NUCLEAR ENERGY INSTITUTE

James W. Davis
DIRECTOR, OPERATIONS
NUCLEAR GENERATION DIVISION

March 2, 2001

Mr. Glenn M. Tracy, Chief
Operator Licensing, Human Performance and
Plant Support Branch
U. S. Nuclear Regulatory Commission
Mail Stop O-6 D17
Washington, DC 20555-0001

Dear Mr. Tracy:

In a May 2000 public meeting, the industry provided a conceptual document that proposed a logical sequencing of requirements and effective grouping of related parts of the rule. The industry recommended that all security requirements for nuclear power plants should be included in 10 CFR 73.55 and that the use of appendices be limited where possible.

Enclosed is a NEI Security Working Group paper that suggests modifications to security rule language that would bring some requirements into 10 CFR 73.55 and eliminate the need for some appendices. I request the NRC staff consider the proposed language as it prepares a draft security rule.

If you have any questions or comments, please contact me at 202-739-8105.

Sincerely,

James W. Davis

Enclosure

1776 I STREET, NW SUITE 400 WASHINGTON, DC 20006-3708 PHONE 202.739.8000 FAX 202.785.4019 www.nei.org

Suggested modifications to *Security Rule Language*

March 2, 2001

In May 2000 the industry provided the NRC with a conceptual document describing suggested revisions to the currently existing 10CFR73.55 that was predicated on numerous discussions with the staff. This conceptual document was intended to be supportive of staff's on-going effort to produce a comprehensive revision to security regulations applicable to nuclear power reactors. Subsequent to the informal submission of this conceptual document, the industry working group reviewed other portions of 10CFR73 in an effort to consolidate all other portions of 10CFR73 and related regulations into this revised §73.55 so that it encompasses all applicable requirements for nuclear power reactors. This would result in a single source for security requirements for the facilities and would eliminate ambiguities created by intermingling references to transportation and fuel facility requirements. The working group review of security related regulations other than § 73.55 has been completed and results in the following suggested detailed additions to the conceptual document presented on May 18, 2000.

The definition of the design basis threat taken from 73.1 and some description of the adversary characteristics document should be added to the Purpose and Scope (introductory paragraph) of the revised 73.55.

"Design Basis Threat and Adversary Characteristics
...defined as follows:
(i) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (A) Well-trained (including military training and skills) and dedicated individuals, (B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor integrity or features of the safeguards system, and (E) a four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment, and
(ii) An internal threat of an insider, including an employee (in any position), and
(iii) A four-wheel drive land vehicle bomb.

The specific capabilities of the adversary are contained in a Safeguards classified Adversary Characteristics Document, subject to an appropriate rulemaking/review

process for classified information, formally issued by the Commission to all licensees."

A "definitions" section specific to the needs of nuclear power reactors should be added immediately following the "Purpose and Scope" section.

"Definitions.

Armed security officer means a person, not necessarily uniformed, whose primary duty in the event of attempted radiological sabotage shall be to respond, armed and equipped, to defend against such actions.

Authorized individual means any individual, including an employee, a student, a consultant, or an agent of a licensee who has been designated in writing by a licensee to have unescorted access or has been screened and cleared for unescorted access.

Bullet resisting means protection as defined in Underwriter's Laboratory Standard 752, Level 4, against complete penetration, passage of fragments of projectiles, and spalling (fragmentation) of the protective material that could cause injury to a person standing directly behind the bullet-resisting barrier.

Force means violent methods used by an adversary to attempt to attempt to sabotage a nuclear facility or violent methods used by response personnel to protect against such adversary actions.

Incendiary device means any self-contained device intended to create an intense fire that can damage normally flame-resistant or retardant materials.

Intrusion alarm means a tamper indicating electrical, electromechanical, electro-optical, electronic or similar device which will detect intrusion by an individual into a building or protected area and actuates visible and audible signals.

Isolation zone means any area adjacent to a physical protected area barrier, normally clear of all objects which could aid in breaching the barrier or defeat its intent.

Lock means commercial grade locks with hardened shanks considered appropriate to the service applied by the licensee. Locked means protected by an operable lock.

Need to know means a determination by a person having responsibility for protecting Safeguards Information that a proposed recipient's access to Safeguards Information is necessary in the performance of official, contractual, or licensee duties of employment.

