



RELEASED TO THE PDR
3/7/94 g
date initials

POLICY ISSUE
(Notation Vote)

December 2, 1993

SECY-93-326

FOR: The Commissioners

FROM: James M. Taylor
Executive Director for Operations

SUBJECT: RECONSIDERATION OF NUCLEAR POWER PLANT SECURITY REQUIREMENTS
ASSOCIATED WITH AN INTERNAL THREAT

PURPOSE:

To inform the Commission of the results of the staff's reconsideration of security requirements associated with an internal threat at nuclear power plants and to provide the Commission with alternatives and options.

SUMMARY:

In response to Commission direction, the staff has reconsidered the details of SECY-92-272, "Re-examination of Nuclear Power Plant Security Requirements Associated With the Internal Threat." The staff held three public meetings with the Nuclear Management and Resources Council (NUMARC), analyzed NUMARC's proposed Alternative Protection Strategy (APS), and considered recent vehicle events. The staff believes that fully implementing the APS without alternative compensating measures could significantly decrease the ability of some licensees to protect against the design basis threat. However, the staff developed alternative approaches that could be expeditiously implemented and would achieve many of NUMARC's goals. The staff continues to recommend concurrently proceeding with rulemaking to assure that 10 CFR 73.55 clearly reflects changes in physical security program elements made as a result of this paper and accepted by the NRC.

Contact:
Robert Dube, NRR
504-2912

NOTE: TO BE MADE PUBLICLY AVAILABLE
WHEN THE FINAL SRM IS MADE
AVAILABLE

9312130228 xA

3/14/94

080060

FOR 1/1

BACKGROUND:

In SECY-92-272, the staff made six rulemaking recommendations related to the APS, which are summarized in Enclosure 1. In a memorandum dated November 5, 1992 (Enclosure 2), the Commission directed the staff to reconsider the details of SECY-92-272 and to work with NUMARC, as necessary, to fully understand the goals of its APS, as a base from which to explore alternatives. The Commission also directed the staff to consider two related issues.

On February 7, 1993, there was a forced vehicle entry into the protected area at Three Mile Island (TMI) Unit 1. On February 25, 1993, a van bomb was detonated at the World Trade Center in New York City. The staff considered these events in its re-examination of requirements associated with the internal threat. The forced vehicle entry at TMI is pertinent to issues regarding vital area locks and alarms. However, staff recommendations in SECY-93-270, "Proposed Amendments to 10 CFR Part 73 to Protect Against Malevolent Use of Vehicles at Nuclear Power Plants," would require licensees to install a barrier system that would protect against forced vehicle entry. The World Trade Center bombing is pertinent to issues regarding escorting of vehicles allowed inside the protected area. Vehicle escort issues are addressed in this paper rather than in SECY-93-270.

Actions taken as a result of this evaluation may have a bearing on another ongoing staff evaluation of the scope of random drug testing for nuclear power plant licensees. In COMSECY-92-018, the Commission requested the staff to examine the justification for imposing random drug tests on workers with no direct safety functions, particularly for clerks, secretaries, or other employees who have unrestricted access to a nuclear plant's protected area. One argument supporting limiting the scope of drug testing is that many of the administrative and clerical workers who have access to the protected area (and therefore are subject to random drug testing) do not have access to vital areas. Reductions in protected area to vital area access control measures could compromise this argument. The staff is addressing the interrelationship of these issues in its response to COMSECY-92-018.

DISCUSSION:

In meetings on November 20, 1992, January 22, 1993, and September 1, 1993, NUMARC representatives and NRC staff discussed each of the nine recommendations in SECY-92-272 in relation to the associated positions in NUMARC's APS. The staff believes that it fully understands the goals of the APS. Although some differences exist between the staff's recommendations and the APS, NUMARC representatives indicated at the September 1st meeting that they understand the staff's concerns (although not agreeing with all of them) and that options being considered by the staff would help meet some of the goals of the APS.

A representative of the International Union, United Plant Guard Workers of America, also attended the January 22nd and September 1st meetings with NUMARC and submitted comments in a letter dated January 29, 1993 (Enclosure 3). The representative expressed concerns about personnel job security and any reduction in the level of plant physical security.

As part of its reconsideration of SECY-92-272, the staff also reviewed NUREG-1485, the Incident Investigation Team report on the unauthorized forced entry into the protected area at Three Mile Island (TMI) on February 7, 1993; SECY-93-166, "Staff Recommendation for Protection Against Malevolent Use of Vehicles at Nuclear Power Plants;" and SECY-93-270. Details of the staff's analysis of NUMARC's APS and the staff's proposed alternative approach are provided in Enclosure 4.

NUMARC has stated that the APS can be implemented without a rule change because the strategy provides protection equivalent to certain physical protection requirements contained in 10 CFR 73.55 (b) through (h). NUMARC emphasized that trustworthiness programs, including criminal history checks, fitness-for-duty, access authorization, and behavioral observation programs, enhance protection against an internal threat. In promulgating 10 CFR 73.55, the Commission recognized that the rule was incomplete with respect to insider threat protection and specifically noted that trustworthiness issues would be dealt with separately in further rulemaking. Consequently, the criminal history fingerprint check program has been required by 10 CFR 73.57 since March 2, 1987, the fitness-for-duty program has been required by 10 CFR Part 26 since June 7, 1989, and the access authorization and behavioral observation programs have been required by 10 CFR 73.56 since April 25, 1991. None were promulgated as substitutes for any element of 10 CFR 73.55.

These trustworthiness requirements complement the physical protection requirements of 10 CFR 73.55. The general performance objective and requirements of 73.55(a) state that the Commission may authorize a licensee to provide measures for protection against radiological sabotage, other than those specified in (b) through (h), if the licensee demonstrates that the measures have the same high assurance objective and that the overall level of system performance provides equivalent protection. Compliance with complementary individual trustworthiness requirements dealing with special aspects of the insider threat are not a substitute for the required physical protection measures that cover both the external threat and internal security controls of a more general nature not necessarily related to trustworthiness. NUMARC confirmed the staff's initial understanding that the APS does not include any proposals for specific alternative physical protection measures that would provide protection equivalent to that provided by the provisions of 10 CFR 73.55 (b) through (h).

The staff finds merit in some of NUMARC's recommendations that could result in reductions in requirements beyond what the staff proposed in SECY-92-272. However, the staff believes that fully implementing the APS without alternative compensating measures could significantly decrease the ability of some licensees to protect against the external design basis threat and could also decrease, to a lesser degree, the ability of licensees to protect against an internal threat. The staff's basis for this conclusion is discussed on pages 2 through 4 of Enclosure 4. Therefore, the staff does not support full implementation of the APS.

One of the goals of the APS was to reduce requirements without time-consuming rulemaking. However, most of the proposals in the APS involved elimination of security program elements specifically detailed in the regulations.

Therefore, the staff finds that most of the proposals in the APS cannot be implemented generically without rulemaking.

NUMARC's APS recommended changes in regulatory positions in four areas: (1) security requirements for vital area access, (2) posting a security guard at containment during periods of frequent access, (3) vehicle escort requirements, and (4) repeated search of on-duty armed security guards.

Vital Area Access Controls

NUMARC proposed to change the first area by eliminating all security requirements, such as for locks and alarms, for vital area doors. The staff believes that the NRC would need to decrease its design basis threat, as requested by NUMARC in Enclosure 5,¹ before it could completely eliminate these requirements. As directed by the Commission, the staff is reevaluating the design basis threat for radiological sabotage in response to the TMI vehicle intrusion and the World Trade Center bombing. However, the staff developed the following alternative approach that could be expeditiously implemented and should achieve many of NUMARC's goals without requiring a decrease in the design basis threat.

In the staff's alternative approach, the licensee could eliminate or reduce certain vital area access controls upon confirmation that certain other site-specific measures are in place or will be implemented. These measures would include the demonstration by the licensee that a capability exists to protect against an external adversary after reducing its commitments for vital area locks, alarms, and other provisions. For an internal adversary, licensees not already doing so would have to commit to examine hand-carried packages for explosive² using equipment specifically designed for that purpose. Licensee commitment to these measures could enable the NRC to reduce site-specific vital access requirements using the license amendment provisions of 10 CFR 50.90, or the exemption provisions of 10 CFR 73.5, in conjunction with the provisions of 10 CFR 50.54(p). If many licensees pursued this approach, rulemaking would still be advisable to ensure that the regulations properly reflect generally approved practices.

The staff developed three options for the alternative approach for reducing the requirements for access to vital areas. All three options would provide for expeditious site-specific implementation, but include rulemaking for ultimate resolution.

Option 1 incorporates three of the recommendations for rule change presented in SECY-92-272. Recommendation 1 eliminates requirements for compensatory measures for failure of mechanical lock hardware if the access control hardware and alarm are operable. Recommendation 2 would eliminate the requirement to maintain discrete lists of persons allowed access to each

¹NUMARC also identified in Enclosure 5 two issues related to logging and reporting of safeguards events that were outside the scope of NUMARC's APS and this paper. Recommendations related to these issues will be included in the Regulatory Review Group Implementation Plan.

separate vital area and eliminate the requirement for reviewing the lists every 31 days. Recommendation 3 would reduce the requirements for responding to nuisance alarms at vital area doors, such as not responding to certain types of door alarms or responding only to a percentage of all alarms. In addition to the staff's earlier proposal to implement these recommendations generically through rulemaking, the staff's alternative approach would allow expeditious site-specific implementation because of alternative licensee commitments that would satisfy the equivalency test of 10 CFR 73.55.

Option 2 would include recommendation 2 and revise recommendations 1 and 3. Timeliness requirements for compensatory measures for any malfunctioning element of the vital area access system would be extended from 10 minutes to a period similar to that permitted in technical specifications for safety equipment to be out of service, typically 1 to 3 days, if either the lock or alarm are operable. Licensees would be required to respond only to those vital area door alarms that coincide with an unresolved alarm at the protected area perimeter, a known intrusion, or a constant alarm such as that caused by an open door.

