



UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

June 14, 2000

MEMORANDUM TO: Glenn Tracy, Chief
Operator Licensing, Human Performance
and Plant Support Branch
Division of Inspection Program Management
Office of Nuclear Reactor Regulation

FROM: Richard P. Rosano, Chief
Reactor Safeguards Section
Operator Licensing, Human Performance
and Plant Support Branch
Division of Inspection, Program Management
Office of Nuclear Reactor Regulation

SUBJECT: MINUTES OF THE MAY 18, 2000, PUBLIC MEETING WITH THE
NUCLEAR ENERGY INSTITUTE (NEI) TO DISCUSS RISK INFORMING
10 CFR PART 73 RULEMAKING AGENDA.

On May 18, 2000, NRC staff held a public meeting with representatives from NEI, industry, and the public. The purpose of this meeting was to discuss risk-informing 10 CFR 73.55 rulemaking agenda and specify items to be in the new rule.

A review of salient points of past public meetings was presented by NEI representatives to establish a foundation to discuss NEI's "Revised Security Rule Language" dated May 18, 2000, (Attachment 1). NRC staff presented comments to NEI's working draft of the prospective rule and discussed the NRC approach to the rulemaking issue in SECY-00-0063 (Attachment 2).

Future public meetings on risk-informing 10 CFR Part 73.55 will be scheduled as required.

CONTACTS: Jesse Arildsen, NRR
301-415-1026

Brad Baxter, NRR
301-415-1088

G. Tracy

- 2 -

The information above and the information in Attachments 1 and 2 document information shared and discussed between NRC staff, NEI representatives, and the public, and is not intended as a verbatim record. Attachment 3 lists the attendees of the May 18 , 2000, public meeting.

Attachments: As stated.

cc. R. Beedle, NEI
R. Enkeboll, NEI
J. Brons, NEI
J. Davis, NEI
E. Lyman, NCI

**Revised Security Rule Language
May 18, 2000**

Rulemaking guiding principles:

Provide, as feasible, a single source for security requirements for nuclear power plants.

A looking forward rule that supports the reactor oversight process four key elements (Maintain safety, enhance public confidence, improve effectiveness and efficiency, reduce unnecessary regulatory burden.)

The structure of the proposed rule is a performance-based approach using risk insights, resulting in a new logical order. Each performance objective supports the previous objective.

Consideration should be given to reducing any confusion of older and overlapping or contradictory guidance. Since this proposal is intended to lead to a revised regulation, only post-issuance guidance or interpretations should be valid, since earlier material pertains to the old version of the rule.

Throughout this proposal, we are focusing resources to support the key processes necessary to protect public health and safety, including new requirements (i.e. target set identification) and the elimination of some unnecessary regulatory burden.

Attachment 1

WORKING DRAFT

Proposed Rule Structure

(a) Purpose and Scope

The objective of nuclear power plant security is to provide adequate protection of public health and safety from a radiological release caused by attempted radiological sabotage (malevolent acts) by design basis threats. This is accomplished through the key process of positive access controls to counter the design basis threats as described in 73.1 (a) (1).¹ As part of this objective the security program design will incorporate supporting processes such that no single event can disable the security response capability because of defense-in-depth principles including diversity and redundancy. Operator action, design and engineering features will be credited during attempted radiological sabotage as part of the integrated plant response process.

(b) Access Authorization Program

The objective of the access authorization program is to ensure that those granted unescorted access are trustworthy and reliable and that they remain so through continuing programs. Each licensee will establish an access authorization program in accordance with 10 CFR 73.56. FBI criminal records checks will be conducted using the criteria of 10 CFR 73.57.

(c) Physical Protection Program

The objective of the physical protection program is to ensure that unauthorized personnel or materials (firearms, explosives or incendiary devices) are prevented unimpeded access to protected areas. This program also provides for a system of responses in the event of an attempt to introduce unauthorized personnel or materials into the facility.

C o n c e p t s	<ul style="list-style-type: none">• The licensee shall establish and maintain an onsite physical protection system and security organization which will meet the objectives of (c).• These programs also provide for a system of responses in the event of an attempt to introduce unauthorized personnel or materials into the facility.• The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in §73.1(a) such that the requirements of 10 CFR Part 100 are met.• To achieve this general performance objective, the onsite physical protection system and security organization must include, but not necessarily be limited to, the capabilities to meet the specific requirements contained in this section.
--------------------------------------	--

(1) Systems:

¹ All references will need to be updated to reflect the actual revised paragraph.