Physical barrier means:

(1) Fences constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire or similar material (razor ribbon is the equivalent of 3 or more strands of barbed wire) on brackets angled inward or outward between 30° and 45° from the vertical except at corner or gate posts, with an overall height of not less than eight feet, including the barbed topping;

(2) Building walls, ceilings and floors constructed of stone, brick, cinder block, concrete, steel or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening); or

(3) Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.
Protected area means an area encompassed by physical barriers and to which access is controlled.
Radiological sabotage means any attempt by deliberate act directed against a plant in which an activity licensed pursuant to the regulations in this chapter is conducted, or against a component of such a plant which attempts to endanger the public health and safety by exposure to radiation.
Safeguards Information means information classified by the licensee but not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's detailed, specific security measures for the physical protection of target sets or other information not otherwise available that would significantly enable an adversary to perpetrate radiological sabotage or information generated by the NRC or other power reactor licensees which they have classified as *Safeguards Information.*
Security management means persons responsible for security at the policy and general management level.
Security supervision means persons, not necessarily uniformed or armed, whose primary duties are supervision and direction of security at the day-to-day operating level.
Target Set is a licensee defined grouping of Structures, Systems and Components, SSCs, that are developed based on a safety focused approach considering design, operational capabilities, security characteristics, and physical layout of the facility such that all elements must be rendered nonfunctional to achieve significant core damage.
Unarmed member of the security force an individual not necessarily uniformed, whose duties do not require him/her to carry a firearm."

The specific requirements expected of licensee's Safeguards Contingency plans now found in Appendix C should be incorporated in the revised regulation in conjunction with related discussion of contingency response activity.

"Licensee Safeguards Contingency Plans

A licensee safeguards contingency plan is a documented plan to give guidance to licensee personnel in order to accomplish specific defined objectives in the event of threats or radiological sabotage relating to nuclear power reactors licensed under the Atomic Energy Act of 1954, as amended. An acceptable safeguards contingency plan must contain: (1) a predetermined set of decisions and actions to satisfy stated objectives, (2) an identification of the procedures or mechanisms necessary to efficiently implement the decisions, (3) an integration of the licensee response with the responses by outside entities, and (4) a measurable performance in response capability.
The goals of licensee safeguards contingency plans are to make provisions for responding to threats and radiological sabotage such that public health and safety

are reasonably assured at the licensee's level of responsibility. It is noted that the licensee is not responsible to prepare plans to counter threats from sources which are deemed to be "enemies of the state".
It is important to note that a licensee's safeguards contingency plan is intended to be an integrated part of overall operations and to be complementary to any emergency plans developed pursuant to appendix E to part 50 of this chapter. Periodic review of plan effectiveness will be accomplished by the licensee's assessment process."

The general requirements for security personnel now contained in Appendix B should become an integral part of the training and qualifications section of the revised regulation as indicated in the conceptual document.

"General Criteria for Security Personnel

Introduction
Security personnel who are responsible for the protection of nuclear power reactors against radiological sabotage should be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties. In order to ensure that those individuals responsible for security are properly equipped and qualified to execute the job duties prescribed for them, the NRC has developed general criteria that specify security personnel qualification requirements.
These general criteria establish requirements for the selection, training, equipping, testing, and qualification of individuals who will be responsible for protecting nuclear power reactors .
When required to have security personnel that have been trained, equipped, and qualified to perform assigned security job duties in accordance with the criteria specified below, the licensee must establish, maintain, and follow a plan that shows how the criteria will be met.
Definitions
Terms defined in parts 50 of this chapter have the same meaning when used in this section.
Criteria
I. Suitability and qualification for security duties.
A. Suitability: 1. Prior to assignment to duties within the security organization, an individual shall meet the following suitability criteria:
a. Educational development -- Possess a high school diploma or pass an equivalent performance examination designed to measure basic job-related mathematical, language, and reasoning skills, ability, and knowledge, required to perform security job duties.
b. Felony convictions -- Have no felony convictions involving the use of a weapon and no felony convictions that reflect on the individual's reliability consistent with the standards established by the licensee pursuant to 10CFR 73.56.