Option 3 would include recommendations 1, 2, and 3, as revised by Option 2. In addition, it would permit reduction of the commitments for locks on vital area doors, except for those doors licensees determine necessary to delay an external threat. This option would allow vital area doors to normally be unlocked, but licensees would be required to retain locking mechanisms and to have the capability to remotely lock the doors from the central and secondary alarm stations in the event of a security contingency. Access control systems also would be retained on vital area doors to maintain a record of personnel access and would generate an alarm if a door was opened without a keycard.

Option 3 would further reduce any safety impact, which is already low, of vital area security measures by allowing licensees to leave some or all vital area doors unlocked but still retain alarm systems to detect unauthorized entry. In conjunction with option 1 or 2, the staff also recommends that licensees be encouraged through an information notice to (1) have the ability to remotely unlock vital area doors from security alarm stations, (2) ensure that malfunctions result in doors failing unlocked rather than locked, and (3) allow all operators and auxiliary operators to carry hard keys that can override keycard lock mechanisms.

The licensee's ability to protect against an external adversary would not diminish under any of these options. The staff believes that to retain an adequate capability to protect against an external adversary, a licensee should be required to at least retain the ability to lock vital area doors on demand and to generate an alarm if a vital area door is opened without a keycard. GPU Nuclear Corporation used both of these capabilities in responding to the forced vehicle entry into the protected area at TMI.

Although each of these three options would incrementally decrease the effectiveness of the licensee's measures to protect against an internal threat, the staff believes that with the additional licensee commitments discussed previously, licensees could still meet the general performance objective of 10 CFR 73.55(a).

Containment Access Control

The second area discussed by NUMARC was the requirement that guards or watchpersons exercise positive access control to containment to ensure that only authorized personnel and materials are permitted entry any time frequent access is permitted, such as during a refueling outage or major maintenance. NUMARC's APS recommended either deleting the requirement or modifying it to allow access to be controlled by other than security personnel. However, at meetings with the staff, NUMARC stated that their goal was to eliminate the requirement.

NUMARC's recommendation to delete the requirement is essentially the same as the staff's rulemaking recommendation 4 in SECY-92-272, which the staff still supports. In effect, containment would not have to be treated as a separate vital area. This change would require rulemaking because of the specific nature of 10 CFR 73.55(d)(8) and because NUMARC's APS contains no elements that specifically address protection alternatives to controlling access to containment.

With respect to NUMARC's alternative recommendation, the staff believes that the definition of "watchman" in 10 CFR 73.2 is sufficiently broad to allow access to be controlled by persons other than security personnel. However, some licensees may have to amend their security plans if they contain narrower definitions of a watchman or if other duties are assigned to a watchman that require specific security training.

Vehicle Escort Requirements

The third area discussed by NUMARC relates to requirements that vehicles have escorts. The NRC regulations require that, except for designated vehicles owned by the licensee and normally kept in the protected area, vehicles entering the protected area must be escorted by a security officer. NUMARC recommended that the escort requirement be waived for any vehicles with drivers who have been authorized unescorted access to the protected area, regardless of whether the licensees owned the vehicle, who employed the driver, or the normal location of the vehicle.

The staff agrees that under the conditions indicated in recommendation 6 of SECY-92-272, the requirement for an escort (in essence, a two-person rule) may not contribute significantly to protection of the public health and safety. However, the staff believes that NUMARC's proposal would not provide sufficient protection in all cases. Specifically, in many instances behavioral observation programs for a non-licensee employee whose regular job is driving a vehicle are less rigorous than for licensee employees. It also is more difficult to effectively search a vehicle and its cargo than to search an individual or a hand-carried package. In addition, NUMARC's recommendation to reduce control of vehicles is inconsistent with the staff's recommendation in SECY-93-166 to increase protection against the malevolent use of vehicles, in light of the TMI event and the vehicle bomb that exploded at the World Trade Center. Therefore, the staff still recommends that the escort requirements be eliminated only for licensee-owned vehicles entering the protected area for work-related purposes, when these vehicles can be

effectively searched for explosives and are driven by licensee employees who have unescorted access. This would require a rule change because it would allow vehicles (other than specially designated vehicles normally kept in the protected area) to be driven into the protected area with only a single occupant.

Repeat Searching of Armed Security Guards

The fourth area discussed by NUMARC was the repeated search of armed security guards exiting and reentering the protected area on official duty. NUMARC recommended that guards be exempt from all search requirements upon reentry. The staff recommended eliminating the metal detector search, but not the explosives search (SECY-92-272, recommendation 5). During followup discussions, NUMARC said the problem of guard reentry to the protected area was exacerbated because some licensees use the same portal for both metal and explosives detection. Since these dual portal detectors generate separate alarms for metal and explosives, the staff modified its original recommendation to allow licensees using dual portal detectors to ignore the metal alarm for on-duty guards carrying a weapon.

The goal of eliminating repeated metal detector searches of armed security guards could be expeditiously implemented. Under the provisions of 10 CFR 73.55(a), the staff would authorize alternative licensee procedures that ensure that metal detector searches would be waived only for on-duty security officers who have already been searched during their current shift and who are carrying a weapon in accordance with assigned duties. Final resolution of this item would require a rule change to assure that the regulations are consistent with generally accepted practices.

Commission Identified Related Issues

In its memorandum of November 5, 1992, the Commission asked the staff to give consideration to two points related to access controls. The staff response to these points is given in Enclosure 6. The staff agrees with the Commissioners' observation that during some situations, such as outages, the staff's assumption may not always be true that most persons granted access to the protected area also have access to vital areas. However, the staff has carefully evaluated the basis for its recommendations and still concludes that the decrease in the security diversity and effectiveness resulting from a relaxation of vital area access controls would be acceptably small.

The Commission also asked the staff to consider permitting licensee employees to carry security badges home. If the badges are not properly controlled, they could be stolen or counterfeited and the coding system that would allow unauthorized personnel to gain access to the protected and vital areas could be copied. Current regulations do not prohibit licensee employees from leaving the protected area with their badges if adequate safeguards are in place to ensure that the security of the badge is not jeopardized. Recently, one licensee has proposed an access control approach that includes a hand geometry system that uniquely identifies an individual. This approach is currently under review by the staff and may prove an acceptable alternative to maintaining control of badges at the site. Acceptable alternatives also could

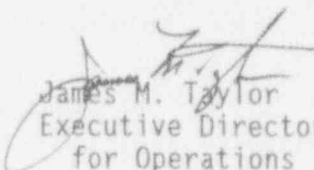
be developed based on the use of a personal identification number to gain entry to the protected area.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objection.

RECOMMENDATIONS:

1. Approve the staff's issuance of an information notice to power reactor licensees informing them of the opportunity to: (1) expeditiously implement recommendations 1, 2, and 3 (related to vital area access control measures) of SECY-92-272, as revised in Option 3 of this paper and subject to licensee confirmation that certain other site-specific measures as specified in this paper are in place or will be implemented; (2) expeditiously implement recommendation 5 (related to repeated search of armed security guards) as revised herein; (3) use non-security personnel as watchmen for the purpose of controlling access to containment during times of frequent access, if the definition for watchman in 73.2 is met; and (4) propose alternative measures that would permit licensee employees to carry security badges home.
2. Approve the staff's concurrently proceeding with rulemaking to implement SECY-92-272 recommendations 1 through 6, as revised in this paper, on a generic basis.


James M. Taylor
Executive Director
for Operations

Enclosures:

1. Summary of SECY-92-272 Rulemaking Recommendations
2. Memorandum from the Secretary dated November 5, 1992
3. Letter from United Plant Guard Workers of America dated January 29, 1993
4. Analysis of NUMARC's APS and Alternative Staff Approach
5. Enclosure 2 to NUMARC letter dated December 21, 1992
6. Response to Commission Requests for Additional Staff Considerations

Commissioners' comments or consent should be provided directly to the Office of the Secretary by COB Thursday, December 16, 1993.

Commission Staff Office comments, if any, should be submitted to the Commissioners NLT Thursday, December 9, 1993, with an information copy to the Office of the Secretary. If the paper is of such a nature that it requires additional review and comment, the Commissioners and the Secretariat should be apprised of when comments may be expected.

DISTRIBUTION:

Commissioners

OGC

OCAA

OIG

OPA

OCA

OPP

EDO

ACRS

ASLBP

SECY

ENCLOSURE 1

Summary of SECY-92-272 Recommendations

SUMMARY OF SECY-92-272 RULEMAKING RECOMMENDATIONS

1. Revise the regulations to specify that the licensee need not take compensatory measures for failure of mechanical lock hardware if the access control hardware and alarm are operable.
2. Revise the regulations applicable to vital area access controls to eliminate the requirement to maintain discrete lists of persons allowed access to each separate vital area. Continue to require the licensee to maintain a list of persons requiring access to vital areas, but eliminate the requirement for maintaining separate lists for each vital area and for reviewing the lists every 31 days.
3. Revise the regulations to reduce the requirements for responding to nuisance alarms at vital area doors. Further study is needed to determine the best approach for reduced response. The NRC might consider not requiring a response to certain types of door alarms or requiring a response only to a certain percentage of all alarms.
4. Revise the regulations to delete requirements for controlling the access of personnel and materials into containment from a security standpoint during periods of high traffic such as refueling and major maintenance. This change only applies to access from vital areas into containment and does not negate radiological controls or other requirements for personnel accountability.
5. Revise the regulations to eliminate the need for armed guards who are going out of the protected area and re-entering it on official duty to pass through the metal detector each time. Guards would still be expected to submit to the search requirements for explosives.
6. Revise the regulations to eliminate the escort requirements for licensee-owned vehicles entering the protected area (following normal search procedures) for work-related purposes only, when these vehicles are driven by licensee employees who have unescorted access. During the time that these vehicles were unattended in the protected area, they would have to remain locked and the keys would have to be removed. This relaxation would apply to licensee-owned vehicles, but not to vendor or contractor vehicles.

