leader—Management of plant security response and defensive strategy implementation
  - CAS and SAS
  - Armed Responders

2.6 CLARIFYING NOTES

Evaluated simulator training evolutions that contribute to the drill or exercise performance indicator statistics could be considered as opportunities for key ISSO member participation and may be used for this indicator. However, there is no intent to disrupt ongoing operator qualification programs. Appropriate operator training evolutions should be included in this indicator only when physical protection aspects are consistent with training goals.

If a key ISSO member or operating crew member has participated in more than one drill during the twelve quarter evaluation period, the most recent participation should be used in the indicator statistics.

If a change occurs in the number of key ISSO members, this change should be reflected in both the numerator and denominator of the indicator calculation.

Participation may be as a participant, mentor, coach, evaluator, or controller, but not as an observer. Multiple assignees to a given key ISSO position could take credit for the same drill if their participation is a meaningful opportunity to gain proficiency in the assigned position.

The meaning of "drill" in this usage, is intended to include proficiency enhancing evolutions (table top drills, mini drills, etc.) that reasonably simulate the interactions between appropriate organizations and/or individuals that would be expected to occur during security events. For example, control room interaction with security could be simulated by a controller performing security functions.

A Fundamental Element of the Security Cornerstone is Prevention of a Part 100 Release

The basis for the design of redundant systems, structures, and components in every nuclear plant is based on multiple layers of protection (defense in depth) for the barriers that prevent the release of radioactivity to the environment. The design measure for these layers of protection is to prevent exceeding radiological release limits based on Part 100 assuming a single failure of any redundant system, structure, or component. In addition, operator training focuses on emergency procedures designed to protect the health and safety of the public by maintaining the integrity of the protective barriers. These procedures consider failures that may occur and the actions to be taken to utilize the remaining functional items to maintain the integrity of the protective barriers.

If barriers are challenged by external or internal plant conditions, Emergency Action Level criteria exist that directs the emergency response organization to take actions to protect the public from the potential release of radioactivity. These action levels are also based on the integrity of the protective barriers and actions are taken to prevent exposure to the public in excess of Part 100 limits.

Physical security elements and the security force contingency response at a nuclear plant need to be based on the same criteria as the plant design basis accidents and the emergency action level classifications for emergency response. By using the same criteria, security becomes an integrated part of the plant's defense in depth response to an external or internal malevolent act. By utilizing that same approach in security of a preplanned strategy of protecting the radioactivity barriers, security, operations, and the emergency response organization can obtain synergy by having the same goal. That goal is to protect all the barriers through a systematic strategy that will limit the release of radioactivity to the environment to prevent exceeding the Part 100 limits.

Security contingency response will accomplish its function by defending critical redundant systems, structures, and components against an attempted attack using a layered defense in depth approach to protect the barriers to radioactivity release. Security in concert with operations personnel will take the necessary actions to mitigate any damage based on preplanned emergency response and defensive strategies.

Utilizing Part 100 criteria also provides a method of evaluating security of non core sources of radioactivity such as spent fuel both in the pool and in other locations.

Distribution: Mtg. Summary w/ Dated January 8, 2000

Hard Copy
PUBLIC
RSS R/F
OGC
ACRS
JBirmingham
RSkelton
JWhite, RI
RConte, RII
KBarr, RIII
GGood, RIV

EMail
SCollins/RZimmerman
BSheron
BBoger
FGillespe
BGallo
RRosano
AMadison
DHickman
JBirmingham
GTracy, EDO
ANelson, NEI

NRC / NEI Public Meeting
Dec. 2, 1999
SAFEGUARDS

Attendance Sheet

NAME	TITLE	ORGANIZATION
Dennis Gordon	Reactor Security Specialist	NRR
Lee Miller	Tech. Prog. Spec.	NRR
Gerard A. Bird	Mgr. Protection Services	FPL
Lonnie Wilkerson	Manage Security Svcs	NSP, Monticello NGS
Dan Martin	Manager Security Programs	Energy Northwest
Jim Ahvey	General Supervisor	Constellation Energy Group
Victor Dricks	NRC Public Affairs	OPA
Gregory Jaczko	staff	Rep. Ed Markey
Tom Clements	Ex. Director	Nuclear Control Institute
Dennis Schaefer	Security Inspector	Region II, NRC
David Thompson	Security Inspector	Region II, NRC
David N. Orrik	OSRE Team Leader	NRC (301) 415-3213
Richard P. Rosano	Chief, Reactor Safeguards	NRC, 301-415-3282
Robert E. Skelton	Senior Program Mgr.	" 301 415 3309
Jesse A. Arildsen	Senior Program Mgr	NRC 301-415-1026
Rich Enkeboll	" " "	NEI 202-739-8102
Jim Davis	Operations Director	NEI 202-739-8105
Lance Terry	Senior Nuclear Officer	TXU 254 817-897-8920
Robert Caruso	CHIEF, Operator Licensing/Human Performance Branch	301-415-1031
Ray Hsu	Nuc Engineer, NRR, RSS	301-415-3212
Andy Rayland	Phys. Protection Spec/nmss	nmss/FCSS/CID - 415-8102
John C. Brons	NEI	202-739-8121
Barry M. Saunders	ComEd / Supervisor, Nuclear Security Operations	ComEd (630)-663-6125
Thomas E. Malone	Plant Manager Security	4410 280-5314

Name	Title	Organization
Terry G. Sims	Nuclear Eng. & Licensing	Southern Company
Frank Gillespie	NRC Dep Div Dir	NRC
Robert T Allen	Mgr Reg Affairs	Con Edison IP2
Wayne Barber	McGraw-Hill — Reporter	
Craig Seaman	Director, Emergency Services	- APS / Palo Verde
A. David Huttie	Security Manager	- APS / Palo Verde
Ronald C. Teed	Security Manager	- R6E / Ginna
James A. Isom	INSPECTION PROGRAM BRANCH OPERATIONS ENGINEER	NRC
LES ENGLAND	Sr. Staff Engineer - Licensing	Entergy Operations
PAUL LEVENTHAL	President, ~~NAC~~	Nuclear Control Inst.

Due at NEI August 16, 1999

SPECIAL SECURITY SURVEY

From: Point of Contact:

(Plant name)
(Contact name)
(Contact phone)
(Contact e-mail)

This is an industrywide survey—your cooperation in responding is necessary. Please direct your questions to Rich Enkeboll, 202-739-8102, ree@nei.org.

Survey purpose: To obtain information for the Security Working Group for determining variances in regional and/or plant interpretation/execution that have resulted in Physical Security Plan (PSP) or other commitments. The plant responses will be examined in a comparison matrix to evaluate the following:

A. What security requirements/commitments the plant must comply with that are considered to be in excess of regulation, 10 CFR Part 73. [For this, do not consider the PSP as a regulatory basis.]

B. Requirement source—the mechanism (inspection result/inspector interpretation/Notice of Violation response/internal Quality Assurance, etc.) that caused plant acceptance of the requirement/commitment.

C. Impact on manpower/training/maintenance.

D. Proposed resolution—what would be the appropriate process to obtain relief—rule change/exemption/deletion/§ 50.54(p)/§ 50.90, etc.

From this Matrix the SWG will develop modification proposals for industry review and NRC concurrence/action to result in generic uniformity.