2. Prior to employment or assignment to the security organization in an armed capacity, the individual, in addition to (a) and (b) above, must be 18 years of age or older.
B. Physical and mental qualifications. 1. Physical qualifications:
a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall have no physical weaknesses or abnormalities that would prevent the performance of assigned security job duties.
b. In addition to a. above, armed security officers shall successfully pass a physical examination directed and documented by a licensed physician which shall attest to the individual's ability to participate in the licensee's physical fitness tests. The examination shall be designed to measure the individual's physical ability to perform assigned security job duties as identified in the licensee physical security and contingency plans.
3. Other physical requirements -- An individual who has been incapacitated due to a serious illness, addiction, injury, disease, or operation, which could interfere with the effective performance of assigned security job duties shall, prior to resumption of such duties, provide medical evidence of recovery and ability to perform such security job duties. Where applicable, provisions of the licensee's program pursuant to 10CFR26 shall apply.
2. Mental qualifications and emotional stability shall be established based on licensee programs pursuant to 10CFR 26 and §56 of this Part.
C. Physical fitness qualifications Subsequent to physical examinations, armed security officers shall demonstrate physical fitness for assigned security job duties by performing a practical physical fitness demonstration. The physical fitness program performance objectives shall be described in the license training and qualifications plan and shall consider job-related functions such as strenuous activity, physical exertion and levels of stress as they pertain to each individual's assigned security job duties for both normal and emergency operations.
D. Physical requalification --Biennially, armed security officers shall be required to meet the physical examination and physical fitness requirements of this section.

II. Training and qualifications.
A. Training and qualification requirements -- Each individual who requires training to perform assigned security-related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained and qualified to perform these tasks and duties in accordance with the licensee or the licensee's agent's documented training and qualifications plan.
B. Security knowledge, skills, and abilities -- The areas of knowledge, skills, and abilities that shall be considered in the licensee's training and qualifications plan are as follows:
i. General Knowledge
1. Protection of nuclear power reactors.
2. NRC requirements and guidance for physical security at nuclear power reactors.

3. The private security officer's role in providing physical protection for the nuclear industry.
4. The authority of privatesecurity officers.
5. The use of less lethal weapons (if employed).
6. The use of deadly force.
7. Power of arrest and authority to detain individuals.
8. Authority to search individuals and seize property.
9. Adversary group operations.
10. Motivation and objectives of adversary groups.
11. Tactics and force that might be used by adversary groups to achieve their objectives.
12. Facility security organization and operation.
13. General concepts of fixed site security systems.
14. Vulnerabilities and consequences of radiological sabotage of a facility.
15. Personal equipment use and operation for normal and contingency operations.
16. Site security information protection.
17. Security and situation reporting, documentation and report writing.
ii. System Design and Use
1. Recognition of sabotage related devices and equipment that might be used against the licensee's facility.
2. Types of physical barriers and delay systems.
3. Weapons control, lock and key control system operation.
4. Protected area security and vulnerability.
5. Types of alarm systems and their operation.
6. Surveillance and assessment systems and techniques.
7. Communications systems operation.
8. Access control systems and operation for individuals, packages, and vehicles.
9. Contraband detection systems and techniques.
10. Duress alarm operation.
11. Alarm stations operation.
12. Night vision devices and systems (if employed).
iii. Normal Operations
1. Fixed post station operations.
2. Search techniques and systems for individuals, packages and vehicles.
3. Escort and patrol responsibilities and operation.
4. Security system operation after component failure.
5. Security equipment testing.
6. Security procedures.
7. Security command and control system during normal operation.
iv. Contingency Operations
1. Response and assessment to alarm annunciations and other indications of intrusion.
2. Personal equipment use and operation for normal and contingency operations.
3. Response force organization.

4. Response force mission.
5. Response force operation.
6. Response force engagement.
7. Defensive strategies and target sets.
8. Security command and control system during contingency operation.
9. Use of weapons.
10. Contingency response to confirmed intrusion or attempted intrusion.
11. Security coordination with local law enforcement agencies.
12. Contingency duties.
13. Self defense.
14. Use of and defenses against incapacitating agents.
15. Contingency procedures.
16. Mechanics of detention.
17. Basic armed and unarmed defensive tactics.
18. Response force deployment.
19. Security alert procedures.

C. Requalification - Security personnel shall be requalified biennially to perform assigned security-related job knowledge, tasks and duties which are not demonstrated by continued on the job proficiency and oversight. Oversight of periodic sampling, drills and exercises which test proficiency shall be documented.