ENCLOSURE 2

Memorandum from the Secretary
dated November 5, 1992

ACTION - MURLEY, NRR

OFFICE OF THE
SECRETARY

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

November 5, 1992

Cys: Taylor
Sniezek
Thompson
Blaha
PMcKee, NRR

MEMORANDUM FOR: James M. Taylor
Executive Director for Operations

FROM: Samuel J. Chilk, Secretary

SUBJECT: SECY-92-272 - RE-EXAMINATION OF NUCLEAR POWER
PLANT SECURITY REQUIREMENTS ASSOCIATED WITH
THE INTERNAL THREAT

The Commission (with all Commissioners concurring) has agreed that the staff should reconsider the details of SECY-92-272 and should work with NUMARC, as necessary, to fully understand the goals of their proposed Alternate Protection Strategy as a stepping-off point for exploring alternatives. The Commission believes that an opportunity and justification exists to explore a less prescriptive approach to current security requirements which were driven by concern over employee trustworthiness.

As part of this re-examination, the Chairman and Commissioners Curtiss and de Planque would like the staff to consider and specifically present its conclusions on the following matters:

First, an underlying assumption in the staff's rationale for two of its recommendations -- relaxation of compensatory measures for mechanical lock failures for vital area doors (recommendation 1) and relaxation of requirements for access lists for vital areas (recommendation 2) -- is that most persons granted access to the protected area also have access to the vital areas. While this may be true during normal plant operations, it may not be the case during outages, when many contractor employees are brought onsite. In the outage situation, where effective behavioral observation for contractor personnel may be more difficult, it may be appropriate for licensees to limit contractor access to vital areas to reduce any potential for sabotage. Therefore, the staff should carefully evaluate the basis for the recommendations it is making, to ensure that NRC accounts for the fact that the

SECY NOTE: THIS SRM, SECY-92-272, AND THE VOTE SHEETS OF THE
CHAIRMAN AND COMMISSIONER ROGERS WILL BE MADE
PUBLICLY AVAILABLE 10 WORKING DAYS FROM THE DATE
OF THIS SRM

above assumption underlying its two recommendations in this area may not always be valid. The staff should address this point.

Second, if we are to assume that the internal threat has been reduced through implementation of the fitness-for-duty and access authorization rules, it may be appropriate to consider permitting licensee employees to carry their security badges home at the end of the work day, much as we do with our badges here at the NRC. This approach would eliminate the need for employees to first check-in with security personnel solely for the purpose of obtaining a badge. Such a procedure could reduce the time it takes for employees to process into the protected area when they report for work each day. It may additionally allow a reduction in the number of security personnel required at protected area access control points. For these reasons, the staff should evaluate this option, and present its conclusions.

The staff should inform the Commission of the results of its re-examination.

(EDO) (NRR)

(SECY Suspense:

3/5/93)

9100185

cc: The Chairman
Commissioner Rogers
Commissioner Curtiss
Commissioner Remick
Commissioner de Planque
OGC
OIG
Office Directors, Regions (via E-Mail)
OP, SDBU/CR, ASLBP (via FAX)

ENCLOSURE 3

Letter from the United Plant Guard Workers of America
dated January 29, 1993

International Union, UNITED PLANT GUARD WORKERS OF AMERICA (UPGWA)

INTERNATIONAL HEADQUARTERS: 25510 Kelly Rd., Roseville, Michigan 48066
TELEPHONE: (313) 772-7250 FAX: (313) 772-9644



EUGENE P. McCONVILLE
President

LOUIS R. SCOBY
Vice President

RONALD L. WARFIELD
Secretary Treasurer

January 29, 1993

BY FAX (301/504-2260), ORIGINAL BY MAIL

Mr. Robert J. Dube
Section Chief
Regulatory Effectiveness Reviews
U.S. Nuclear Regulatory Commission
Mail Station OWFN 9-D-24
Washington, D.C. 20555

**RE: Regulatory Requirements For Protection Against
The Insider and Impact Of These Requirements
On Operational Safety**

Dear Mr. Dube:

Established in 1948 as a consequence of the Taft-Hartley Act, the International Union, United Plant Guard Workers of America (UPGWA) is the country's largest union of security personnel only in both the private and public sector. The UPGWA represents security officers in every major industry, business, and government facility throughout the United States.

We have bargaining units at government owned, operated or licensed facilities which employ security officers directly or indirectly. The government agencies include NASA, GAO, Navy, Air Force, Army, DOE and others.

Our Union has years of experience with nuclear security at all levels at both DOE and NRC sites. We can make a significant contribution to the consideration of those matters recommended by NUMARC and adopted by the staff.

The comments of the UPGWA should rank with those of NUMARC. After all we speak on behalf of those security personnel who are actually on the front line in providing security at nuclear facilities licensed by the NRC. The UPGWA represents security inspectors and other security personnel at approximately twenty-five (25) nuclear power sites throughout the United States.

While cost containment is a significant factor, it must not reduce the fundamental purpose of security to safeguard persons and property at nuclear sites, and the citizens in the area. We are concerned with

the statement that "While factors for determining potential manpower savings are very site specific, the staff estimates nominal savings of 3 to 5 persons per site, and possible savings of up to 10 persons at some sites." The termination of even one trained and dedicated security inspector is not "nominal savings" to that employee and his family.

The UPGWA has always been a willing partner in legislation, rules and regulations and policies which maintain and enhance the nuclear security profession and advance nuclear safeguards. Such developments, however, must proceed cautiously, and with due consideration for the level of security and those employees who maintain it. For example, Recommendation 3 " . . . to reduce the requirements for responding to nuisance alarms at vital area doors." is frightening. How does one know in advance that an alarm is a nuisance? The very purpose of any alarm is to give warning and evoke a response. An unattended "nuisance alarm" may be the event which triggers a major catastrophe at the site.

It appears that Recommendations 1 through 6 are designed and intended to reduce - not improve - the level of security. While NUMARC's proprietary interest is understandable, cost savings should not compromise security without a compelling showing that certain safeguards are no longer necessary. It does not appear that such a showing has been made as to Recommendations 1-6. Moreover, no provision is made for the possible reduction of security personnel. The Commission, NUMARC, and licensees have a duty to protect the interests of those security inspectors who have given their dedicated service to nuclear security.

The UPGWA respectfully requests that the Commission hold the recommendations in abeyance pending further study and review. Hearings and workshops should be held for the purpose of receiving the views and recommendations of security inspectors and other line security personnel. The UPGWA will attend such proceedings to protect the interests of those men and women whose job security might be threatened by any change in Commission rule or policy.

Thank you for your consideration.

Respectfully submitted,



Louis R. Scohy
International Vice President

LRS/srn/opeiu42

cc: James E. Taylor
E. McConville
G. Gregory, Esq.

ENCLOSURE 4

Analysis of NUMARC's APS
and Alternative Staff Approach

ANALYSIS OF NUMARC'S ALTERNATIVE PROTECTIVE STRATEGY
AND STAFF'S ALTERNATIVE APPROACH

1. ANALYSIS OF NUMARC'S ALTERNATIVE PROTECTIVE STRATEGY.

The staff analyzed NUMARC'S Alternative Protective Strategy (APS) in detail and sought clarification from NUMARC. NUMARC has stated that the recommendations for changes in the APS allowed security resources to be redirected without diminishing the level of security effectiveness. In discussions, NUMARC confirmed that the goal of the redirection was to spend less money on security. NUMARC also reaffirmed that it was seeking to eliminate all requirements identified in its paper on the basis of an equivalency argument, without the need for rulemaking.

NUMARC has stated that the APS can be implemented without a rule change because the strategy provides protection equivalent to certain physical protection requirements contained in 10 CFR 73.55 (b) through (h). NUMARC emphasized that trustworthiness programs, including criminal history checks, fitness-for-duty, access authorization, and behavioral observation programs, enhance protection against an internal threat. In promulgating 10 CFR 73.55, the Commission recognized that the rule was incomplete with respect to insider threat protection and specifically noted that trustworthiness issues would be dealt with separately in further rulemaking. Consequently, the criminal history fingerprint check program has been required by 10 CFR 73.57 since March 2, 1987, the fitness-for-duty program has been required by 10 CFR Part 26 since June 7, 1989, and the access authorization and behavioral observation programs have been required in their current form by 10 CFR 73.56 since April 25, 1991. A behavioral observation program was also required by the fitness-for-duty rulemaking in 1989.

None of these regulations were promulgated as substitutes for any element of 10 CFR 73.55. Although §73.56 is recent, power reactor access authorization programs are not. The statement of considerations for §73.55, published on February 24, 1977, noted that to reduce the vulnerability of operating facilities from an internal threat, the Commission was considering a program to require personnel security clearances for licensee employees. It also stated that licensees should continue to use the employee screening guidance from the American National Standards Institute, ANSI N18.17, "Industrial Security for Nuclear Power Plants," in use at that time. The statement of considerations for 10 CFR Part 26, §73.56, and §73.57 made no reference to these new requirements replacing portions of 10 CFR 73.55.

These trustworthiness requirements complement the physical protection requirements of 10 CFR 73.55. The general performance objective and requirements section of 73.55(a) states that the Commission may authorize a licensee to provide measures for protection against radiological sabotage other than those specified in (b) through (h) if the licensee demonstrates that the measures have the same high assurance objective and that the overall level of system performance provides equivalent protection. Compliance with complementary individual trustworthiness requirements dealing with special aspects of the insider threat are not a substitute for the required physical

protection measures that cover both the external threat and internal security controls of a more general nature not necessarily related to trustworthiness. NUMARC confirmed the staff's initial understanding that the APS does not include any proposals for specific alternative physical protection measures that would provide protection equivalent to that provided by the provisions of 10 CFR 73.55 (b) through (h).

A fifth program identified in the APS is described as a Law Enforcement Intelligence Network. However, on April 4, 1978, the Commission established an agency operating assumption that a prudent and viable safeguards system should not rely for its effectiveness on the accuracy and timely availability of intelligence information concerning the plans, characteristics, and intentions of a hostile adversary. On this basis, safeguards for licensed facilities have been structured to prevent sabotage regardless of whether or not such information is known in advance.

The staff finds merit in some of NUMARC's recommendations that could result in reductions in requirements beyond what the staff proposed in SECY-92-272. However, the staff believes that fully implementing the APS without alternative compensating measures could significantly decrease the ability of some licensees to protect against the external design basis threat and could also decrease, to a lesser degree, the ability of licensees to protect against an internal threat. The staff's basis for this conclusion is discussed below. As a result of this conclusion, staff does not support full implementation of the APS.

