corrected to notation vote on 9/25/92

POLICY ISSUE

(NEGATIVE CONSENT)

August 4, 1992 SECY-92-272

For: The Commissioners

From: James M. Taylor
Executive Director for Operations

Subject: RE-EXAMINATION OF NUCLEAR POWER PLANT SECURITY REQUIREMENTS ASSOCIATED WITH THE INTERNAL THREAT

Purpose: To inform the Commission of the results of the staff's analysis of the appropriateness of security requirements associated with the insider threat and to receive approval for the intended action by the staff.

Background: In a memorandum of September 3, 1991, (COMFR-91-005) the Commission requested the staff to re-examine the NRC's nuclear power plant security requirements imposed by 10 CFR Part 73 to determine if the requirements associated with the internal threat might impair the ability of an operator to safely operate the plant. The Commission directed the staff to consider whether or not the security requirements remain appropriate in light of the recent regulations concerning fitness for duty and access authorization.

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

Contact:
Phillip F. McKee, NRR
504-2933

Discussion: The staff has completed its evaluation and documented its findings in Enclosure 1.

The staff evaluation documents the extensive regulatory history of measures established to protect against the insider and documents past actions to address potential safety impacts associated with these measures. The staff found that present implementation of requirements to protect against the insider at power reactor sites does not adversely impact plant safety.

The report identifies a number of regulatory requirements associated with the insider threat that appear to be only marginally effective. The report includes recommendations for reducing or deleting certain of these requirements based upon their marginal effectiveness, and based on the additional confidence in plant personnel provided by the fitness-for-duty and access authorization rules.

In the report, the staff also recommends issuing generic correspondence to state the NRC's position more explicitly in two areas: (1) the acceptability of vital islands and (2) the designation of certain types of documentation as safeguards information. By clarifying its position in these two areas, the NRC would encourage some licensees to make changes to their security programs to improve the efficiency of their operations.

The staff recognizes the importance of properly implemented access authorization programs and is developing an inspection plan to ensure that this program is appropriately implemented.

In a letter of June 24, 1992, the Nuclear Management and Resources Council (NUMARC) gave the NRC a June 1992 paper, "NUMARC Protective Measures Requirements Re-evaluation"

(Enclosure 2). In this paper, NUMARC recommends eliminating certain security requirements for protecting against the insider threat. NUMARC describes an alternate protective strategy as a basis for the recommended changes. NUMARC asserts that this strategy provides protection equivalent to that provided by the requirements proposed for deletion. The licensee's fitness-for-duty and access authorization programs are the main elements of NUMARC's alternate strategy. The four areas in which NUMARC proposed changes are security requirements for vital areas; posting a security guard at containment; vehicle escort requirements; and re-searching on-duty armed security guards. Each of these areas are covered in detail in the staff's report. While the staff does not entirely agree with the NUMARC rationale, the staff recommendations arrive at similar practical results in each area.

The recommendations contained in the enclosed staff report should serve to allow licensees to reduce security force staffing at power reactor facilities. 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.

Recommendation: Unless directed otherwise by the Commission, the staff will proceed with implementation of the nine recommendations in the enclosed report as part of its normal activities. The staff also plans to publish the enclosed report as a NUREG document and will request comments on the report in a Federal Register Notice. These comments will be used in developing the proposed rule

changes and should assist the staff in expediting this process. The rule changes will be reviewed by the CRGR.

James M. Taylor
Executive Director
for Operations

Enclosures:
1. Regulatory Requirements for Protection Against the Insider and Impact of These Requirements on Operational Safety
2. NUMARC letter to B. K. Grimes dated June 24, 1992

SECY NOTE: In the absence of instructions to the contrary, SECY will notify the staff on Tuesday, August 18, 1992, that the Commission, by negative consent, assents to the action proposed in this paper.