III. Weapons training and qualification.

A. Training. Armed security officers requiring weapons training to perform assigned security related job tasks or job duties shall be trained in accordance with the licensees' documented weapons training programs. Each individual shall be trained in the use of assigned weapon(s) and shall meet prescribed standards in the following areas:

1. Weapons cleaning and storage.
2. Combat firing, day and night.
3. Safe weapons handling.
4. Clearing, loading, unloading, and reloading.
5. Rapid fire techniques.
6. Stress firing.

B. Weapons Qualification.

Qualification firing for the assigned weapon(s) must be for daylight firing, and each individual shall perform night firing for familiarization. Each individual shall be requalified at least every 12 months.

IV. Guard and armed response personnel equipment.

Armed security officers shall either be equipped with or have available the following security equipment appropriate to the individual's assigned contingency security related tasks or job duties as described in the licensee physical security and contingency plans. Equipment shall be maintained in good working order and in sufficient quantity.

1. Semiautomatic rifles of at least .223 caliber.
2. 12 gauge shotguns (if shotguns are designated for use in the security or contingency plan).
3. Semiautomatic pistols or revolvers of at least .354 caliber.
4. Ammunition, magazine and clip capacity.
The licensee shall maintain an ammunition supply suitable to meet the needs of the contingency plan.
E. Personal equipment determined by the licensee as necessary to meet the requirements of assigned physical security and contingency plan duties shall be readily available for individuals who warrant such equipment.
V. Documentation -- The results of suitability, physical, mental, training, weapons qualifications and re-qualifications including appropriate data and test results must be documented by the licensee or the licensee's agent. The licensee or the agent shall retain this documentation as a record for three years from the date of obtaining and recording these results."

The reporting and record keeping requirements now contained in § 73.70, 73.71 and Appendix G should be modified and made part of the revised regulation.

"Reporting of safeguards events.

(1) Reporting of events requiring telephonic notification must be made to the NRC Operations Center via the Emergency Notification System. If the Emergency Notification System is inoperative or unavailable, the licensee shall make the required notification via commercial telephonic service or other dedicated telephonic system or any other methods that will ensure that a report is received by the NRC Operations Center within one hour. The exemption of §73.21(g)(3) applies to all telephonic reports required by this section.
(2) The licensee shall, upon request of the NRC, maintain an open and continuous communication channel with the NRC Operations Center provided that the maintenance of such an open channel does not limit the ability of the licensee to address the event being reported.
(4) The initial telephonic notification must be followed within a period of 30 days by a written report submitted to the U.S. Nuclear Regulatory Commission, Document Control Desk, Washington, DC 20555. The licensee shall also submit one copy to the appropriate NRC Regional Office. The report must include sufficient information for NRC analysis and evaluation.
(5) Significant supplemental information which becomes available after the initial telephonic notification to the NRC Operations Center or after the submission of the written report must be telephonically reported to the NRC Operations Center and also submitted in a revised written report (with the revisions indicated) to the Regional Office and the Document Control Desk. Errors discovered in a written report must be corrected in a revised report with revisions indicated. The revised report must replace the previous report; the update must be a complete entity and not contain only supplementary or revised information. Each licensee shall

maintain a copy of the written report of an event submitted under this section as record for a period of three years from the date of the report.
(6) If subsequent information indicates that the basis for any report made pursuant to these requirements was unfounded the licensee shall retract the report using the same procedure as was used to report the information."

"Reportable Safeguards Events

Licensees shall report or record, as appropriate, the following safeguards events.
I. Events to be reported within one hour of discovery, followed by a written report within 30 days.
(a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause:
(1) Significant physical damage to a nuclear power reactor or its equipment or to the nuclear fuel or spent nuclear fuel at the facility; or
(2) Interruption of normal operation of a licensed nuclear power reactor through the unauthorized use of or tampering with its machinery, components, or controls including the security system.
(b) An actual entry of an unauthorized person into a protected area.

II. Events to be recorded
The licensee shall maintain a record of any other threatened, attempted, or committed act not previously defined in I above with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness. The effects of transient environmental conditions need not be recorded."

General instructions relevant to record keeping should be included in the revised stand alone regulation.

"Records.