Protection Against an External Threat

In support of its proposal, NUMARC contends that the NRC's Regulatory Effectiveness Review (RER) drills have shown that vital area doors are of minimal value as an obstacle to an external threat. The staff disagrees with NUMARC's broad contention regarding vital area doors. RER and Operational Safeguards Response Evaluation (OSRE) teams have observed licensee drills at some sites in which locked doors were not a primary factor in protecting against an adversary with the equipment and training necessary to penetrate the doors quickly. However, at other sites RER and OSRE teams have observed drills in which locked vital area doors or door alarms made an important contribution to the licensee's ability to protect against an external adversary. The value of locked and alarmed doors becomes more important with fewer armed responders available to the licensee and against adversaries that lack the equipment or training necessary to penetrate doors quickly. At a meeting with the staff on January 22, 1993, NUMARC agreed that locked doors are important at some sites in protecting against an external adversary.

The forced vehicle entry into the protected area at TMI also demonstrated the value of alarmed doors. The fact that a vital area door alarm was not generated after the vehicle penetrated the protected area indicated that the vehicle occupant had not gained access to vital equipment.

Protection Against an Internal Threat

NUMARC contends that the APS provides high assurance against an internal threat because personnel granted unescorted access to the protected area are considered trustworthy, reliable, and not likely to become involved in radiological sabotage. However, NUMARC has not provided any studies to support its contention that trustworthiness programs alone provide high assurance against radiological sabotage. The staff agrees that employee trustworthiness is an important element of protection against an internal threat; nonetheless, as discussed above, the statement of considerations for 10 CFR 73.55 noted that the Commission was considering personnel security clearances for licensee employees as an additional measure to reduce the vulnerability of operating facilities from the internal threat. The recommendations made in SECY-92-272 for reducing security requirements were based in large part on the additional confidence in plant personnel provided by the fitness-for-duty and access authorization rules. However, since sufficient examples exist of even more comprehensive trustworthiness programs failing, such as people who have high levels of security clearance committing espionage against their own governments, the staff believes it would not be prudent to place sole reliance on such programs for protecting the public from malevolent acts.

For protection against an internal threat, current requirements designate four diverse groups of measures that complement but are essentially independent of each other. First, a perimeter fence and a badging system ensure that only authorized individuals are permitted unescorted access to the protected area. In conjunction with this, the programs that comprise NUMARC's APS help to ensure that individuals who are authorized to have unescorted access to the protected area are trustworthy. The trustworthiness programs can be effective in helping licensees avoid granting unescorted access to persons who exhibit evidence of undesirable characteristics. However, it is difficult to determine the effectiveness of these programs in detecting (1) an individual who may be predisposed to radiological sabotage and who intentionally tries to conceal that predisposition, (2) an employee with desirable characteristics who may be coerced into tampering with safety equipment, or (3) subtle character changes that may threaten public health and safety.

Second, individuals, packages, and vehicles entering the protected area are searched to protect against the introduction of unauthorized weapons, explosives, and incendiary devices into the protected area. Explosives and, to a lesser degree, weapons and incendiary devices make radiological sabotage leading to significant core damage easier to commit. It also would be more difficult for plant operators to mitigate or provide damage control for sabotage caused by explosives or other contraband than for sabotage created using tools readily available within the protected area.

Third, security officers patrol vital areas, typically at random times using different routes. The unpredictable nature of these random patrols provides some deterrence to anyone considering malevolent acts. Patrolling security officers also could detect insider attempts to sabotage a facility.

Fourth, vital safety equipment is located behind vital area barriers that have locked and alarmed doors. Keycard control systems and computers maintain a record of entry through the vital area doors. However, to operate a nuclear power plant safely, licensee personnel must have prompt access to the same safety equipment that the security systems are supposed to protect. When the staff last conducted a survey, roughly 70 percent of licensee personnel authorized unescorted access to protected areas also had unescorted access to vital areas. Thus, except for outage situations, vital area locks have limited benefit in excluding individuals who do not need access to vital areas to perform their jobs.

If vital areas were highly compartmentalized and individual employees were granted access to only a limited number of vital areas, locked and alarmed doors could provide significant protection against an internal threat. However, because compartmentalization and limited access could also increase the safety risks of locking doors, the staff has allowed licensees considerable latitude in limiting the number of vital areas and granting individuals access to as many vital areas as the licensee deems appropriate. For plants that have few vital areas or that grant access to most vital areas to most people who have access to the protected area, locked doors are for the most part ineffective protection against an internal threat.

The primary benefit of vital area door controls for protection against an internal threat is the deterrent effect of maintaining a record of entry. Access records also are helpful for facility evacuation in safety emergencies and for investigative purposes.

The effectiveness of most measures used to protect against an internal threat cannot be quantified. The staff's assessment that licensee programs provide the required high degree of assurance of protection against an internal threat is based largely on the overall effectiveness achieved by the diversity and independence of measures, rather than on a demonstration that individual measures provide high assurance. Because of the difficulty of quantifying the effectiveness of different types of measures for protection against an internal threat, the staff believes it is important to use diverse measures.

One of the goals of the APS was to reduce requirements without time-consuming rulemaking. However, most of the proposals in the APS involved elimination of security program elements specifically detailed in the regulations. Therefore, the staff finds that most of the proposals in the APS cannot be implemented generically without rulemaking.

2. ANALYSIS OF STAFF'S ALTERNATIVE APPROACH.

NUMARC's APS recommended changes in regulatory positions in four areas: (1) security requirements for vital area access, (2) posting a security guard at containment during periods of frequent access, (3) vehicle escort requirements, and (4) repeated search of on-duty armed security guards. The staff has considered each of these four recommendations.

Vital Area Access Controls

NUMARC proposed to change the first area by eliminating all security requirements, such as for locks and alarms, for vital area doors. As discussed above, this could significantly decrease the ability of some licensees to protect against the external design basis threat. Therefore, the staff believes that the NRC would need to decrease its design basis threat, as requested by NUMARC in Enclosure 5, before it could completely relax these requirements. As directed by the Commission, the staff is reevaluating the design basis threat for radiological sabotage in response to the TMI vehicle intrusion and the World Trade Center bombing. However, the staff developed the following alternative approach that could be expeditiously implemented and should achieve many of NUMARC's goals without requiring a decrease in the design basis threat.

In the staff's alternative approach, the licensee could eliminate or reduce certain vital area access controls upon confirmation that certain other site-specific measures are in place or upon committing to implement these measures. In committing to these measures, the licensee could enable the NRC to reduce vital access requirements using the license amendment provisions of 10 CFR 50.90, or the exemption provisions of 10 CFR 73.5, in conjunction with the provisions of 10 CFR 50.54(p). The staff believes that any costs associated with these optional new commitments could be significantly less than the cost savings potentially resulting from reduced vital area requirements. If many licensees pursued this approach, rulemaking would still be advisable to ensure that the regulations properly reflect generally approved practices.

To obtain approval under this alternative approach, a licensee would have to demonstrate a capability to protect against an external adversary after reducing its commitments for vital area locks, alarms, and other provisions. For some licensees, the results from previous OSREs could serve as a basis for much of this demonstration. Some licensees that have not had an OSRE may have already conducted sufficient drills to demonstrate a continued capability to protect against the design basis threat. Other licensees may have to modify their defensive strategy and demonstrate its effectiveness. Some licensees may choose to continue to lock some or all doors because of site-specific or operational considerations. The staff also would expect the licensees to conduct sufficient contingency drills to periodically confirm the adequacy of their defensive strategy for protecting the plant and to ensure that armed responders are adequately trained. The staff would use future OSREs to confirm the adequacy of the licensees' defensive strategies.

About one third of current licensees also may have to make additional commitments with regard to protection against an internal threat. During RERs, the staff identified a number of licensees that were not searching packages for explosives. Rather than purchase new equipment, many of these licensees rearranged their portal monitors so that people entering the search area carried packages through the portal explosives detector. Although this provided some capability to detect explosives concealed in packages, it was less effective than using one of several types of equipment specifically designed to search for explosives in packages. Having people carry packages through the explosives detector also could potentially decrease the

effectiveness of the portal monitor in detecting explosives concealed on an individual. Because of the other measures in place to protect against an internal threat, the staff accepted this corrective action. However, if other current physical protection measures are eliminated, the staff believes that those licensees not already doing so should commit to examine hand-carried packages using search techniques specifically designed for that purpose.

Recommendations Related to Requirements Associated With Vital Area Access

The staff developed three options for the alternative approach for reducing the requirements for access to vital areas. All three options would provide for expeditious site-specific implementation, but include rulemaking for ultimate resolution.

Option 1 incorporates three of the recommendations for rule change presented in SECY-92-272. However, in addition to proceeding with rulemaking to eliminate selected requirements for vital area controls, the staff's alternative approach would allow expeditious implementation because of alternative licensee commitments that would satisfy the equivalency test of 10 CFR 73.55.

Recommendation 1 would eliminate §73.55(g)(1) requirements for compensatory measures for failure of mechanical lock hardware if the access control hardware and alarm are operable. Although the doors would be temporarily unlocked, an individual would still have to use a keycard for normal access to avoid generating a door alarm. Licensees whose defensive strategy relies on locked doors would be required to supplement their contingency response capability for an external adversary during the period that the doors were unlocked. Compensatory measures at doors would be required for any malfunctions that exceed three days. Current requirements for compensatory measures would be retained for other types of door control failures.

Recommendation 2 would eliminate the §73.55(d)(7)(A) requirement to maintain discrete lists of persons allowed access to each separate vital area and to eliminate the requirement for reviewing the lists every 31 days. Licensees would be allowed to maintain a single list of persons allowed general access to vital areas, without specifying specific areas.

Recommendation 3 would reduce the §73.55(h)(4) requirements for responding to nuisance alarms at vital area doors. Further study is needed to determine the best approach for reduced response. Possibilities include requiring a response to certain types of alarms, such as an alarm that indicates that someone may be tampering with the door alarm, or requiring a response only to a percentage of all alarms.