WORKING DRAFT

(i) Vehicle Barriers—The objective of vehicle barriers is to prevent penetration by the NRC defined design basis vehicle.

C o n c e p t s	<ul style="list-style-type: none">• Vehicle control measures, including vehicle barrier systems, must be established to protect against use of a land vehicle as a means of rapid introduction of personnel and/or explosives and to provide substantial protection against a land vehicle bomb.• These measures must be described in the site security plan.• Analyses supporting the efficacy of these measures in meeting the access denial criteria and maintaining the required safe stand-off distance shall be retained in accordance with 10CFR73.70.
--	---

(ii) Personnel Barriers—The objective of personnel barriers is to delineate areas where access is controlled, to impede personnel attempting to gain unauthorized access and to provide an opportunity for assessment of the threat. Personnel barriers shall be configured so as not to obstruct safe plant operation (e.g. rapid ingress and egress).

C o n c e p t s	<ul style="list-style-type: none">• A protected area shall be established as defined in accordance with the provisions of § 73.2.• The physical barriers at the perimeter of the protected area shall be separated from any other barriers designated as physical barriers.• Barriers shall be designed to channel persons and material to access entry control points and to allow detection of unauthorized penetration attempts by persons in such a manner as to permit a response to penetration of the barrier by unauthorized means.• Barriers shall be designed to support detection of attempts to gain unauthorized access or introduce unauthorized materials into protected areas by deceit using the following subsystems and subfunctions:<ul style="list-style-type: none">(i) Access controls and procedures to provide entry criteria for both persons and materials; and(ii) Entry controls and procedures to verify the identity of persons and materials and assess such identity against current authorization schedules and entry criteria before permitting entry and to initiate response measures to deny unauthorized entries.• The individual responsible for the last access control function at the normal personnel access portal (controlling admission to the protected area) must be within a bullet-resisting structure as described in paragraph (c)(6) of this section or other location not located within the access control area, to assure his or her ability to respond or to summon assistance. This
--	---

WORKING DRAFT

	<p>requirement may be waived in those installations where technology has been deployed which provides alternate assurance of this control and ability to respond.</p> <ul style="list-style-type: none">• 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 within each zone of detection.• Isolation zones shall be provided with illumination sufficient to support monitoring and observation.• The access control system shall be designed to accommodate the potential need for rapid ingress or egress of individuals during emergency conditions or situations that could lead to emergency conditions.• Keys, locks, and combinations for the protected area barrier will only be issued to individuals granted unescorted access to protected areas and must be controlled to reduce the probability of compromise. Whenever there is evidence that any key, lock, or combination may have been compromised, or an individual who has had access to these devices has his or her unescorted access revoked for cause, the keys, locks, and combinations must be changed or rotated.
--	--

(iii) Detection—The objectives of the detection systems are to provide indications to the security organization of an attempt at unauthorized personnel entry or activity.

<p>C o n c e p t s</p>	<ul style="list-style-type: none">• A detection system will be installed which will annunciate alarms at the central alarm station upon attempted penetration of the protected area barrier to allow adequate response by the security organization.• Periodic patrols by security personnel will be conducted to visually inspect the integrity of the protected area barrier and intrusion detection system.• All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other station not necessarily onsite that is capable of being manned in accordance with site requirements.• All emergency exits in each protected area barrier must be alarmed.• Onsite secondary power supply systems for alarm annunciator equipment and non-portable communications equipment as required must be located within the protected area.
---	--

WORKING DRAFT

(iv) Assessment - The objective of assessment is to determine the validity and extent of the threat, if any.

C o n c e p t s	<ul style="list-style-type: none">• Upon detection of unauthorized persons, vehicles, or activity within an isolation zone or protected area; or upon evidence or indication of intrusion into a protected area, the licensee security organization shall:<ul style="list-style-type: none">(i) Determine whether or not a threat exists,(ii) Assess the extent of the threat, if any,• To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided by closed circuit television or by other suitable means which limit exposure of responding personnel to possible attack.
--	--

(2) Contingency Response:

The objective of contingency response is to take immediate concurrent measures to defend against the threat of unauthorized access or activity.