DISTRIBUTION:
Commissioners
OGC
OCAA
OIG
OPP
REGIONAL OFFICES
EDO
ACRS
ASLBP
SECY

CONTENTS

EXECUTIVE SUMMARY

In a memorandum of September 3, 1991, the Commission directed the staff to re-examine the Nuclear Regulatory Commission's (NRC's) nuclear power plant security requirements imposed by Part 73 of Title 10 of the Code of Federal Regulations (10 CFR Part 73) to determine if those requirements regarding the internal threat remained appropriate in light of the recent regulations concerning fitness for duty (FFD) and access authorization. The Commission directed the staff to consider whether or not the security requirements impair the ability of an operator to safely operate the plant. This report presents the results of the staff's examination.

The staff documented the extensive regulatory history of measures established to protect against the insider and documented the actions taken to address potential safety impacts associated with security measures.

The staff also thoroughly reviewed all safeguards measures required by regulation. The staff determined which requirements pertain to physical protection against the insider and the safeguards requirements that could affect safe plant operations, whether or not associated with the insider threat. For the purposes of study the staff eliminated security requirements primarily related to the external threat and arranged the remaining security program elements into the following nine categories:

A. protected area perimeter systems
B. search equipment and protected area access controls
C. access authorization programs
D. fitness-for-duty programs
E. vital area barriers
F. vital area access controls
G. vital island/compartmentalization
H. security patrols and response to alarms
I. safeguards information

The staff analyzed each of these areas in detail and found that none of the measures individually significantly affect plant safety, which is consistent with previous staff reviews. The security measures of vital area barriers, vital area access controls, and the compartmented vital area concept together could most affect safe plant operations although the effect is small. If a facility were highly compartmented, operators could be delayed in responding to events, which could affect safety. However, licensees have addressed most access problems in response to the NRC's past concerns and actions. For example, the NRC changed a rule to give licensees the authority to suspend safeguards measures during emergencies. Many licenses with more compartmented vital areas have revised their security programs to decrease the number of separate vital areas.

The staff found several security measures that, for various reasons, are marginally effective in protecting against the insider threat and therefore could be revised or eliminated. By implementing access authorization and FFD programs effectively and with consideration of other measures, licensees can

adequately protect against the insider threat without the need for these marginally effective measures.

The staff recommends making changes to NRC regulations applicable to security requirements in six areas.

1. key controls for access to vital areas
2. maintenance of access lists for each vital area
3. response to vital area doors
4. access controls to containment during periods of increased traffic
5. search requirements for on-duty guards
6. requirements for vehicle escort.

The staff also recommends informing licensees of the NRC's position on (1) the legitimacy of the "vital island concept," and (2) the criteria for designating safeguards information. The staff believes it should closely monitor the effectiveness of the licensee's access authorization programs to verify the continued trustworthiness and reliability of individuals granted unescorted access.

REGULATORY REQUIREMENTS FOR PROTECTION AGAINST THE INSIDER AND IMPACT OF THESE REQUIREMENTS ON OPERATIONAL SAFETY

I. INTRODUCTION AND PURPOSE

By memorandum dated September 3, 1991, the Commission requested the staff to re-examine the NRC's nuclear power plant security requirements imposed by 10 CFR Part 73 to determine if those requirements associated with the internal threat will remain appropriate in light of the recent regulations concerning fitness for duty and access authorization. The Commission directed that consideration be given to whether the security requirements impair the ability of an operator to safely operate the plant. This report presents the results of the staff's re-examination.

II. BACKGROUND

This section discusses the development of safeguards requirements associated with the internal threat, previous studies and regulations regarding the effect of security requirements on safe plant operations (safety/safeguards interface), related practices and experience of other agencies, a review of related security events, and the international perspective associated with internal security requirements.