In the context of the above purpose, each licensee is requested to provide narrative information to the queries on the following pages:

1. What in your plan/procedures exceed § 73.55 requirements and does not contribute added value for prevention of radiological sabotage (consider Part 100 criteria as well as core damage)? What is the impact on manpower/training/maintenance?

2. What commitments do you have that are without specific rule basis? Identify the basis, e.g., response to NOV, QA, order, letter of commitment, Regional Assist or OSRE finding, etc.? What is the impact on manpower/training/maintenance?

3. Please identify commitments/activities known to exist at specific other companies and compare that information with your company's commitments/activities. Describe those that you consider to be:

a. More than required at other companies, and/or

b. Less than required at other companies?
How do they impact on manpower/training/maintenance?

4. What changes would you suggest to make security more like operations—limiting condition for operation (LCO), technical specification (TS), or other plant disciplines? How would you justify suggested changes.

5. What security modifications should the industry pursue for better resource efficiency/effectiveness while maintaining necessary security? Identify the item location—rule, generic letter, inspection criteria, etc., and include justification to support the desired change.

6. What regulatory requirements do you consider unimportant and should be eliminated. Provide justification/rationale.

NEI SWG SURVEY MATRIX

Prepared by SONGS Standard Configuration 11/30/1999

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1		Plant A	Plant B	Plant C	Plant D	Plant E	Plant F	Plant G	Plant H	Plant I	Plant J	Plant K	Plant L	Plant M	Plant N	Plant O	Plant P	Plant Q	Plant R	Plant S	Plant T	Plant U	Plant V	Plant W	Plant X	Plant Y	Plant Z	Pl
2	Region	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	**ISSUE**																											
4																												
5	Search train modifications/requirements	x					x									x	x	x										
6	Staffing @ 100% for total system failure					x								x				x	x	x			x	x	x				
7	Reporting	x													x	x	x						x	x	x				
8	PA/VA compensation		x	x	x	x	x	x		x	x				x	x	x						x	x	x				
9	Security patrols	x			x			x		x			x		x	x	x	x	x	x	x	x	x	x	x	x	x		
10	Lighting	x	x	x	x	x	x	x	x	x	x		x		x	x	x	x	x	x			x	x	x	x	x		
11	Vehicles in PA/searches/controls	x		x	x		x	x	x	x			x	x		x	x		x	x	x	x	x	x	x	x	x	x	x
12	Key card controls						x				x																		
13	VA/PA portal/barrier controls/checks			x	x		x	x			x			x			x	x			x					x	x	x	
14	Final PA access controls	x				x						x	x						x	x		x	x				x	x	x	
15	Weapons/special equipment			x		x						x																	
16	Insider threat											x																	
17	SI classification/program			x			x				x	x				x	x	x		x									
18	Alarm criteria/reporting/assessment					x	x															x							
19	Monitoring warehouse searches																												
20	Catastrophic compensatory measures																												
21	Securing vehicles in PA				x			x						x				x											
22	Records retention			x											x														
23	Alarm station operators/armed S/Os			x																							x		
24	Isolation zones			x																									
25	CAS/SAS manning/duties			x		x	x								x														
26	Visitors/escorting	x		x			x				x					x	x	x									x	x	x
27	Access authorization process			x							x	x				x	x		x										
28	OSRE commitments	x		x	x	x		x				x		x				x			x		x	x	x				
29	Independent spent fuel storage controls															x	x												
30	FFD																					x	x	x					
31	Inconsistent PSPs/SCPs											x									x								
32	Commitment cross reference library need					x				x	x	x		x	x	x	x	x	x	x			x	x	x			x	x
33	DBT details/response levels	x	x	x			x																						
34	Inconsistent compensatory measure	x										x																	
35	Breached barrier criteria (96x6 rule)											x			x														
36	Maint. tech escort requirements																												
37	Training/requalification/physicals			x		x	x					x		x	x				x				x	x	x		x		
38	Safeguards suspension authority															x	x												
39	Barrier construction											x		x		x	x												
40	Testing/frequency												x			x	x		x		x		x	x	x				
41	Lock/key change/control										x															x				
42	Inconsistent 50.54(p) & 50.90 guidance	x											x	x									x	x	x				
43	Extra pair eyeglasses																												
44	Annual review requirements																												
45	Grace period (e.g., +25%)																												
46	Inconsistent vulnerability guidance					x						x		x								x							
47	Material/personnel searches						x																x						
48	Performance based regulation																						x	x	x				
49	Tracking/trending	x							x			x														x			
50	Publish NRC exceptions/exemptions																												
51	NRC enforcement																												
52	Vehicle barriers											x																	
53	Definitions																												

	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX
1	Plant AA	Plant AB	Plant AC	Plant AD	Plant AE	Plant AF	Plant AG	Plant AH	Plant AI	Plant AJ	Plant AK	Plant AL	Plant AM	Plant AN	Plant AO	Plant AP	Plant AQ	Plant AR	Plant AS	Plant AT	Plant AU	
2	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4		
3																						
4																						
5																						
6			x	x	x	x	x	x	x		x	x			x			x	x	x		
7	x				x	x	x	x	x	x	x	x		x	x		x	x		x		
8	x					x	x	x		x	x	x			x		x	x		x		
9	x		x		x	x	x	x	x	x	x	x	x		x		x	x		x		
10					x	x	x		x	x	x	x	x		x		x		x	x		
11	x	x			x	x	x	x	x	x	x	x	x	x	x		x	x	x	x		
12	x	x	x		x	x	x	x	x	x	x	x	x	x			x	x		x		
13					x				x			x			x							
14	x	x	x		x	x	x	x				x	x				x	x		x		
15	x					x	x					x					x	x		x		
16	x		x		x	x	x	x				x								x		
17												x	x				x			x		
18	x		x	x		x	x		x	x	x	x	x	x	x	x	x	x	x	x		
19		x	x		x	x	x															
20		x																				
21		x															x					
22		x				x	x		x					x						x		
23						x	x															
24																						
25						x												x				
26	x		x	x		x	x	x	x	x					x			x		x		
27	x					x											x	x		x		
28	x																					
29				x	x	x	x	x	x		x			x	x		x			x		
30				x												x				x		
31																x						
32	x															x	x			x		
33																x						
34	x		x		x	x	x	x	x		x	x		x	x	x	x	x	x	x		
35	x		x		x	x	x	x	x	x	x	x	x		x		x	x		x		
36					x			x		x		x					x	x		x		
37													x				x					
38	x					x	x		x									x		x		
39															x							
40					x	x	x													x		
41					x	x	x			x								x	x	x		
42	x																					
43	x							x		x					x					x		
44	x					x	x		x								x			x		
45	x																			x		
46																				x		
47					x			x	x	x						x	x			x		
48			x		x	x	x		x		x				x					x		
49						x	x				x						x			x		
50																		x				
51																		x		x		
52																	x	x		x		
53						x	x						x							x		

SCREENING CRITERIA FORM
(ASSESSMENT OF ACCEPTABILITY OF 10 CFR 50.54(p) PLAN CHANGE)

SECTION/TITLE: Material Searches

PROPOSED COMMITMENT:

NEI proposes to modify licensee methods employed to search material and packages, and subsequent control of these items once inside the Protected Area (PA). Specifically, the plan changes define "adequate search" as it applies to the inspection of "generic (hazardous and non-hazardous)" products prior to admittance to the PA. NEI proposes applicable all licensee Physical Security Plans (PSP) be supplemented as follows, where applicable:

Generic products that if opened could constitute a danger to the individual performing the search or would render the material unusable or contaminated are considered adequately searched when:

1. The exterior of the container is verified not to have been compromised, and
2. If sealed in the manufacturing process, the seal is not compromised, and
3. The delivery is expected, and
4. The item is identified and accepted by a licensee badged person, other than the deliverer, who is familiar with the contents.