Option 2 would revise recommendations 1 and 3. Under this option, timeliness requirements for compensatory measures for any malfunctioning element of the vital area access system would be extended from 10 minutes (the time specified for most licensees in their security plans) to a period similar to that permitted in technical specifications for safety equipment to be out of service, typically 1 to 3 days, if either the lock or alarm are operable. Currently, most licensees are required to take compensatory measures within 10

minutes. Failure to do so could require a report to the NRC within 1 hour. This extended period would apply to all types of vital area access control malfunctions, not just to lock failures as in option 1. Licensees whose defensive strategy relies on locked doors or door alarms would be required to supplement their contingency response capability for an external adversary during the period that the doors were unlocked.

Recommendation 3 would be revised to allow licensees to respond only to those vital area door alarms that coincide with an unresolved alarm at the protected area perimeter, a known intrusion, or a constant alarm such as that caused by an open door. Because prompt detection and resolution of a protected area intrusion is essential to protection against an external adversary, licensees must maintain an effective system for resolving perimeter alarms. Licensee capabilities to resolve perimeter alarms improved significantly as observed by NRC's RER program, which was completed in June 1991. The last significant alarm assessment weakness was identified in August 1990. If licensees have maintained effective perimeter alarm resolution capabilities, there should be few door alarms that are coincident with unresolved perimeter alarms.

Option 3 would reduce the §73.55(d)(7)(B) and (D) commitments for locks on vital area doors, except for those doors licensees determine necessary to delay an external threat. This option would allow vital area doors to normally be unlocked, but licensees would be required to retain locking mechanisms and to have the capability to remotely lock the doors from the central and secondary alarm stations in the event of a security contingency. Licensees would have to demonstrate in their 10 CFR 50.90 application that they can protect against the external design basis threat without locks on doors that they normally unlocked, or that the doors can be locked promptly enough if needed as part of the defensive strategy. Compensatory measures for locked doors and response to alarms would be identical to option 2.

Access control systems would also be retained on all vital area doors to maintain a record of personnel access and would generate an alarm in the central alarm station (CAS) and secondary alarm station (SAS) if a vital area door was opened without a keycard. Maintenance of access records would continue to provide some deterrence against an internal threat, although significantly less than current requirements. It would also maintain the current capability of tracking the movement of adversaries in an overt external attack. Licensees would be required to respond to any door alarm that coincided with an unresolved alarm at the protected area perimeter. They would be allowed to respond to other door alarms at their discretion.

Option 3 would further reduce any safety impact of vital area security measures, which is already low, by allowing licensees to leave some or all vital area doors unlocked but still retain alarm systems to detect unauthorized entry. In conjunction with option 1 or 2, the staff also recommends that licensees be encouraged to (1) have the ability to remotely unlock vital area doors from security alarm stations, (2) ensure that malfunctions result in doors failing unlocked rather than locked, and (3) allow all operators and auxiliary operators to carry hard keys that can override keycard lock mechanisms. Recommendation 1 of SECY-92-272 would facilitate allowing operators to carry hard keys by reducing the burden for

key controls for vital area locks. Reducing key controls could be approved without waiting for a rule change as part of a 10 CFR 50.90 application demonstrating a decrease in safety risk.

Under the staff's alternative approach, a licensee's ability to protect against an external adversary would not diminish under any of these options. The staff believes that to retain an adequate capability to protect against an external adversary, a licensee should be required to at least retain the ability to lock vital area doors on demand and to generate an alarm if a vital area door is opened without a keycard. GPU Nuclear Corporation used both of these capabilities in responding to the forced vehicle entry into the protected area at Three Mile Island on February 7, 1993.

Although each of these three options would incrementally decrease the effectiveness of licensee's measures to protect against an internal threat, the staff believes that with the additional licensee commitments discussed previously, licensees could still meet the general performance objective of 10 CFR 73.55(a).

Recommendation Related to Containment Access Control

The second area discussed by NUMARC was the §73.55(d)(8) requirement that guards or watchpersons exercise positive access control to containment to ensure that only authorized personnel and materials are permitted entry any time frequent access is permitted, such as during a refueling outage or major maintenance. NUMARC's APS recommended either deleting the requirement or modifying it to allow access to be controlled by other than security personnel. However, at meetings with the staff, NUMARC stated that their goal was to eliminate the requirement.

NUMARC's recommendation to delete the requirement is essentially the same as staff's rulemaking recommendation 4 in SECY-92-272, which staff still supports. In effect, containment would not have to be treated as a separate vital area. This change would require rulemaking because of the specific nature of 10 CFR 73.55(d)(8) and because NUMARC's APS contains no elements that specifically address alternatives for control of access to containment.

With respect to NUMARC's alternative recommendation, the staff agrees with NUMARC that, except for attempted forced entry, guards or watchpersons have no unique capability for controlling access to containment. The staff believes that the definition of "watchman" is sufficiently broad to allow access to be controlled by persons other than security personnel. However, some licensees may have to amend their security plans if they contain narrower definitions of a watchman or if other duties are assigned to a watchman that require specific security training.

Recommendation Related to Vehicle Escort Requirements

The third area discussed by NUMARC relates to §73.55(d)(4) requirements that vehicles have escorts. The NRC regulations require that, except for designated vehicles owned by the licensee and normally kept in the protected area, vehicles entering the protected area must be escorted by a security

officer. NUMARC recommended that the escort requirement be waived for any vehicles with drivers who have been authorized unescorted access to the protected area, regardless of whether the licensees owned the vehicle, who employed the driver, or the normal location of the vehicle.

The staff agrees that under the conditions indicated in recommendation 6 of SECY-92-272, the 73.55(d)(4) requirement for an escort (in essence, a two-person rule) may not contribute significantly to protection of the public health and safety. Recommendation 6 in SECY-92-272 took a position that would somewhat reduce requirements for escort of non-designated vehicles inside the protected area. The staff proposed that vehicles owned by the licensee and driven by licensee employees who have unescorted access could be driven into the protected area for work-related purposes. In light of the bombing at the World Trade Center, the staff further limits this recommendation to vehicles that can be effectively searched.

The staff was concerned that a policy which was too open ended, as proposed by NUMARC, would significantly increase sabotage risk because of the potential for increased unescorted vehicle presence within the protected area. The staff believes that NUMARC's proposal would not provide sufficient protection in all cases. Specifically, in many instances behavioral observation programs for a non-licensee employee whose regular job is driving a vehicle are less rigorous than for licensee employees. It also is more difficult to effectively search a vehicle and its cargo than to search an individual or a hand-carried package. There is a risk that a vehicle could be used to get unauthorized people, weapons, and explosives into the protected area. In addition, NUMARC's recommendation to reduce control of vehicles is inconsistent with the staff's recommendation in SECY-93-166 to increase protection against the malevolent use of vehicles, in light of the TMI event and the vehicle bomb that exploded at the World Trade Center. The staff considers complete relaxation of the vehicle escort requirement to be excessive.

This issue concerning the extent of controls for vehicles allowed in the protected area is not new. The proposed version of 10 CFR 73.55, published in the *Federal Register* on November 13, 1974, would have limited the admission of vehicles designed primarily for carrying passengers within the protected area to those only designated as emergency or security vehicles except under emergency conditions. Upon consideration of comments received during rulemaking, the Commission concluded that additional transportation, other than for emergency and security purposes, is required in order to perform necessary plant activities. Therefore, the staff modified 10 CFR 73.55 to permit designated licensee vehicles necessary to perform official plant functions within the protected area but with certain necessary controls. NUMARC's proposal would essentially remove all controls.

The staff has been receptive to allowing certain vehicles specified by the licensee to be within the protected area unescorted, in accordance with licensee-proposed controls. The staff has previously approved site-specific requests that were more limited in scope than NUMARC's, but that offered some latitude not included in recommendation 6 of SECY-92-272. However, the staff found some cases in which alternative provisions once permitted were abused.

Therefore, the staff still recommends (SECY-92-272, recommendation 6) that the escort requirements be eliminated only for licensee-owned vehicles entering the protected area for work-related purposes, when these vehicles can be effectively searched for explosives and are driven by licensee employees who have unescorted access. This would require a rule change because it would allow vehicles (other than specially designated vehicles normally kept in the protected area) to be driven into the protected area with only a single occupant.

Recommendation Related to Repeated Search of Armed Security Guards

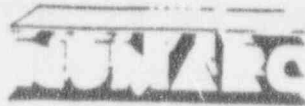
The fourth area discussed by NUMARC was the repeated search of armed security guards exiting and reentering the protected area on official duty, required by §73.55(d)(1). NUMARC recommended that guards be exempt from all search requirements upon reentry. The staff recommended eliminating the metal detector search, but not the explosives search (SECY-92-272, recommendation 5). During followup discussions, NUMARC said the problem of guard reentry to the protected area was exacerbated because some licensees use the same portal for both metal and explosives detection. Since these dual portal detectors generate separate alarms for metal and explosives, the staff modified its original recommendation to allow licensees using dual portal detectors to ignore the metal alarm for on-duty guards carrying a weapon.

The staff discussed its revised recommendation with NUMARC at the meeting on January 22, 1993. Since law enforcement personnel on official duty are exempt from equipment searches, NUMARC asserted that searching licensee security officers implies that they are less trustworthy and that any search, including the search for explosives, would lower the morale of security officers. However, the staff noted that law enforcement personnel entering a protected area are normally escorted.

The goal of eliminating repeated metal detector searches of armed security guards could be expeditiously implemented. Under the provisions of 10 CFR 73.55(a), the staff would authorize alternative licensee procedures that ensure that metal detector searches would be waived only for on-duty security officers who have already been searched during their current shift and who are carrying a weapon in accordance with assigned duties. Final resolution of this item would require a rule change to assure that the regulations are consistent with generally accepted practices.

ENCLOSURE 5

Enclosure 2 to NUMARC Letter
dated December 21, 1993



NUCLEAR MANAGEMENT AND RESOURCES COUNCIL

1776 Eye Street NW • Suite 300 • Washington DC 20006-3706
(202) 672-1280

Joe F. Colvin
President & Chief
Executive Officer

December 21, 1992

The Honorable Ivan Selin
Chairman
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

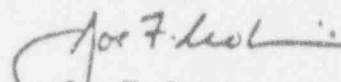
Dear Chairman Selin:

At the June 25, 1992, NUMARC Board of Directors' meeting you discussed the status of the Commission's review of NRC regulations which have unnecessarily increased costs to licensees without a commensurate safety benefit. You requested specific examples of changes to NRC regulations and regulatory processes that the industry believes were appropriate based upon the industry's knowledge and experience in the operation and management of commercial nuclear power plants and the maturity of the nuclear technology. The purpose of this letter is to provide you with our initial response and, because of the importance of this matter, to request expedited Commission action in the areas identified.