C o n c e p t s	<ul style="list-style-type: none">• Take immediate measures to neutralize the threat by:<ul style="list-style-type: none">(A) Executing the site contingency response strategy and(B) Informing local law enforcement agencies of the threat and requesting assistance.• Require responding guards or other armed response personnel to oppose with force or threat of force any adversary attempting entry for the purpose of radiological sabotage.• The licensee shall instruct armed response personnel to prevent or impede attempted radiological sabotage by using force sufficient to counter the force directed at them including the use of deadly force when there is a reasonable belief it is necessary in self-defense, defense of others or to prevent radiological sabotage.
--	---

(i) CAS/SAS—The objective of the CAS/SAS is to provide a central point of control for monitoring, assessment, security communications control and notification (LLEA, etc.)

C o n c	<ul style="list-style-type: none">• The CAS must be considered a security controlled area and its walls, doors, ceiling, floor, and any windows in the walls and in the doors must be bullet-resisting.• The CAS must be located within a building in such a manner that the
----------------------------	---

WORKING DRAFT

e p t s	<p>interior is not visible from the perimeter of the protected area.</p> <ul style="list-style-type: none">• CAS must not contain any operational activities that would interfere with the execution of the alarm response function.• SAS will provide an additional alarm station capability, not necessarily on site, that is capable of being manned in accordance with site requirements. The SAS does not have to be bullet resistant.
------------------	--

(ii) Communications—The objective of communications is to provide an effective method to transfer information needed for a coordinated plant response.

C o n c e p t s	<ul style="list-style-type: none">• Security personnel on access control or contingency response duty shall be capable of communication with CAS.• An effective means of communications will be maintained between CAS and the Control Room.• To provide the capability of reliable communication with local law enforcement authorities, in addition to conventional telephone service, a separate communication path using alternate technology (i.e., cellular, wireless) shall be established between local law enforcement authorities and the facility and shall terminate in any continuously manned station.
--------------------------------------	--

(iii) Armed responders—The objective of an armed response force is to ensure properly trained and equipped personnel are available to execute response strategies.

(iv) Response strategies—The objective of the response strategies is to ensure that a site-specific plan provides adequate facilities, equipment, deployment tactics and personnel, appropriately equipped, responding in a timely manner to predetermined protected positions to neutralize the threat.

C o n c e p t s	<ul style="list-style-type: none">• Each licensee shall develop and maintain a response strategy appropriate for the defense of their facility against the Design Basis Threat.• Full plant capability and personnel actions should be considered in developing the response strategy. An integrated response provides for planned, organized and controlled actions of plant individuals across disciplines to minimize or mitigate a threat and/or prevent adversarial actions that could result in a radiological release that would endanger public health and safety.
--------------------------------------	---

WORKING DRAFT

	<ul style="list-style-type: none">• The plant response may be augmented, within committed time frames, by law enforcement or other government agencies having jurisdiction and by utilizing off-site licensee resources.• Each licensee will have, as a component of the response strategy, an adequate number of armed responders, with appropriate equipment and weapons, responding in accordance with site-specific plans to protected positions to counter a threat.• The response strategy must be designed to prevent disabling all targets within each target set for the time necessary to prevent significant core damage.
--	--

(A) Target sets

C o n c e p t s	<ul style="list-style-type: none">• Each licensee must develop site-specific target sets, which identify SSCs that should be protected by the response strategy. Target sets are comprised of structures, systems and components (SSCs) such as valves, pumps, switches, electrical power sources, containment and buildings, piping and electrical busses that are specifically designed for, or may be used, to keep the reactor core cooled or preserve containment integrity.• Target sets should be developed based on a safety-focused approach considering design, operational capabilities and physical layout of the facility.• Each target set is developed to provide reasonable assurance that, if any element of the target set is protected, public health and safety will not be endangered by a radiological release..
--------------------------------------	--

(B) Command and control

C o n c e p t s	<ul style="list-style-type: none">• Each licensee must ensure that the response strategy includes the necessary command and control functions to assure an effective, organized response to a threat.• Command and control functions include organizational structure, communications and team tactics necessary to provide clear direction to the response organization implementing the response strategy.• The response strategy must provide the ability for those individuals responding to the threat to transmit information between responders and command personnel relevant to the threat.
--------------------------------------	--

WORKING DRAFT

(C) Operator actions

C o n c e p t s	<ul style="list-style-type: none">• Each licensee should consider inclusion of plant operator actions in the plant response strategy.• Operations personnel, to the extent practical, should be informed immediately of any attack against the plant and should take appropriate actions to place the plant in a safe condition.• To the extent practical, operations personnel should be informed of changes in the threat and take mitigating actions as necessary to compensate for any lost SSCs.• To the extent practical, operations personnel should inform the armed response team of equipment status that may assist them in prioritizing the protection of appropriate SSCs.• If an entire target set is compromised, contingency measures employed by operations or other response personnel may prevent significant core damage.• The Control Room will be bullet resistant.
--	--

(3) Training and qualification—The objective of the training and qualification program is to ensure those individuals responsible for implementing the plant physical protection program have been trained and qualified to perform each assigned plant-protection associated duty.