Generic products sealed in the manufacturing process are considered adequately searched when:

1. The exterior of the container is verified not to have been compromised, and
2. The manufacturer's seal is not compromised, and
3. The delivery is expected, and
4. The item is identified and accepted by a licensee badged person, other than the deliverer, who is familiar with the contents.

Packages and materials unable to be searched in accordance with these requirements shall not be allowed into the PA unless they meet the requirements of, and are controlled in accordance with search exempted material as defined by the licensee's PSP.

IMPACT ON EFFECTIVENESS OF A GENERIC PLAN:

1. ☐ Yes ■ No DOES THIS CHANGE, DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

SCREENING CRITERIA FORM
(ASSESSMENT OF ACCEPTABILITY OF 10 CFR 50.54(p) PLAN CHANGE)

IMPACT ON EFFECTIVENESS OF A GENERIC PLAN (cont'd):

2. ☐ Yes ■ No WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73.55 TO PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1(A)?

Rationale: This change supplements the NUREG-0908, "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans," guidance and further defines "adequate search" for generic items and allows these items to be released to the PA when the required searches and verifications have been completed. These controls take into consideration the safety of the security force members and the operational necessity for processing materials in the PA. This consideration of safety and operational necessity is in accordance with 10 CFR 73.55(d)(3), "Access Requirements."

The likelihood that a generic item contains concealed contraband for the PA is minimal. During the manufacturing of generic items, the producer is not aware of the material's final destination. The lack of this crucial information is in itself sufficient assurance to rule out this possibility as a credible threat. The ability to smuggle contraband into the PA would be further complicated by the fact that generic products could typically be routed through any of a number of distribution networks, adding additional assurance the manufacturer would have little or no chance of directing material to a specific destination. Therefore, the ability to plan and implement the concealment of contraband (firearms, explosives, incendiary devices, or other items which could be used for radiological sabotage) for entry into the PA is neither feasible nor probable.

SCREENING CRITERIA FORM
(ASSESSMENT OF ACCEPTABILITY OF 10 CFR 50.54(p) PLAN CHANGE)

IMPACT ON EFFECTIVENESS OF A GENERIC PLAN (cont'd):

Conversely, products which have been produced specifically for the licensee have a greater probability that contraband could be concealed in them for access into the PA. During the production of these types of material the producer is aware of its destination and could potentially conceal contraband within the shipping container. For this reason, these packages and materials will be searched and controlled in accordance with existing PSP requirements.

These methods are different than those previously used in that generic material which has been searched in accordance with guidance above would be released into the PA and would not be required to be maintained in a locked area. NEI is aware that these methods have been previously reviewed and approved by the NRC.

These changes would not decrease the effectiveness of the access requirements as described in 10 CFR 73.55(d). The commitment to search packages and materials in accordance with this proposed change has no impact on the effectiveness of the physical security organization [73.55(b)], physical barriers [73.55(c)], detection aids [73.55(e)], communication requirements [73.55(f)], testing and maintenance [73.55(g)], or response requirements [73.55(h)].

3. ☐ Yes ☐ No FOR ANY LICENSEE THAT HAS NRC-APPROVED SECURITY PLAN COMMITMENTS AS ALTERNATIVES TO ONE OR MORE OF THE REQUIREMENTS OF 10 CFR 73.55(b) THROUGH (h): DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED TO PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1(a)?

SCREENING CRITERIA FORM
(ASSESSMENT OF ACCEPTABILITY OF 10 CFR 50.54(p) PLAN CHANGE)
SECTION/TITLE:

PROPOSED COMMITMENT:

Licensees' current plans specify that security audits, physicals, and weapons training [required by 10 CFR 73.55(g)(4) and 10 CFR 73.55, Appendix B] be completed one (1) year or less after the audit, physical examination, or training was last accomplished. This results in the periodic audits, requalification physicals, and requalification training due dates being adjusted each year and the audits and requalification requirements, over a period of years, being completed more than once each 12 months. A similar situation exists with security surveillance requirements, e.g., access list updating at least once every thirty-one (31) days [10 CFR 73.55(d)(7)(I)], and intrusion alarm testing to be performed at least once every seven (7) days [10 CFR 73.55(g)(2)].

This change provides scheduling latitude in performing annually required security audits, physicals, and weapons training, and periodic access authorization list updating and security equipment testing. It allows use of the Technical Specification Surveillance Requirement (SR) 3.0.2 grace period to provide flexibility in meeting security commitments. The revised commitment would allow fixed dates in the plan with a provision for extending, e.g., the audit, physical, training, access list updating, and security equipment periodic testing, intervals beyond the required 1 year, 31 day, or 7 day frequency (i.e., a maximum allowable extension not to exceed 25% of the surveillance interval could be applied).

SCREENING CRITERIA FORM
(ASSESSMENT OF ACCEPTABILITY OF 10 CFR 50.54(p) PLAN CHANGE)
IMPACT ON EFFECTIVENESS OF A GENERIC PLAN:

1. ☑ Yes ☐ No DOES THIS CHANGE, DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

2. ☑ Yes ☐ No WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73.55 TO PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1(A)?

Rationale: There would no impact on performance capabilities of the security program or security officer weapons proficiency. Audits, physicals, and security training would still be conducted on an annual basis with only minor variations. Similarly, periodic access authorization list updating and security equipment testing would still be conducted on their required regulatory frequency with only minor variations.

This change is similar to that proposed in Generic Letter 95-08, "10 CFR 50.54(p) Process For Changes To Security Plans Without Prior NRC Approval," Attachment 2, which contains 10 examples of previously accepted changes made by licensees without NRC approval pursuant to 10 CFR 50.54(p). Specifically, this is similar to Example VII, titled, "Requalification Schedule."

SCREENING CRITERIA FORM
(ASSESSMENT OF ACCEPTABILITY OF 10 CFR 50.54(p) PLAN CHANGE)

3. ☐ Yes ☐ No FOR ANY LICENSEE THAT HAS NRC-APPROVED SECURITY PLAN COMMITMENTS AS ALTERNATIVES TO ONE OR MORE OF THE REQUIREMENTS OF 10 CFR 73.55(b) THROUGH (h): DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED TO PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1(a)?

SCREENING CRITERIA OUTLINE
ASSESSMENT OF ACCEPTABILITY OF
10 CFR 50.54(p) SECURITY PLAN CHANGES

GENERIC NUCLEAR STATION SECURITY PLAN

REVISION SUMMARY:

A change has been made to the commitment to provide immediate compensatory measures for degraded vital area doors. Instead, a 72-hour security action statement will be entered, during which the problem must be corrected. Vital area alarm response requirements have modified.