The Executive Summary (enclosed) provides a brief description of the initial results of our review. Attachments 1 through 8 discuss specific issues where we believe immediate action can be taken without further study or analysis. Attachments 9 through 11 address longer-term issues where efforts need to be commenced in the near future to effect positive change in the needed time frames. In addition, we ask the Commission's consideration of the industry's comments on the Systematic Assessment of Licensee Performance (SALP) program, which were submitted on October 20, 1992 (copy included as Attachment 12), where we believe significant changes are also warranted. We will be forwarding information on other issues for your consideration as our evaluations continue.

We look forward to working with the Commission and the NRC staff to address these matters, which are of critical importance to the industry. Because cost control is an urgent problem to the industry, we would like to meet with the Commission in early January to discuss these and related issues to facilitate their timely resolution.

Sincerely,


Joe F. Colvin

SECURITY

The major industry concerns related to plant security are addressed in this attachment as seven specific issues. Each is described below with recommended actions and the associated rationale.

ISSUE # 1

Section 73.1(a) specifies the potential radiological terrorist threat basis (i.e., the design basis threat) that the licensee's physical security plan must address. World conditions have changed significantly since 1977 when the design basis threat was promulgated. In order to bring plant security programs into line with today's environment, a reassessment of the design basis threat is appropriate.

ACTIONS NEEDED

Reassess the present design basis threat (DBT) taking into consideration what has been implemented internationally; modify § 73.1(a) where applicable to reflect the terrorist threat (both external and internal) of today. Update the methods used for periodic threat assessments.

DISCUSSION

Although it is reviewed every six months by the Commission, there has been minimal change in the DBT since 1977, even though the world situation has changed markedly. Terrorism is nearly non-existent in the U.S. today. In the introduction to the FBI's 1991 report on Terrorism in the United States (Reference 1), Director Sessions states *"Terrorism inside the United States continued at a low ebb and none of the five incidents recorded [in 1991] were associated with international terrorism."*

The FBI has been recording and analyzing terrorist incidents for over ten years. It published a report (Reference 2) on terrorist incidents occurring in the period 1980 to 1986 in December of 1986. Discussing the 190 terrorist incidents that occurred in the United States and Puerto Rico during these years, the report notes that New York alone accounted for 52 of these (39 percent). The FBI notes that, *"This is not unexpected since New York, particularly New York City, has a high concentration of Government buildings, diplomatic establishments, national monuments and world - renowned commercial and cultural institutions."* During that period seven known terrorist groups were active in New York. More recently, in the FBI's report for 1990 (Reference 3), seven terrorist incidents were recorded - five in Puerto Rico and two in California. Of the two in California, one involved an explosive device detonated in a car parked within sixty feet

of a building containing the offices of the Internal Revenue Service (IRS), and the other involved power poles that were discovered sawed in half. Of the five terrorist incidents recorded by the FBI in 1991 (Reference 1), four occurred in Puerto Rico and one in California. The incident in California involved numerous explosive devices detonated in the parking lot and on the roof of an IRS center. These attacks were not directed against installations as secure as nuclear power plants. Importantly, in this same two year period, nine terrorism preventions were also recorded. Such precautions are the primary goal of the FBI's Counterterrorism program.

The industry is not suggesting that terrorism should no longer be considered a threat in the United States. Director Sessions noted that because a segment of the world community views this activity as a legitimate means of promoting group ideologies, "*...we in the United States must maintain our strong, proactive position against terrorism.*" However, the profile of the terrorist or terrorist group and the motivation to target a commercial nuclear power plant needs to be examined. A review of terrorist incidents over the last five years reveals that the people taking part in these attacks are very different from the personifications of the DBT used in regulatory effectiveness reviews (RER) and operation safeguards response evaluations (OSRE). It indicates that terrorists are likely to lack the training, weapons and education that are considered in the DBT.

Historically, special interest terrorist groups have chosen targets that represented or sympathized with the government or cause the group opposed. People opposed to nuclear power have chosen to demonstrate at the plant, seek media time and other activities to express their point of view to mass audiences. None of these groups match the description of the DBT. In the discussion of a behavioral science approach to understanding terrorists in its 1990 terrorism report (Reference 3) the FBI states, "*Terrorists carefully assess which targets are most vulnerable, and may conduct surveillance to further develop their intelligence on a target. They select operations that pose a minimum of risk with a maximum chance of success.*" The well-lighted protected area, the perimeter fence with its barbed wire and the armed security personnel alone should be more than sufficient to convince the known terrorist groups to look elsewhere for targets of opportunity.

Terrorist activity in other countries is greater than in the United States. For example, in its report on the patterns of global terrorism in 1989 (Reference 4), the Department of State noted (page 9) that in the spillover of international terrorism from the Middle East, 23.3 percent of the incidents involved the United Kingdom while 6.9 percent involved the United States. In the list of significant terrorist - related events in 1989, none were identified as occurring in the United States, while nine occurred in Europe.

Even though more terrorism is experienced in other countries, it appears that the security requirements for commercial nuclear power plants there are not as prescriptive as in the United States. For example, information from U.S. utility personnel who had just returned from Europe indicates that a commercial nuclear plant they visited uses the IAEA standards as guidance for security provisions. This facility does not perform random drug testing, does not have a continual employee behavioral observation training and has no employee assistance program. The security officers at this site carry no weapons, and plant worker identification badges required to gain entry into the protected area are carried home by each employee. No search devices (x-rays, explosive detectors, etc.) are used, although the plant retains the right to search all persons entering the protected area; security force manning is approximately six officers per shift. Entering a radiological control area requires two independent forms of identification (i.e., picture badge and assigned dosimeter). The basic philosophy with respect to protection against an outside threat is to make the site more secure than other political targets of opportunity, such as banks, churches, etc. The continued absence of terrorist incidents at operating nuclear power plants worldwide confirms this philosophy.

Instead of the current practice of maintaining a large, well-armed response force at the plant to counter a well-trained paramilitary force, the NRC should consider adopting a system of declaring alert stages of based on intelligence assessments. The FBI is committed to monitor for, confront and handle acts of nuclear terrorism. As noted above, the primary goal of the counterterrorism program is prevention. Logic similar to that outlined in Generic Letter 89-07 could be used. Licensees would continue to provide high quality security for the plant site. When the intelligence networks operating at the local, state and federal levels determined the possibility of increased threat to one or more facilities, the licensee would be alerted. Augmentation of site security measures would be determined based on the nature of the increased threat.

It is extremely important to re-assess the DBT. In the next four issues to be discussed, the DBT affects how these subjects are addressed. In the discussion portions of SECY-92-272, the staff's arguments clearly agree. It is our understanding that the staff positions in SECY-92-272 are based on the current DBT. We strongly recommend that the Commission avail itself of the most up-to-date assessments by federal intelligence gathering agencies. A reevaluation of the DBT will greatly simplify the resolution of the security issues which follow.

ISSUE # 2

Section 73.55 requires the use of locked and alarmed doors between protected and vital areas as part of plant security inside the protected area. Upon receipt of a door alarm in a vital area, security personnel are required to respond and to investigate. Additionally, if the security system for a door becomes inoperable, compensatory measures are required within 10 minutes. Vital area doors are given little or no value as either a deterrent to the insider threat or to would-be external saboteurs. Conversely, these doors could impede personnel movement during time of emergency.

ACTION NEEDED

Remove the requirement to maintain vital area door locks and alarms as part of the physical security plan.

DISCUSSION

Threats to nuclear plant security fall into two categories -- internal and external. The internal, or "insider," threat is described as a lone person with unescorted access and the knowledge and opportunity to commit radiological sabotage. The rationale behind key-carded vital area doors is that they limit entry only to those having vital area access and would deter unauthorized persons from entering. Since most persons with protected area access are granted vital area access as well, the distinction between these authorizations is not significant. As noted on page 32 of SECY-92-272:

"Locks on vital area doors are only marginally effective in protecting against the insider because (1) most persons at many sites who are granted access to the protected area also have access to all vital areas by card key and, (2) vital areas at many sites are not highly compartmented which allows broad access to many vital areas."

The external threat is assumed to be a well-trained paramilitary force of several individuals equipped with weapons and explosives. Intrusion detection systems and perimeter barriers are designed to detect and hamper the penetration of such a threat. The external threat would also encounter an armed response from the plant security force. It is anticipated that vital area doors would not be a serious obstacle for any intruding force sufficiently strong to neutralize both the perimeter barriers and the armed response. Indeed, several NRC regulatory effectiveness reviews have concluded that locked vital area doors would delay the external threat by only 10 to 15 seconds.

Vital area doors, therefore, add little value to the protective measures against the internal and external threats and constitute a resource burden that must be monitored, responded to, and repaired. Due to the number of vital area doors, the frequency of

alarm malfunctions and the expected response time, numerous guards are often required to fulfill the 10 minute compensatory requirement (NUREG-1045). The compensatory measures for security far exceed what is required for systems designed to protect the fuel. For example, when two Emergency Core Cooling System (ECCS) injection subsystems are inoperable, the licensee has 72 hours to restore one ECCS injection/spray subsystem to operability or bring the unit down (NUREG-1434, page 3.5-2).

On the other hand, locked doors to vital equipment could be a hindrance in an emergency as has actually been experienced in the past. For example, experiences during the Davis-Besse event of June 1985 and the Limerick event of July 1986 demonstrated the ways in which locked vital area doors hinder prompt response in an emergency.

NUREG-1154 (The Davis-Besse Event 6/9/85) - Page 3-7

"As the operators ran to the equipment, a variety of troubling thoughts ran through their minds. One operator was uncertain if he would be able to carry out the task that he had been directed to do. He knew that the valves he had to open were locked valves, and they could not be operated manually without a key. He did not have a key and that concerned him. As he moved through the turbine building, he knew there were numerous locked doors that he would have to go through to reach the valves. He had a plastic card to get through the card readers, but they had been known to break and fail. He did not have a set of door keys and he would not gain access if his key card broke and that concerned him too."