C o n c e p t s	<ul style="list-style-type: none">• Licensees shall provide a training and qualification program to ensure security officers are trained and qualified to perform assigned duties.• Licensees shall define in a training and qualification plan, all requirements related to the suitability and qualification for Security Officers.• Specific program requirements are included in Appendix B to this section.• Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities. Each armed security officer, watchman, armed response person, and other member of the security organization shall requalify annually. This requalification must be documented. The licensee shall retain the documentation of each requalification as a record for three years after the requalification.• The licensee shall maintain the current training and qualifications plan as a record until the Commission terminates the license for which the plan was developed and, if any portion of the plan is superseded, retain that superseded portion for 3 years after the effective date of the change. The
--	---

WORKING DRAFT

	training and qualifications plan must be followed by the licensee 60 days after the submitted plan is approved by the NRC.
--	--

(4) Maintenance, testing and calibration—The objective of the maintenance, testing and calibration program is to ensure security equipment is capable of performing its intended function when needed.

C o n c e p t s	<ul style="list-style-type: none">• Each licensee shall test and maintain intrusion alarms, emergency alarms, communications equipment, physical barriers, and other security related devices or equipment utilized pursuant to this section as follows:<ol style="list-style-type: none">(1) All alarms, communication equipment, physical barriers, and other security related devices or equipment shall be maintained in operable condition. The licensee shall develop and employ compensatory measures to assure that the effectiveness of the security system is maintained.(2) Each intrusion alarm shall have a provision for testing which shall be exercised at a periodicity consistent with the equipment design or demonstrated characteristics.(3) Communications equipment required for use onsite shall be tested for performance not less frequently than once at the beginning of each security personnel work shift unless it is in continuous use.(4) Communications equipment required for offsite communications shall be tested for performance not less than once a day.• {How is performance testing considered??}
--------------------------------------	--

(5) Search programs—The objective of the search program is to examine all personnel, vehicles and materials entering the protected area identify certain unauthorized materials are not surreptitiously introduced.

C o n c e p t s	<ul style="list-style-type: none">• The licensee shall control all points of personnel and vehicle access into a protected area. Identification and search of all individuals unless otherwise provided in this section must be made and authorization must be checked at these points. The search function for detection of firearms, explosives, and incendiary devices must be accomplished through the use of firearms and explosive detection equipment capable of detecting those devices or physical pat-down as appropriate. The licensee shall subject all persons except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry into a protected area.
--------------------------------------	---

WORKING DRAFT

- Armed security guards who are on duty and have exited the protected area may reenter the protected area without being searched for firearms.
- When the licensee has cause to suspect that an individual is attempting to introduce firearms, explosives, or incendiary devices into protected areas, the licensee shall conduct a search of that individual using portable manual detection equipment or physical pat-down as appropriate.
- Whenever firearms or explosives detection equipment at a portal is out of service or not operating satisfactorily, the licensee shall conduct a search of all persons who would otherwise have been subject to equipment searches using portable manual detection equipment or physical pat-down as appropriate.
- At the point of personnel and vehicle access into a protected area, all hand-carried packages shall be subject to search for devices such as firearms, explosives, and incendiary devices, or other items which could be used for radiological sabotage. Search may be conducted on a random sampling basis which provides reasonable assurance that these devices will not be introduced into the protected area.
- Packages and material for delivery into the protected area shall be checked for proper identification and authorization and shall be subject to search 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 protected areas for reasons of safety, security or operational necessity. Search may be conducted on a random sampling basis which provides reasonable assurance that these devices will not be introduced into the protected area.
- All vehicles, except under emergency conditions, must be searched for items which could be used for sabotage purposes prior to entry into the protected area. Vehicle areas to be searched must include the cab, engine compartment, undercarriage, and cargo area. Escort is not required for vehicles entering the protected area that are driven by personnel having unescorted access.

(6) Positive ID—The objective of the positive ID program is to assure that the person granted access is the person with proper authorization.