Major Changes:

Paragraph 5.3, Vital Area Intrusion Detection Hardware is changed to replace the commitment to provide immediate and continuous compensatory measures for loss of a vital area alarm or lock. The requirement to respond to all vital area alarms has been deleted. Response is required only when there is a concurrent, unresolved protected area alarm.

IMPACT UPON EFFECTIVENESS OF THE PLAN

1. ≤ Yes P No Does this change delete or contradict any regulatory requirement?

   Rationale: Yes, this change is contrary to the requirement of 10 CFR 73.55(d)(7)(I)(D) to lock and protect with an activated intrusion alarm system all unoccupied vital areas. It also contradicts the requirement of 10 CFR 73.55(e)(3) that all emergency exits in each protected and vital area be alarmed. An exemption request has been approved under the provisions of 10 CFR 73.5, "Specific Exemptions." The standards of the rule are satisfied in that the change will not endanger life or property or the common defense and security, (as shown in the rationale for items 2 and 3 below), and is the public interest by contributing to the reduction of overhead costs associated with power generation.

2. ≤ Yes P No Would the change decrease the overall level of Security system performance as described in Paragraphs (b) through (h) of 10 CFR 73.55 to protect with the objective of high assurance against the design basis threat of radiological sabotage?

   Rationale: The overall level of security system performance would not be decreased during a "security action statement," because simultaneous lock and alarm failures rarely, if ever, occur, the door would always be locked or alarmed. In the

event of an concurrent, unresolved perimeter alarm, the response requirement would be reinstated, providing the previous level of assurance against unauthorized entry to a vital area. Video capture systems make it possible to positively determine whether a perimeter alarm is the result of an unauthorized entry.

Vital area alarms are, with extremely rare exceptions, caused by inadvertent actions of persons authorized access to the area. These include holding a door open too long; grabbing and pulling on the door handle before the badge is read, etc.

3. ≤ Yes P No For any licensee that has NRC-approved Security Plan commitments as alternatives to one or more of the requirements of 10 CFR 73.55 Paragraphs (b) through (h): Does this change decrease the overall level of security system performance needed protect with the objective of high assurance against the design basis threat of radiological sabotage?

Rationale: The Security Plan has one provision approved as an alternative to 10 CFR 73.55 Paragraphs (b) through (h), that allows non-employees to take home their photobadges. The changes to the plan, do not decrease the overall protection provided to safety-related equipment. Lock and alarm failures are random, short-term events, not predictable or exploitable by a potential adversary. There is no visual indication of the failure. It is concluded that the change does not decrease the overall ability to protect the Generic Nuclear Station from the Design Basis Threat of radiological sabotage.

Prepared by _____ Title _____ Date _____

Reviewed by _____ Title _____ Date _____

Approved by: _____Title _____ Date _____

Evaluation of Proposed Change to Site Security Plan
(Assessment of Acceptability of 10 CFR 50:54(P) Plan Change)

The following changes are proposed for the Station Security Plan. All changes comply with the requirements of 10 CFR 50:54 (p).The guidance provided in NRC Generic Letter 95:08 has been applied and documented accordingly.

Sections:

Identify Applicable Plan Sections

Proposed Change:

Protected Area patrols shall be conducted at least once per 12-hour shift.

note: Vital area patrols are not required.

1. DOES THIS CHANGE DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

☐ Yes ☒ No

10 CFR 73:55 (c) (4) *Physical Barriers* states " Detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier shall assure that adequate response by the security organization can be initiated. *All exterior areas within the protected area shall be periodically checked to detect the presence of unauthorized persons, vehicles or materials."*

2. WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73:55 TO PROTECT WITH THE OBJECTIVE OF HIGH PERFORMANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73:1(a)?

☐ Yes ☒ No

Protected Area Perimeters are monitored by CCTV or manned Defensive Positions and all alarms are responded to accordingly. Barrier integrity, proper isolation zone clearances and adequate lighting is maintained through these surveillance features in place.

3. DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1 (a)?

☐ **Yes** ☒ **NO**

The Security Plan has taken no exceptions to 10 CFR 73:55 (b) through (h). A periodic check of Protected Area barriers will be conducted once every 12 hours. Vital Areas will be checked at least once each 12 hours.

These changes do not decrease the effectiveness of the security force to assess and respond to threats and any acts of radiological sabotage. This proposed change has no impact on the effectiveness of the physical security organization {73:55 (b)}, physical barriers {73:55 (c)},detection aids {73:55 (e)}, communications equipment {73:55 (f)}, testing and maintenance {73:55 (g)}, or response requirements {73:55 (h)}.

Evaluation of Proposed Change to Site Security Plan
(Assessment of Acceptability of 10 CFR 50:54(P) Plan Change)

The following changes are proposed for the Station security Plan. All changes comply with the requirements of 10 CFR 50:54 (p). The guidance provided in NRC Generic Letter 95:08 has been applied and documented accordingly.

Sections:
Identify Applicable Plan Sections

Proposed Change: Add one or more of the following to the lighting commitment;

"Shadows may reduce the illumination levels in certain areas. Patrol Officers equipped with flashlights periodically inspect these areas during hours of darkness," or low light CCTV's.

"Areas of illumination less than 0.2 foot-candles may be permitted, provided the average light level measured at six points equidistant on the circumference of a circle of two foot diameter from the point of minimum illumination shall not be less than 0.2 foot-candles."

"Exceptions to illumination requirements are vehicles, trailers, and other mobile devices, maintenance equipment, materials storage areas or similar obstructions that cause shadows or dark areas."

"During the construction of facilities, outages and maintenance operations, dark areas or shadows may exist in exterior areas of the protected area. Scaffolding, ladders or other access devices installed to provide a ready means of access to the tops of buildings in excess of eighteen (18) feet in height not provided with 0.2 foot-candles of illumination may be allowed in the protected area. These conditions may exist during construction or maintenance activities requiring access to normally inaccessible tops of buildings."

1. DOES THIS CHANGE DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

☐ **Yes** ☒ **No**

10 CFR 73:55 (c) (5) states " Isolation zones and all exterior areas within the protected area shall be provided with illumination sufficient for the monitoring and observation requirements of paragraphs (c) (3), (c) (4), and (h)(4) of this section, but not less than 0.2 foot-candle measured horizontally at ground level."

C (3) Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and shall be of sufficient size to permit observation of the activities of people on either side of that barrier in the event of its penetration. If parking facilities are provided for employees or visitors, they shall be located outside the isolation zone and exterior to the protected area barrier.
(4) Detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier shall assure that adequate response by the security organization can be initiated. All exterior areas within the protected area shall be periodically checked to detect the presence of unauthorized persons, vehicles, or materials.

H (4) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, material access area, or a vital area; or upon evidence or indication of intrusion into a protected area, a material access area, or a vital area, the licensee security organization shall:

(i) Determine whether or not a threat exists,

(ii) Assess the extent of the threat, if any,

2. WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73:55 TO PROTECT WITH THE OBJECTIVE OF HIGH PERFORMANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73:1(a)?

☐ **Yes** ☒ **No**

This change does not decrease the lighting requirements needed for assessment at the perimeter or in isolation zones.

3. DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1 (a)?

☐ **Yes** ☒ **NO**

This change does not decrease the overall effectiveness of the security organization to assess and properly respond to threats of radiological sabotage.