IN 86-55, July 10, 1986 - Delayed Access to Safety Related Areas

"During a Limerick remote reactor cooldown demonstration on September 11, 1985, a reactor core isolation cooling (RCIC) injection valve failed to open automatically and it became necessary for an operator to enter this locked area to manually open the valve. At this point the operator discovered that the compartment and equipment access keys had not been made available for the remote shutdown function. A technician was requested to obtain a key to the RCIC area from a set maintained by the health physics personnel. However, the technician had the wrong key when he met the operator at the RCIC area 15 minutes later. When the operator finally got the right key and entered the area, he found the valve handwheel chained and locked. Neither the operator nor the operating crew back at the remote shutdown panel had a key for this lock. Bolt cutters finally were located and the chain was cut. Again this problem was resolved without the occurrence of any damage. However, this event occurred early during plant startup when the decay heat was low and the control rod drive system was able to provide sufficient water for makeup. Had an actual emergency required abandonment of control room following full-power operation, it

questionable whether the operators would have been able to take the necessary action in a timely manner."

In SECY-92-272, the staff has suggested that all personnel anticipated to need emergency access be given keys to vital area doors. As actually experienced during the events cited above, valuable time could be lost locating the correct key.

In a June 24, 1992 letter to B.K. Grimes (Appendix A) the industry suggested that the likelihood of the insider threat has been reduced because of the additional regulatory requirements addressing access authorization and fitness-for-duty. Through background and criminal history investigations, psychological evaluations and other trustworthiness checks, together with continual behavioral monitoring, these programs give reasonable assurance of the continuing integrity of the nuclear power plant workforce. As noted in NUREG-0525, there have been no instances of radiological sabotage and one report of non-radiological sabotage. That event occurred in May 1986 when three of four transmission lines outside the protected area of Palo Verde were sabotaged.

It is not possible to conclude that the insider threat has been completely eliminated as a result of these programs. However, they do address the insider threat without the potential adverse impact on plant safety that locked doors to vital equipment introduce. The history of the past twenty years of commercial nuclear power experience demonstrates the absence of such incidents, and current programs provide additional assurance that the pattern will continue. Positive, constructive programs such as the encouragement of more professionalism, the development of teamwork, and accountability are even more powerful means of discouraging a worker from doing something to harm his/her fellow workers or the plant equipment than the negative flavor associated with locked doors, guards, etc. Something valuable has been lost when a 20-year plant operator looks at all the protective measures and thinks, "They don't trust me."

In summary, the locked doors are acknowledged by the staff to add little in the way of protective measures. Based on actual plant experience, locked doors may actually impede response in an emergency and may be less effective than more positive ways of discouraging sabotage and other malevolent acts inside the plant. The requirement for locked vital area doors should be eliminated.

ISSUE # 3

Section 73.55(d)(8) requires a guard or watchman to be posted at the containment entrance during times of frequent access to control entry of personnel and material. This is essentially an administrative function that does not enhance plant security.

ACTION NEEDED

Delete the requirement for a guard or watchman to be posted at the containment entrance to control access of personnel and material. This should apply whether the entrance to the containment is from a vital area or the protected area. Otherwise, the industry supports the staff proposal outlined in SECY-92-272.

DISCUSSION

The performance of this monitoring is more logically the responsibility of operations or maintenance rather than the security force. The purpose of such controls should be, for example, fire prevention and tool accountability. Additional security precautions at this point are redundant, unnecessary, and an inefficient use of licensee resources.

Except for verification that an individual can be allowed in containment, no significant security value provided by a guard or watchman posted at the containment entrance. The guard is not required to search material going into the containment; this is not necessary since each individual has gone through the required screening before being allowed to enter the protected area. Additionally, the individual carrying tools or material into containment is not questioned by the guard as to their use inside containment; nor is there any follow up to verify how the tools or materials were actually used.

ISSUE # 4

Section 73.55(d)(4) requires all vehicles, except designated licensee vehicles, to be escorted by a member of the security organization while in the protected area. In light of existing access authorization requirements for personnel, this requirement is unnecessary when the vehicle driver has been granted unescorted access.

ACTION NEEDED

Modify the regulations so that any security-searched vehicle driven by an individual with unescorted access may be driven inside the protected area without a security escort. Although it does not completely resolve the issue, the industry supports the staff proposal as outlined in SECY-92-272 to modify § 73.55(d)(4) to waive the escort requirement for all designated licensee vehicles.

DISCUSSION

Prior to entry into the protected area, a vehicle is subjected to a search in accordance with § 73.55(d)(4). The vehicle's driver is also searched as are all personnel entering the protected area. If the driver has been granted unescorted access to the protected area, he/she is deemed to be trustworthy and reliable based upon his/her participation in the access authorization and fitness-for-duty programs. The industry agrees with the staff's statement in SECY-92-272 that *"...this [escort] requirement does little in protecting against the insider."*

There is minimal value added to safe plant operation for a driver possessing unescorted access authorization to have a security escort while operating a vehicle in the protected area. If this person was on foot within the protected area, no escort would be needed. The fact that the driver is operating a vehicle in no way degrades his/her reliability or trustworthiness.

Some vehicles are difficult to search. However, as with the fitness-for-duty program, searching the vehicle does provide deterrent to the concealment of contraband. If explosives were concealed in the vehicle without the driver's knowledge and these went undetected in the search, the presence of the security officer escort would achieve little since the escort would not search the vehicle further once it is within the protected area.

ISSUE # 5

Armed security officers who have left the protected area in the performance of their duty must be re-searched before they can again enter the protected area. Section 73.55(d)(1) requires that all persons be subjected to an equipment search for firearms, explosives, and incendiary devices prior to entering the protected area. But, federal, state, and local law enforcement personnel on official duty at the plant site are specifically exempted from these searches. Thus, these personnel may enter the protected area without passing through search equipment. In Generic Letter 87-08, the staff has interpreted this regulation to exclude on-duty plant security guards from this exemption.

ACTIONS NEEDED

Delete the requirement to re-search armed security guards who leave the protected area in the course of their duties and remove the distinction between law enforcement officers in § 73.55(d)(1) and licensee security personnel. The industry supports the staff proposal outlined in SECY-92-272 to not require re-searching armed guards for firearms.

DISCUSSION

Neither law enforcement officers nor on-duty licensee security personnel should be searched when entering the protected area. Members of a licensee's security force are provided unescorted access based upon stringent screening controls including access authorization, fitness-for-duty, and continual behavioral observation programs. Law enforcement personnel on official duty are exempt from detector/pat-down searches but the licensee's on-duty, armed security guards are not. This implies that law enforcement officers are more trustworthy than the plant's own security officers. (Appendix A, p. 13). No basis is given for this distinction.

The industry supports the staff's proposal to eliminate re-search of an armed guard for firearms prior to re-entering the protected area. Clearly, conducting a firearms search on an individual who is authorized to carry a weapon within the protected area is an incongruous activity.

However, the staff recommends that guards be re-searched for explosives. The industry does not support this recommendation. The officer was searched for explosives when he/she reported for duty. There have been no instances where security guards have been found attempting to bring explosives into the protected area. The security officer is trusted to perform a thorough search of vehicles before entering the protected area and is allowed to carry firearms inside vital areas while on patrol while the plant is

at full power. It is only logical to trust him/her to re-enter the protected area without a re-search for either firearms or explosives.

At many sites there is little practical consequence to requiring the guard to pause for the requisite time in the explosives detection portal. There are some sites, however, where both metal and explosives detection is accomplished in the same portal.

The re-search requirement for firearms and explosives on armed on-duty security officers should be eliminated.

ISSUE # 6

Current one-hour reporting requirements for safeguards events can place an unrealistic burden on licensee personnel by requiring the prompt collection and reporting of detailed and accurate facts regarding many events that may take several hours of investigation to confirm. Only confirmed security incidents should be reported under this event classification.

ACTIONS NEEDED

Delete § 73.55 from the list of licensees subject to the provisions of § 73.71(b)(1) and Part 73, Appendix G. Separately, require § 73.55 licensees to report in accordance with the industry's recommendations, "Safeguards Incidents to be Reported Within One Hour," provided in Enclosure 6 to a September 30, 1992 letter to D.L. Meyer (Appendix A to Attachment 5). Include these reporting criteria in a separate section of Appendix G for § 73.55 licensees.

DISCUSSION

A one-hour report, which is currently initiated upon event discovery, frequently results in incomplete and/or inaccurate information being provided that must later be supplemented, revised, or in some cases, withdrawn. The industry has proposed a methodology that would focus on malevolent incidents that actually occur and/or require immediate NRC attention. It is suggested that the term "incident" be used to differentiate between routine safeguards events (e.g., CCTV camera failure) and the more significant events such as a credible bomb threat. These safeguards incidents should be reported within one hour of confirmation (not discovery). This will avoid unnecessary confusion and public concern caused by inaccurate information being used to meet the one-hour reporting requirements. Safeguards incidents can subsequently be documented by each licensee, following an appropriate cause determination, with the record being available for tracking, trending and review by the NRC during routine inspections.

NUMARC transmitted the industry's recommendations and rationale for changes to the one-hour reports to the NRC on September 30, 1992 (See Appendix A to Attachment 5). In the development of these recommendations, the industry was aware of the policy revisions contained in Generic Letter 91-03 and the changes to the guidance in Regulatory Guide 5.62 and NUREG-1304. It appears that the modifications provided by Generic Letter 91-03 have resulted in the elimination of many of the unnecessary reports. The recommendations transmitted in the September 30, 1992 correspondence (Appendix A to Attachment 5) were developed using both industry experience identifying and reporting safeguards incidents and the contents of Generic Letter 91-03. These additional refinements will correct the remaining deficiencies.

ISSUE # 7

Section 73.71(c) requires each licensee to submit to the NRC copies of all safeguards event log entries not previously submitted. The quarterly submittal of the Safeguards Event Log does not provide useful information to measure and trend security system performance.