Each licensee shall maintain records of the following security activities: (1) Alarm records, (2) Training and Qualification, (3) Visitor logs, (4) Access to the Protected Area, (5) Validated failures of alarms and communications equipment, (6) Degradation of security equipment other than for transient environmental conditions, which requires compensatory measures.
Each record required by this part must be legible throughout the retention period. The content of these records shall be such that the recorded activity may be understood by a knowledgeable individual. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media.
Unless otherwise specified records shall be maintained for one year."

The authority to make changes to security and contingency plans required by the revised regulation should be modified and move from part 50 to be integral with the revised regulation since it has no other applicability.

"**Changes**
(1) The licensee shall prepare and maintain security and contingency plans and procedures for effecting the actions and decisions determined appropriate to the defense of the facility against radiological sabotage and to control access. The licensee may make changes, without prior Commission approval, to these plans provided the licensee maintains the ability to control access and defend against radiological sabotage pursuant to this part. Changes which involve deviations from specific requirements of this part require prior Commission Approval. A licensee desiring to make such a change shall submit an application for an amendment to the licensee's license pursuant to §50.90.
(2) The licensee shall maintain records of changes to the plans made without prior Commission approval for a period of three years from the date of the change, and shall submit, as specified in §50.4, a report containing a description of each change within two months after the change is made
(3) The licensee shall provide for the development, revision, implementation, and maintenance of its security and contingency plans. The overall efficiency of the licensee's contingency plan is demonstrated through drills and exercises. Supporting and implementing procedures shall be subject to review at the same interval as the licensee's operating procedures."

Finally, the requirement for the protection of Safeguards Information currently found in § 73.21 should be made specific to the needs of nuclear power reactors and included in the revised comprehensive regulation.

"**Requirements for the protection of safeguards information.**

(a) *General performance requirement.* Each licensee who is authorized to operate a nuclear power reactor and each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure. To meet this general performance requirement, licensees and persons subject to this section shall establish and maintain an information protection system for Safeguards Information.

(b) *Access to Safeguards Information.* (1) Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established "need to know" for the information and is:
(i) An employee, agent, or contractor of an applicant, a licensee, the Commission, or the United States Government. However, an individual to be authorized access to Safeguards Information by a nuclear power reactor applicant or licensee must undergo a Federal Bureau of Investigation criminal history check to the extent required by 10 CFR 73.57;

(ii) A member of a duly authorized committee of the Congress;
(iii) The Governor of a State or designated representatives;
(iv) A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC;
(v) A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies; or
(vi) An individual to whom disclosure is ordered pursuant to §2.744(e) of this chapter.
(2) Except as the Commission may otherwise authorize, no person may disclose Safeguards Information to any other person except as set forth in paragraph (c)(1) of this section.

(c) *Protection while in use or storage.* (1) While in use, matter containing Safeguards Information shall be under the control of an authorized individual.
(2) While unattended, Safeguards Information shall be stored in a locked storage container. Access to locked Safeguards Information shall be limited to a minimum number of personnel for operating purposes who have a "need to know" and are otherwise authorized access to Safeguards Information in accordance with the provisions of this section.

(d) *Preparation and marking of documents.* Each document or other matter that contains Safeguards Information shall be marked "Safeguards Information" in a conspicuous manner to indicate the presence of protected information. (f) *Reproduction and destruction of matter containing Safeguards Information.* (1) Safeguards Information may be reproduced to the minimum extent necessary consistent with need without permission of the originator.
(2) Documents or other matter containing Safeguards Information may be destroyed by any method that assures complete destruction of the Safeguards Information they contain.

(e) *External transmission of documents and material.* (1) Documents or other matter containing Safeguards Information, when transmitted outside an authorized place of use or storage, shall be packaged to preclude disclosure of the presence of protected information.
(2) Safeguards Information may be transported by messenger-courier, United States first class, registered, express, or certified mail, or by any individual authorized access.
(3) Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted only by protected telecommunications circuits (including facsimile) approved by the NRC. Physical security events required to be reported are considered to be extraordinary conditions.

(f) *Use of automatic data processing (ADP) systems.* Safeguards Information may be processed or produced on an ADP system provided that the system is self-contained within the licensee's or his contractor's facility and requires the use of an entry code for access to stored information. Other systems may be used if approved for security by the NRC.

(g) *Removal from Safeguards Information category.* Documents originally containing Safeguards Information shall be removed from the Safeguards Information category whenever the information no longer meets the criteria contained in this section."