Evaluation of Proposed Change to Site Security Plan
(Assessment of Acceptability of 10 CFR 50:54(P) Plan Change)

The following changes are proposed for the Station security Plan. All changes comply with the requirements of 10 CFR 50:54 (p). The guidance provided in NRC Generic Letter 95:08 has been applied and documented accordingly.

DRAFT

Sections:

Identify Applicable Plan Sections

Termination of employment is under favorable conditions and circumstances, the individual's security badge must be restricted from the Security Access Control system within forty-eight (48) hours after notification to security of the termination.

1. DOES THIS CHANGE DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

☐ **Yes** ☒ **No**

10 CFR 73:55 (d) (7) (C) states" Revoke, in the case of an individual's involuntary termination for cause, the individual's unescorted access and retrieve his or her identification badge and other entry devices, as applicable, prior to or simultaneously with notifying this individual of his or her termination."

2. WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73:55 TO PROTECT WITH THE OBJECTIVE OF HIGH PERFORMANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73:1(a)?

☐ **Yes** ☒ **No**

Terminations under favorable conditions do not warrant an immediate retrieval of the badge and access device due to it's favorable nature. Adequate time should be allowed to retrieve the individual's badge and access device and delete it from the site's access system.

3. DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1 (a)?

☐ **Yes** ☒ **NO**

The security Plan takes no exceptions to 10 CFR 73:55 (b) through (h). The proposed change does not delete or contradict any requirement of 10 CFR 73:55 (b) through (h).

These changes do not decrease the effectiveness of the access requirements described in 10 CFR 73:55 (d). This proposed change has no impact on the effectiveness of the physical security organization {73:55 (b)}, physical barriers {73:55 (c)},detection aids {73:55 (e)}, communications equipment {73:55 (f)}, testing and maintenance {73:55 (g)}, or response requirements {73:55 (h)}.

Evaluation of Proposed Change to Site Security Plan
(Assessment of Acceptability of 10 CFR 50:54(P) Plan Change)

The following changes are proposed for the Station security Plan. All changes comply with the requirements of 10 CFR 50:54 (p). The guidance provided in NRC Generic Letter 95:08 has been applied and documented accordingly.

Sections:
Identify Applicable Plan Sections

Proposed Change:

Material/equipment may be sealed (in containers) prior to exiting the Protected Area or searched and sealed at a location exterior to the Protected Area. Sealed material/equipment may be stored exterior to the Protected Area until entry into the Protected Area is required provided the material/ equipment is stored in a limited access area or is periodically patrolled. This change allows material to be transferred from one site to another without addition search at the receiving site.

1. DOES THIS CHANGE DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

☐ **Yes** ☒ **No**

10 CFR 73:55 (d) (3) states " All packages and material for delivery into the protected area shall be checked for proper identification and authorization and searched for devices such as firearms, explosives and incendiary devices or other items which could be used for radiological sabotage, prior to admittance into the protected area , except those Commission approved delivery and inspection activities specifically designated by the licensee to be carried out within vital or protected areas for reasons of safety, security or operational necessity."

This requirement is met by the initial search and proper storage of items with a security seal.

2. WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73:55 TO PROTECT WITH THE OBJECTIVE OF HIGH PERFORMANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73:1(a)?

☐ **Yes** ☒ **No**

This change supplements the NUREG –0908, "Acceptance Criteria for the Evaluation of Nuclear Power reactor Security Plans," guidance and further defines "adequate search" for materials/equipment and allows these items to be released to the protected area when the required exterior searches and seal verifications have been completed. These controls take into consideration the safety of the security force members and the operational necessity for processing materials into the protected area. This consideration of safety and operational necessity is in accordance with 10 CFR 73:55 (d) (3), "Access Requirements."

These changes do not decrease the effectiveness of the access requirements described in 10 CFR 73:55 (d). The commitment to search packages and materials in accordance with this proposed change has no impact on the effectiveness of the physical security organization {73:55 (b)}, physical barriers {73:55 (c)},detection aids {73:55 (e)}, communications equipment {73:55 (f)}, testing and maintenance {73:55 (g)}, or response requirements {73:55 (h)}.

3. DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1 (a)?

☐ **Yes** ☒ **NO**

These changes do not decrease the effectiveness of the access requirements described in 10 CFR 73:55 (d). The commitment to search packages and materials in accordance with this proposed change has no impact on the effectiveness of the physical security organization {73:55 (b)}, physical barriers {73:55 (c)},detection aids {73:55 (e)}, communications equipment {73:55 (f)}, testing and maintenance {73:55 (g)}, or response requirements {73:55 (h)}.

EVALUATION OF PROPOSED CHANGES TO SECURITY PLANS

SECTION/TITLE: Remote Search Process

PROPOSED COMMITMENT:

Current licensee Security Plans specify that searches will be conducted on all personnel, material, and vehicles prior to their entry into the Protected Area, in accordance with 10CFR73.55(d). Although not specified in the regulations or the plan, the searches are usually conducted immediately prior to entry, at the appropriate access point to the Protected Area. For materials that are required in large quantities, such as refueling and major maintenance equipment, this results in a major impact on the Security work hours dedicated to the search process and causes delays in the activities that require the materials in question. Many of the items brought into the Protected Area during refueling outages have been loaded at another licensee facility or have been loaded at the same licensee facility during the previous outage.

This changes clarifies the location of where searches may take place and provides latitude as to when the search occurs. It also provides for the use of a unique system to seal packages and containers after the searches are conducted. The process is controlled and documented. The materials that arrive in large carriers that have been searched and sealed at the point of loading may be granted access without searching again. An intact seal assures the licensee that the no prohibited item is entering the Protected Area. A seal that was disturbed requires the licensee to search the material again prior to entry. This practice is currently being used at numerous facilities in the nuclear industry.

IMPACT UPON EFFECTIVENESS OF A GENERIC PLAN:

1. ☐YES ■ NO — DOES THIS CHANGE DELETE OR CONTRADICT ANY REGULATORY REQUIREMENT?

2. ☐YES ■ NO — WOULD THE CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE AS DESCRIBED IN PARAGRAPHS (b) THROUGH (h) OF 10 CFR 73.55 TO PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1(a)?

   Rationale: This change to the access control process does not decrease the effectiveness of the overall Security program. The provision for utilizing searches conducted at a previous time allows the material access process at peak times to be accomplished in a more efficient and organized manner, which enhances both Security and plant operations.

EVALUATION OF PROPOSED CHANGES TO SECURITY PLANS

SECTION/TITLE: Remote Search Process (continued)

3. ☐YES ■ NO

FOR ANY LICENSEE THAT HAS NRC-APPROVED SECURITY PLAN COMMITMENTS AS ALTERNATIVES TO ONE OR MORE OF THE REQUIREMENTS OF 10 CFR 73.55(b) THROUGH (h): DOES THIS CHANGE DECREASE THE OVERALL LEVEL OF SECURITY SYSTEM PERFORMANCE NEEDED TO PROTECT WITH THE OBJECTIVE OF HIGH ASSURANCE AGAINST THE DESIGN BASIS THREAT OF RADIOLOGICAL SABOTAGE AS STATED IN 10 CFR 73.1(a)?