ACTIONS NEEDED

Delete § 73.55 from the list of licensees subject to the provisions of § 73.71(c). Establish a separate paragraph in § 73.71 requiring § 73.55 licensees to record safeguards events using the industry-developed "Guidelines for Recording Safeguards Events," (See Appendix A to Attachment 5) in lieu of paragraphs II (a) and (b) of Appendix G.

Delete all references to § 73.55 licensees in Regulatory Guide 5.62 and NUREG-1304. In Generic Letter 91-03 delete applicability to "nuclear power reactor" licensees.

DISCUSSION

The NRC's rationale for the safeguards events reporting and logging requirements is contained in the transcript of an NRC meeting held on September 14, 1987, concerning "Reporting Requirements for Safeguards Events." Mr. Joseph Yardumian (Safeguards Inspection Branch, Office of Nuclear Material Safety & Safeguards) on page 28 stated that, in *"the latter part of 1975, the agency started to get inquiries from public interest groups, from journalists, from some of the Nader organizations. And in response to that, we started preparing lists of safeguards events to be able to answer those sorts of inquiries."* Further, on pages 37 and 38, he stated: *"...we are looking for pertinent data; not great volumes of trivia. Whether or not this system is useful, provides useful products, and is helpful to us both is our joint concern, ..."* *"We do not intend, in a resource short environment, to either burden you or ourselves with products or a system that is not going to be very useful."* *"And if it ain't no good, we ain't going to do it."*

Five years later, the "products" and the "system" referred to above are judged to have little value to the industry. Comments received from the industry confirm that licensees receive insignificant meaningful information from the NRC's quarterly "Safeguards Events Analysis Report." Further, counterproductive uses of these data have occurred. The NRC's Safeguards Summary Event List, NUREG-0525, Revisions 16 and 17, were used as the main source of a Public Citizen report, dated January 1992, entitled "Safeguard Slip-Ups: A Review of Security Breaches at U.S. Commercial Nuclear Power Plants." Public Citizen's January 10, 1992, press release on "Safeguard Slipups" states that *"...security at the nation's commercial nuclear power plants is being compromised..."* Citing information from NUREG-0525, the Public Citizen report contains more than 350

descriptions of safeguards events reported by nuclear utilities during the years 1988, 1989 and 1990. Quoting a Public Citizen spokesman, the press release noted, "The large number of security breaches regularly occurring at the nation's nuclear power plants underscores the potential for an accident caused by error or malfeasance by plant workers or others." These observations stretch an innocuous one safeguards event per unit per year into serious charges.

Current safeguards event logging and reporting requirements pose an undue burden on licensees to prepare, review and submit and on the NRC to receive, review, and maintain; these reports have minimal value in determining actual security system performance. Licensees are routinely expending limited resources identifying what needs to be logged and reported. Current guidance is not clear and is spread among several documents (e.g., Regulatory Guide 5.62 and NUREG-1304). The requirements focus attention on specific safeguards events (e.g., closed-circuit television failures, door alarms, card reader failures, uncontrolled badges, unsecured doors, uncompensated posts, etc.) rather than on actual system performance as it relates to overall plant safety.

In many cases these individual safeguards events are accorded undue significance. For example, one licensee reported 213 door events (e.g., failure to latch) during one calendar quarter and was criticized by the NRC regional office for not promptly solving this "problem." In fact, there had been approximately 1,685,000 door operations at that plant during that quarter; this implies a proper operation rate of 99.9 percent, which is a performance level worthy of NRC praise. As another example, the NRC's safeguards event analysis report for the second quarter of 1992 noted that, "42 turnstile events occurred at 18 facilities." Assuming that only 400 people go through a turnstile at each of the 74 sites, five days a week for 12 weeks, the turnstile equipment will operate 1,776,000 times. Forty-two failures or malfunctions indicates a proper operation rate of 99.997 percent. In addition, the safety significance of these events, if any, is not provided.

Efforts to measure the effectiveness of security systems should focus on vulnerabilities that would impair the protection of the public health and safety. Licensees could continue to be effective in this regard with minimal logging and reporting regulation. The recommendations above for simplifying § 73.71 were developed to facilitate power reactor safeguards logging and reporting programs that would provide meaningful information on events of significance to security system effectiveness. Specifically, the suggested new paragraph in § 73.71 would read, "Each licensee subject to the provisions of § 73.55 shall establish measures to assure that safeguards events such as failures, malfunctions, deficiencies, deviations, defective material and equipment are promptly identified and corrected. Each licensee will track and trend the site's performance against licensee-established benchmarks that are based on the specific operating circumstances. Each licensee shall record safeguards events using the 'Guidelines for Recording Safeguards Events' in Appendix G. Records shall be retained for at least two

years and made available to the NRC during routine inspections to demonstrate that the information is being recorded, analyzed, and used to correct deficiencies."

Individual nuclear site security programs have significant differences between them that must be taken into account when comparing security system performance data. The number of events reported by each site is dramatically influenced by the number and design of system components, unique physical arrangements, personnel transactions and other variables. Hence, the use of this data for detecting generic trends in industry security system performance is not meaningful. In addition, some licensees have developed backup systems and pre-established compensatory posts so that certain classes of security system failures are not reportable. In other cases, events are not recorded because the licensee is able to demonstrate that circumstances were such that the event did not degrade the effectiveness of the security system. These differences preclude meaningful comparisons of security system performance parameters and access performance based on the safeguards event logs submitted to the NRC. The industry believes the real benefit in recording safeguards events lies in its usefulness to the individual licensee as a management tool to measure a plant's specific performance, independent of other facilities. Continuing to prepare reports from these logs for quarterly submission to the NRC needlessly diverts both industry and NRC resources.

REFERENCES IN SECURITY ISSUES

1. Terrorism in the United States - 1991, U.S. Department of Justice, Federal Bureau of Investigation, Washington, D.C.
2. FBI Analysis of Terrorist Incidents in the United States - 1986, U.S. Department of Justice, Federal Bureau of Investigation, Washington, D.C., December 31, 1986.
3. Terrorism in the United States - 1990, U.S. Department of Justice, Federal Bureau of Investigation, Washington, D.C.
4. Patterns of Global Terrorism: 1989, U.S. Department of State, Washington, D.C., Publication 9743, April 1990.

ENCLOSURE 6

Response to Commission Requests
for Additional Staff Considerations

STAFF RESPONSE TO COMMISSION REQUESTS FOR ADDITIONAL CONSIDERATIONS

In its memorandum of November 5, 1992, the Commission asked the staff to consider two matters related to access controls and specifically present its conclusions on them.

Security Measures During Outage Situations

The Commission's first question was the following:

First, an underlying assumption in the staff's rationale for two of its recommendations -- relaxation of compensatory measures for mechanical lock failures for vital area doors (recommendation 1) and relaxation of requirements for access lists for vital areas (recommendation 2) -- is that most persons granted access to the protected area also have access to the vital areas. While this may be true during normal plant operations, it may not be the case during outages, when many contractor employees are brought onsite. In the outage situation, where effective behavioral observation for contractor personnel may be more difficult, it may be appropriate for licensees to limit contractor access to vital areas to reduce any potential for sabotage. Therefore, the staff should carefully evaluate the basis for the recommendations it is making, to ensure that NRC accounts for the fact that the above assumption underlying its two recommendations in this area may not always be valid. The staff should address this point.

The staff agrees with the Commissioners' observation that during some situations, such as outages, the staff's assumption may not always be true that most persons granted access to the protected area also have access to vital areas. However, the staff notes that access authorization and fitness-for-duty program requirements do not change on the basis of plant status. Therefore, the staff does not consider that there would be a substantial increase in risk on the basis of the trustworthiness and reliability of individuals granted unescorted access. Further, most contractors working during an outage would likely require access to vital areas to perform their work. As the fitness-for-duty and access programs mature, most of these individuals should have a substantial behavioral observation history at their place of employment as well as at sites where they have worked. Also, following plant shutdown, the risk of consequences from radiological sabotage is significantly reduced because of the plant operational mode.

The access authorization rule does allow for special access provisions during certain extended outages. These provisions must be specifically approved by the NRC as part of a license amendment. This would allow the staff to assess and specifically approve special provisions to ensure protection against sabotage during major long-term plant outages during which large numbers of contractor personnel may need special plant access.

The staff has carefully evaluated the basis for its recommendations and still concludes the resulting decrease in the security diversity and effectiveness

resulting from a relaxation of vital area controls would be acceptably small even during periods of plant outage.

Carrying Badges Off Site

In its memorandum of November 5, 1992, the Commission asked the staff to consider permitting licensee employees to carry security badges home. Paragraph 10 CFR 73.55(d)(5) requires individuals not employed by the licensee, who are authorized unescorted access to the protected or vital areas, to return a picture badge upon leaving the protected area. Although 10 CFR 73.55 does not prohibit licensee employees from keeping their badges when leaving a protected area, practices and policies have evolved into security programs that are very restrictive in control of badges. Currently, some licensee programs permit badges to be taken between two separate protected areas on a single licensee site, with controls to ensure that the badges do not leave the owner-controlled area. No licensee programs permit licensee employees to take their badges outside the owner-controlled area. One major concern is that if badges are not properly controlled, they could be stolen or counterfeited, and the coding system that would allow unauthorized personnel to gain access to the protected and vital areas could be copied.

The staff will consider security plan amendment applications, filed in accordance with 10 CFR 50.90, or exemption requests as provided by 10 CFR 73.5 in conjunction with the provisions of 10 CFR 50.54(p), that would allow licensee employees to carry badges home if the licensee commits to safeguards measures to protect against unauthorized persons from using a stolen or counterfeit badge to gain access to the protected and vital areas of the plant. Recently, one licensee has proposed an access control approach that includes a hand geometry system that uniquely identifies an individual. This approach is currently under review by the staff and may prove an acceptable alternative to maintaining control of badges at the site. Acceptable alternatives also could be developed based on the use of a personal identification number to gain entry to the protected area.

Some licensees may choose not to pursue this approach because of operational considerations, such as the need to retain personnel to issue badges to visitors or vendors or the use of badges for multiple purposes such as radiation dosimetry and personnel accountability during safety emergencies.