- | | |
|----------------------------|--|
| C
o
n
c | <ul style="list-style-type: none">• A picture badge identification system must be used for all individuals who are authorized access to protected areas without escort.• Badges shall normally be displayed by all individuals while inside the |
|----------------------------|--|

WORKING DRAFT

e p t s	<p>protected area.</p> <ul style="list-style-type: none">• Badges may be removed from the protected area when measures are in place to confirm the true identity and authorization for access of the badge holder upon entry into the protected area.• Individuals that do not have an authorized picture badge shall be escorted by an individual designated by the licensee while in a protected area and shall be badged to indicate that an escort is required. In addition, the licensee shall require that each escorted individual's name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited is recorded. The licensee shall retain this information for one year.• Revoke, in the case of an individual's involuntary termination for cause, the individual's unescorted facility 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.
------------------	--

(7) Security organization and administrative infrastructure—The objective of the security organization and administrative infrastructure is to identify necessary resources to support physical protection with a management system for the development, revision, implementation, and enforcement of security plans, programs and procedures.

C o n c e p t s	<ul style="list-style-type: none">• The licensee shall establish a security organization, including armed security officers, to protect his facility against radiological sabotage.• If a contract security force is utilized for site security, the licensee's written agreement with the contractor must be retained by the licensee as a record for the duration of the contract and will clearly show that:<ul style="list-style-type: none">(i) The licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan,(ii) The NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor,(iii) The contractor will not assign any personnel to security duties at the site who have not been trained to meet their responsibilities.• At least one full time member of the security organization who has the authority to direct the physical protection activities of the security organization shall be onsite at all times.• The licensee shall have a management system to provide for the
--------------------------------------	--

development, revision, implementation, and enforcement of security procedures. The system shall include:

- (i) Written security procedures that document the structure of the security organization and detail the duties of armed security officers, watchmen, and other individuals responsible for security. The licensee shall maintain a copy of the current procedures as a record until the Commission terminates each license for which the procedures were developed and, if any portion of the procedure is superseded, retain the superseded material for three years after each change.
- (ii) Provision for written approval of these procedures and any revisions to the procedures by the individual with overall responsibility for the security functions. The licensee shall retain each written approval as a record for three years from the date of the approval.
- The Commission may authorize an applicant or licensee to provide measures for protection against radiological sabotage other than those required by this part if the applicant or licensee demonstrates that the measures have the same reasonable assurance objective as specified in this paragraph and that the overall level of system performance provides protection against radiological sabotage equivalent to that which would be provided by the requirements of this part and meets the general performance requirements of this part.
- {There is a need to define circumstances attendant to decommissioning or ISFSI's that would warrant suspension of Part 73 requirements since "radiological sabotage would no longer be possible?"}
- In accordance with §§50.54(x) and 50.54(y) of part 50, the licensee may suspend any safeguards measures pursuant to §73.55 in an emergency when this action is immediately needed to protect the public health and safety and no action consistent with license conditions and technical specification that can provide adequate or equivalent protection is immediately apparent. This suspension must be approved as a minimum by a licensed senior operator prior to taking the action. The suspension of safeguards measures must be reported in accordance with the provisions of §73.71. Reports made under §50.72 need not be duplicated under §73.71.
- The security program must be reviewed at least every three years by individuals independent of both on-site security program management and personnel who have direct responsibility for implementation of the on-site security program or as defined in a NRC approved quality assurance program. The security program review must include security procedures and practices, an evaluation of the effectiveness of the physical protection system, the physical protection system testing and

	<p>maintenance program, and commitments established for response by local law enforcement authorities. The results and recommendations of the security program review, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for the day-to-day plant operation. These reports must be maintained and available for inspection, for a period of 3 years.</p>
--	---

(d) Performance Evaluation Program

The objective of the performance evaluation program is to assess the effectiveness of programs outlined above to ensure they provide adequate protection of the public health and safety. The performance evaluation program is based on performance criteria that assess the effectiveness of the implementation of key contingency response program elements. Drills and exercises are used to assess the effectiveness of the contingency response plans.

<p>C o n c e p t s</p>	<ul style="list-style-type: none">• Each licensee will develop an assessment program that evaluates the effectiveness of the contingency response to attempts at radiological sabotage. Full plant capability and personnel actions may be included in this response strategy. An adequate response strategy is demonstrated if the adversary is unable to disable all targets within the target set for the time necessary to cause significant core damage.• Licensees will conduct a program of evaluated drills and exercises that provide for assessment of program elements over a three-year period. The program of integrated security drills and exercises may include tabletop drills, limited scope shift drills or exercises. A range of adversary force capabilities should be used in developing scenarios.• 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 corrective action program.
--	--