Generic Letter 95-08, "10CFR50.54(p) Process for Changes To Security Plans Without Prior NRC Approval," Attachment 3, describes examples of unacceptable changes proposed by licensees without NRC approval pursuant to 10CFR50.54(p). Item 3 describes a proposal to store previously searched material in an unsecured warehouse prior to entry into the PA. This proposal was categorized as a decrease in effectiveness of the plan. The change described in the above submittal meets the requirements of 10CFR73.55(d), because the seal maintains the integrity of the search, regardless of the time of entry. This submittal is not the same as described in the rejected example.

Evaluation of Proposed Change to Site Security Plan

The following changes are proposed for the Station Security Plan. All changes have been organized according to type and all proposed changes comply with the requirements of 10 CFR 50.54 (p). The guidance provided in NRC Generic Letter 95-08 has been applied to each change and documented accordingly.

Sections:
1.1.1 – Applicable Plan Section(s)
1.1.2 – Applicable Plan Section(s)

Amends the minimum manpower requirements allowing for an unplanned reduction provided that immediate action is taken to restore required manpower composition as follows:

If failures of the security system occur which require additional personnel to effectively compensate for the failure(s), or in the event of an injury, illness, or emergency situation which reduces minimum staffing levels for a period greater than ten (10) minutes, security supervision will call-out security personnel to restore the shift level to the required minimum. Shift levels will be restored within two (2) hours and ten (10) minutes from the time of discovery.

1. **Does this change or delete or contradict any regulatory requirement?**

   ☐ **Yes** ☑ **No**

   Requirements for minimum manpower are described in 10 CFR 73.55 (h)(3). It is the licensee's intention to always meet the minimum requirements of § 73.55 (h)(3). However, an unforeseen situation could occur that results in a reduced shift complement. In an effort to address this unpredictable and unavoidable possibility, it is prudent to describe actions to be taken to correct any manpower deficiency.

   10 CFR 73.55 does not address compensatory measures to be applied for this type of an event. Guidance within Regulatory Guide 5.62. Reporting of Physical Security Events, states that when the minimum number of security personnel become unavailable the following applies: ***"These events do not have to be reported within one hour if properly compensated for in a timely manner; however, they have to be reported within 24 hours."*** This plan change defines the "timely manner" acceptable for restoring the minimum manpower level.

   Additionally, the NRC has approved similar changes at other Stations.

2. **Would the change decrease the overall level of security system performance as described in paragraphs (b) through (h) of 10 CFR 73.55 to protect with the objective of high assurance against the design basis threat of radiological sabotage as described in 10 CFR 73.1 (a)?**

☐ **Yes** ☑ **No**

Because the situation(s) resulting in reduced manpower are not predictable, an adversarial force would not be able to identify the parameters necessary to carry out an act of radiological sabotage concurrent with a manpower reduction. The frequency of these situations occurring is limited and temporary. Aggressive corrective measures have been established making it unrealistic for an adversary to exploit any decrease in minimum security manpower. Based on the short duration that a manpower deficiency would exist, overall security system performance is not decreased.

3. **For any licensee that has NRC-approved security plan commitments of 10 CFR 73.55 (b) through (h): Does this change decrease the overall level of security system performance needed to protect with the objective of high assurance against the design basis threat of radiological sabotage as stated in 10 CFR 73.1 (a)?**

☐ **Yes** ☑ **No**

The security plan has taken no exceptions to 10 CFR 73.55 (b) through (h). Because the situations that would result in a temporary manpower decrease are not predictable, identifiable, or exploitable, protection against the design basis threat is maintained. The proposed change does not delete or contradict any requirement of 10 CFR 73.55 (b) through (h).

Evaluation of Proposed Change to Site Security Plan

The following changes are proposed for the Station Security Plan. All changes have been organized according to type and all proposed changes comply with the requirements of 10 CFR 50.54 (p). The guidance provided in NRC Generic Letter 95-08 has been applied to each change and documented accordingly.

Sections:
1.1.1 – Applicable Plan Section(s)
1.1.2 – Applicable Plan Section(s)

Adds the ability to utilize Response Team Members to perform compensatory measures for Perimeter Intrusion Detection or CCTV failure.

With the advent of the outside defensive strategy, Response Team Members can be relocated to strategic positions to provide detection/assessment capability while still providing required protection against the design basis threat as described in 10 CFR 73.1. Moving Response Team Members to positions that allow for earlier interdiction of an adversarial force while providing first-hand detection and assessment capability actually increases the ability to defend the station.

1. **Does this change or delete or contradict any regulatory requirement?**

   ☐ **Yes** ☑ **No**

   This change still meets the requirements for perimeter, barrier observation and response team capability as described in 10 CFR 73.55. This change addresses compensatory measures on the perimeter whenever alarm and/or camera assessment capabilities are reduced. Justification for this change is based on the comparison of the roving patrols capability vs. the capability of stationary officers ability to adequately detect and assess potential threats to the station that originate at the perimeter.

   - Quantity of patrols: Roving patrols continuously evaluate portions of the perimeter that equate to a 100 percent check of the perimeter. This plan change places officers in strategic locations in order to optimize the observation of delay barriers. In addition, these positions are located such that they may observe a high percentage of the perimeter fence and large areas of the Protected Area. This officer can observe (section by section) the Protected Area and their position cannot be determined as could a roving, vehicle, or foot patrol.

- Quality of patrols: The quality of patrols is considered equal to that of the stationary positions. The vehicle patrol, when stopped, allows the officer to concentrate their efforts on observation and evaluation. The vehicle patrol can modify the angle and distance to an object where as the stationary officer is dependent on the use of magnification aids and the field of vision available. Environmental conditions that reduce the quality of vision to an extent that the stationary officer could not see the entire scope of the designated area are considered to be minimal, random, and unpredictable. The elevated patrol and/or a continuous roving patrol would, as stated previously, assist in providing assessment capabilities.

- This change provides greater assessment capability of the Protected Area, provides greater protection to the officers, and focuses the officers' task to assessment and reporting.

2. **Would the change decrease the overall level of security system performance as described in paragraphs (b) through (h) of 10 CFR 73.55 to protect with the objective of high assurance against the design basis threat of radiological sabotage as described in 10 CFR 73.1 (a)?**

☐ **Yes** ☑ **No**

Refer to itemized responses below:

- 10 CFR 73.55 (b) details the requirements of the physical security organization and requirements for the retention of records—this change does not affect any administrative requirement of the 10 CFR 73.55.

- Physical barriers are detailed in 10 CFR 73.55 (c)—there are no changes to the physical barriers at the station. 10 CFR 73.55 (c) (4) does address detection of penetration or attempted penetration of the Protected Area or isolation zone in order to assure that the security organization can be initiated. The change to the defensive strategy places officers in the Protected Area on a full-time basis and virtually eliminates the question of *"initiation of adequate response of the security force"*. 10 CFR 73.55 (c) (4) describes a periodic observation of the perimeter fence and the Protected Area—a periodic check of the perimeter and Protected Area will continue to be performed. No other sections of 10 CFR 73.55 (c) apply or are affected by this change.

- 10 CFR 73.55 (d) details the requirements for access—all actions being taken to satisfy this requirement remain unaffected by this change.

- 10 CFR 73.55 (e) details detection aids—all actions taken to satisfy this requirement remain unaffected by this change.

- 10 CFR 73.55 (f) details required communication equipment—all actions taken to satisfy this requirement remain unaffected by this change.

- 10 CFR 73.55 (g) details testing and maintenance requirements—all actions taken to satisfy this requirement remain unaffected by this change.

- 10 CFR 73.55 (h) details the response requirement and specifically refers to the requirements of 10 CFR 73, Appendix C. This change capitalizes on the strategic placement of security officers in order to observe and monitor the perimeter and defensive barriers.

3. **For any licensee that has NRC-approved security plan commitments of 10 CFR 73.55 (b) through (h): Does this change decrease the overall level of security system performance needed to protect with the objective of high assurance against the design basis threat of radiological sabotage as stated in 10 CFR 73.1 (a)?**

☐ **Yes** ☑ **No**

The specific answers to 10 CFR 73.55 (b) through (h) are addressed above in Section #2.

Evaluation of Proposed Change to Site Security Plan

The following changes are proposed for the Station Security Plan. All changes have been organized according to type and all proposed changes comply with the requirements of 10 CFR 50.54 (p). The guidance provided in NRC Generic Letter 95-08 has been applied to each change and documented accordingly.

Sections:
1.1.1 – Applicable Plan Section(s)
1.1.2 – Applicable Plan Section(s)

Eliminates the requirement to remove/control vehicle ignition keys along with "key-check" patrols of vehicles located within the Protected Area. 10 CFR 73.55 (d)(4) requires the licensee to *"exercise positive control of vehicles within the Protected Area to assure that they are operated by an authorized person for authorized purposes."*

1. **Does this change or delete or contradict any regulatory requirement?**

   ☐ **Yes** ☑ **No**
   Requirements for control of designated vehicles are described in 10 CFR 73.55 (d)(4). The basis of the requirement is to protect against the possibility of an adversary utilizing a vehicle as a means to gain proximity or access to a Vital Area. This change does not delete or contradict any regulatory requirement, as the methods for maintaining positive control of vehicles are not defined within § 73.55. The periodic "key-checks" are only performed on the basis of an interpretation of the requirement.

2. **Would the change decrease the overall level of security system performance as described in paragraphs (b) through (h) of 10 CFR 73.55 to protect with the objective of high assurance against the design basis threat of radiological sabotage as described in 10 CFR 73.1 (a)?**

   ☐ **Yes** ☑ **No**
   Instances when a key may be left with a vehicle are not predictable, identifiable, or exploitable. Therefore, the presumption that an adversary would take the time necessary to search for vehicle keys is not realistic. The potential for an insider threat is not valid because "the insider" would already have a reasonable access to vehicle keys. Based on the random and unexpected circumstances related to controlling vehicle keys, eliminating the periodic patrol does not decrease the overall level of security system performance.

3. **For any licensee that has NRC-approved security plan commitments of 10 CFR 73.55 (b) through (h): Does this change decrease the overall level of security system performance needed to protect with the objective of high assurance against the design basis threat of radiological sabotage as stated in 10 CFR 73.1 (a)?**

☐ **Yes** ☑ **No**

The security plan has taken no exceptions to 10 CFR 73.55 (b) through (h). Based on the intrusion detection aids and defensive strategy, periodically searching for keys inadvertently left inside a vehicle does not add an increased protection factor. Prior to having an opportunity to find (and possibly compromise) vehicle keys, an individual attempting radiological sabotage will have to pass through other defensive layers of security. These security measures are designed to protect against a Part 100 radiological release and/or core damage; therefore, the proposed change does not delete or contradict any requirement of 10 CFR 73.55 (b) through (h).

SCREENING CRITERIA OUTLINE
ASSESSMENT OF ACCEPTABILITY OF
10 CFR 50.54(p) SECURITY PLAN CHANGES

GENERIC NUCLEAR STATION SECURITY PLAN

REVISION SUMMARY:

Changes have been made to the controls imposed upon vehicles to delete the requirement to escort any vehicle searched in accordance with the 10 CFR 73.55(d)(4) and driven by a person granted unescorted access pursuant to 10 CFR 73.56.

Major Changes: escorted by a person with Unescorted Access

Paragraph 4.2.2.1 - Vehicle Access Policy: Deletes the phrases "Designated Licensee Vehicle" and "Non-designated Vehicle." Deletes the requirement to disable unattended vehicles. Adds a provision that vehicles driven by persons granted unescorted access to the protected area do not require an escort unless transporting a category of cargo that must be escorted.

Paragraph 4.2.2.2 - Designated Licensee Vehicles: The section is deleted.

IMPACT UPON EFFECTIVENESS OF THE PLAN

1. P Yes No ≤ Does this change delete or contradict any regulatory requirement?

   Rationale: Yes, this change is contrary to the requirements of 10 CFR 73.55(d)(4) regarding designated licensee vehicles and vehicle escorting requirements. An exemption request has been approved under the provisions of 10 CFR 73.5, "Specific Exemptions." The standards of the rule are satisfied in that the change will not endanger life or property or the common defense and security, (as shown in the rationale for items 2 and 3 below), and is the public interest by contributing to the reduction of overhead costs associated with power generation.

2. ≤ Yes P No Would the change decrease the overall level of Security system performance as described in Paragraphs (b) through (h) of 10 CFR 73.55 to protect with the objective of high assurance against the design basis threat of radiological sabotage?

   Rationale: The overall level of security system performance would not be decreased. Searched vehicles driven by a screened person granted unescorted access to a nuclear

plant do not pose a threat to safety related equipment at the Generic Nuclear Station. This equipment is within seismically qualified structures. Vital area vehicle access doors are of massive construction and could not be penetrated by a vehicle.

Given that vehicles do pose a threat to vital equipment, there is no greater security threat posed by vehicles that are kept onsite than those that may enter for a brief period. The vehicles in either case have been properly searched and driven by screened persons determined with high assurance to be trustworthy and reliable. These persons are subject to continual behavior observation and fitness-for -duty program requirements.

The rationale cited above extends to deleting the requirement to remove keys or otherwise secure unattended vehicles. Vehicles do not pose a threat, have been searched, and are within the protected area where they are accessible only to screened or escorted persons. Securing the vehicle therefore yields no security benefit.

The controls inherent in properly searching all vehicles permitted entry which are operated by persons granted unescorted access continue to provide high assurance protection against execution of the Design Basis Threat.

3. ≤ Yes P No For any licensee that has NRC-approved Security Plan commitments as alternatives to one or more of the requirements of 10 CFR 73.55 Paragraphs (b) through (h): Does this change decrease the overall level of security system performance needed protect with the objective of high assurance against the design basis threat of radiological sabotage?

Rationale: The Security Plan has one provision approved as an alternative to 10 CFR 73.55 Paragraphs (b) through (h), that allows non-employees to take home their photobadges. The changes to the plan, being consistent with the exemption to 10 CFR 73.55(d) and shown to present no threat to safety-related equipment, do not decrease the overall ability to protect the Generic Nuclear Station from the Design Basis Threat of radiological sabotage.

Prepared by _____ Title _____ Date _____

October 15, 1999

NEI SECURITY WORKING GROUP

Under the direction of the Chairman, Mr. Douglas R. Gipson (Doug), Senior Vice President Nuclear Generation, The Detroit Edison Company:

Sub-Group	A	B	C	D
Executive	McGaha	Josiger	Hagan/ Brons	Terry
Security	Kelly	Martin	Alvey	Gibson
	Mahon	Gill	Teed	Luffman
	Bird	Wilkerson		Saunders
				Wallace
Operations	Seaman	Allen	McConnell	Blosser
Licensing	England	Allen	England	England
Engineering	Seaman	Sims	Giddens	Sims
PRA	Grantom	Grantom	Grantom	Grantom

A. Develop Guidelines that could be the basis for an interim force-on-force self-assessment program on completion of the OSRE program in Spring 2000. Then as program is being piloted, develop guidance for performance measures/thresholds for the new security cornerstone. Include criteria, objectives, definitions and evaluation standards to codify self-assessment programs that could be used in a safety-significant, performance-based security environment.

- Base approach on expected NRC confirmation of radiological sabotage using Part 100 release criteria.

- Work with NRR/NMSS to establish bounds for adversarial characteristics description (ACD) for prompt issuance of a SGI letter like the vehicle barrier/truck bomb letter.

A. Develop process to establish radiological sabotage criteria for contingency response, target set determination/analysis and operations mitigation.

Develop necessary rule modifications to 10 CFR Part 73 to risk-inform requirements and harmonize with Part 50 while justifying elimination of non safety-significant requirements.

Evaluate variances in regional interpretation, expectation and plan commitment and propose appropriate modifications (§§50.54(p)/50.90) to obtain uniformity across the industry for appropriate/necessary commitments and elimination of those commitments that add no safety-significance for public health and safety.

Mr. John R. McGaha Executive Vice President and Chief Operating Officer Entergy Operations, Inc.	Mr. Charles L. Terry (Lance) Senior Vice President & Principal Nuclear Officer TXU Electric & Gas Comanche Peak Steam Generating Station
Mr. Joseph J. Hagan (Joe) Senior Vice President, Nuclear Operations PECO Energy	Mr. William A. Josiger (Bill) Vice President, Nuclear Engineering and Projects New York Power Authority
Mr. John D. Blosser Manager Operations Support AmerenUE Callaway Nuclear Power Plant	Mr. Robert Allen (Bob) Manager-Regulatory Affairs Consolidated Edison Company Indian Point Station

Mr. Lonnie O. Wilkerson Manager Security Services Northern States Power Company Monticello Nuclear Generation Plant	Mr. Carl R. Grantom (Rick) Administrator, Risk and Reliability Analysis STP Nuclear Operating Company South Texas Project
Mr. Lesley A. England (Les) Senior Staff Engineer Entergy Operations, Inc.	Mr. Craig McConnell Supervising Operator FirstEnergy Corp. Perry Nuclear Power Plant
Mr. Garland Gibson Manager Nuclear Security Public Service Electric & Gas Company	Mr. James H. Alvey (Jim) General Supervisor, Security Operations and Maintenance Constellation Energy Group, Inc. Baltimore Gas & Electric
Mr. Christopher L. Kelley (Chris) Manager, Nuclear Security Tennessee Valley Authority	Mr. Curtis G. Luffman Superintendent Nuclear Security Virginia Electric & Power Company Surry Nuclear Generating Station

Mr. Barry M. Saunders Supervisor, Nuclear Security Operations Commonwealth Edison Company	Mr. Thomas E. Mahon (Tom) Manager Site Protection FirstEnergy Corp. Perry Nuclear Power Plant
Mr. Dan W. Martin Manager, Security Program Energy Northwest	Mr. Craig K. Seaman Director of Emergency Services Arizona Public Service Company Palo Verde Nuclear Generating Station
Mr. Jack E. Wallace Manager, Security Southern California Edison Company San Onofre Nuclear Generating Station	Mr. Ron Teed Supervisor, Nuclear Security Rochester Gas & Electric Corporation R.E. Ginna Nuclear Power Plant
Mr. Robert C. Gill (Bob) Manager, Corporate Security Carolina Power & Light Company	Mr. Gerard A. Bird (Gerry) Protection Services Manager Florida Power & Light Company St. Lucie Nuclear Power Plant
Mr. Jerry G. Sims Project Engineer - Nuclear Engineering and Licensing Mr. John M. Giddens, Jr. Senior Engineer (Licensing Issues) Southern Nuclear Operating Company	***NEI Participation***: Ralph Beedle, Senior Vice President & Chief Nuclear Officer Jack Brons, Special Assistant to the President Jim Davis, Director, Operations, Nuclear Generation ***Contact:*** Rich Enkeboll, Senior Project Mgr. Tel: (202) 739-8102 Fax: (202) 785-1898 ree@nei.org

much additional work can be conducted was discussed at length. The staff advised that it was working on its own definition of radiological sabotage, and it was not based on a10 CFR Part 100 like release criteria, but consistent with existing NRC guidance. NEI suggested that the SAP pilot be conducted for three years to be consistent with the rulemaking schedule and to ensure that each plant would be assessed at leased once. It was agreed that target set development is critical to the self assessment process and noted that NEI is considering recommending that exercise and drill frequency should be driven by the quality of site performance and not necessarily by a specific schedule. Actual pilot data would be used as a determining factor for exercise and drill frequency.

Regarding the Group B function, NEI presented a one page White Paper on the subject of a 10 CFR Part 100 release (attached).

There was no discussion of the Group C function, new 10 CFR Part 73 rule language, during this meeting.

The Group D discussion related to a matrix prepared by NEI based upon survey results from six questions that were sent to each licensee. This Special Security Survey and Screening Criteria Form (attached) was to determine variances in regional and/or plant interpretation/execution of security guidance that have resulted in security plans with inconsistent commitments. The details regarding a number of examples from the matrix were presented by NEI. Issues listed on the matrix are the issues for which NEI wants immediate security plan relief.

Several members of the public were present. The Nuclear Control Institute (NCI) was asked their policy on controlling sensitive information. They indicated that it was their policy to disclose as much information as possible and that they did not want access to sensitive information. They raised the question regarding the role of the "active" insider in the exercise and drill self assessment. Questions were also expressed regarding the perceived lack of NRC interaction with other government agencies in relation to terrorism information and activities. Concerns were raised regarding the possible increased threat at reactor sites that are expected to have mixed oxide fuel. The issue of theft of reactor fuel was also raised by NCI. A staff member of Congressmen Markey raised concerns about the proper definition of radiological sabotage and that there had not been any discussion regarding oversight of the self assessment program.

The next "working level" meeting is scheduled for December 22, 1999 to discuss the "milestone" chart noted earlier.

Attachments:

Attendance List
Self Assessment Document
Prevention of a Part 100 Release
Special Screening Criteria
Matrix
Screening Criteria Form
NEI Security Working Group

DOCUMENT NAME: G:\IOLB\IRSS\Skelton\MEETING SUM.wpd

To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosure "E" = Copy with attachment/enclosure "N" = No copy

OFFICE	RSS/DIPM	E	RSS/DIPM	E	RSS/DIPM		DIPM			
NAME	RSkelton		JArildsen		RRosano		HChristensen			
DATE	1/ /00		1/ /00		1/ 4 /00		1/ 8 /00			

OFFICIAL RECORD COPY