A. Safeguards Requirements Associated with the Internal Threat

On November 13, 1974, the Commission published for comment an amendment to 10 CFR Part 73, "Physical Protection of Plants and Materials," that would establish in a new Part 73.55 specific requirements for nuclear power reactor licensees for protection against sabotage. 10 CFR Part 73.55, "Requirements for the Physical Protection of Nuclear Power Reactors," was published final on February 24, 1977 (42 FR 10836). The final rule included a general performance objective that the physical security measures provide protection against both an external (several persons, armed with automatic weapons and explosives) and internal (a single insider in any position) sabotage threat. The regulations included specific requirements [73.55(b) - (h)] that, if complied with by licensees, the Commission considered would essentially satisfy the general performance objective.

During the development of the rule, there was extensive deliberation on what requirements should be included to protect against the insider. While the staff considered that the measures included in the rule provided a high level of assurance for protection against an external threat, concerns remained about the need for additional measures to protect against the insider. There was recognition that some options to protect against the insider could be onerous and potentially have an adverse impact on plant operations. For example, one option was use of

a "two-man rule," which would have required the presence of at least two persons at any time when a vital area was occupied. Another option considered was time zoning, which would have limited each employee's access to a vital area to specific times during a shift. Neither of these options was selected as a measure to be required. In the statement of considerations for the final rule, the Commission acknowledged the need for further consideration of measures that would provide additional assurance to protect against the insider. The Commission stated:

> "It also should be noted that to reduce the vulnerability of operating facilities from the threat of an insider, the Commission is considering a program to require personnel security clearances for individuals employed in sensitive work activities who have access to or control over special nuclear material. However, applicants and licensees should continue to use the employee screening guidance from the American National Standard, ANSI N18.17, "Industrial Security for Nuclear Power Plants." Should the continuing review of such internal threat by the Commission show changes that would dictate different levels of protection, future changes to meet these new conditions would be forthcoming."

Since 10 CFR Part 73.55 was first issued in 1977, a number of regulatory activities associated with protection against the insider threat have occurred. Provided as Attachment 1 is a chronology of regulatory activities associated with development of agency policy regarding measures to protect against the insider. The major areas where activities have taken place since 1977 include:

1) Vital Area Access
2) Vital Island/Independent Vital Island Concepts
3) Criminal History Checks
4) Fitness-for-Duty Programs
5) Access Authorization Programs

Each of these areas is discussed below.

Vital Area Access

Specific measures for vital area access controls were not included in the rule published in February 1977. In May 1979 an incident at Surry Power Reactor involving a deliberate attempt to damage new fuel assemblies by persons who had unescorted access to vital areas resulted in heightened attention to licensee controls for access to vital areas. IE Bulletin No. 79-16, "Vital Area Access Controls" (IEB 79-16), which was issued as a result of the Surry event, required licensees to commit to specific vital area access control measures including periodic updating of vital area access authorization lists. Proposed changes to the regulations that would have codified most of the measures specified in IEB 79-16 were published on March 12, 1980. Based on public comments and further experience with vital area access controls (see discussion on safety/safeguards impact that follows), the requirements in the

proposed rule were significantly revised to provide appropriate consideration for access for safety purposes while accomplishing the same safeguards objectives. The final regulatory requirements for vital area access controls were published on August 4, 1986, as part of several miscellaneous amendments concerning physical protection of nuclear power plants. Included in the amendments were provisions to allow the suspension of certain safeguards measures during emergencies.

Vital Island/Independent Vital Island Concepts

In an August 1, 1984 notice of proposed rulemaking for miscellaneous amendments concerning physical protection of nuclear power plants, the concepts of "vital island" and "independent vital islands" were introduced in an effort to provide clarification on vital area designation. The vital island concept generally refers to the assembling of many smaller vital areas (with the exception of the control room, containment, and security alarm stations) into a single vital area or a few large vital areas. The concept of independent vital areas generally refers to smaller and discrete vital areas. Introduction of these concepts caused considerable industry confusion regarding the Commission's policy on vital area designation. Confusion appeared to be directed mostly at NRC policy concerning whether vital areas should be compartmentalized as suggested in IEB 79-16 (primarily as a deterrent to the internal threat), or whether less compartmentalization was acceptable. The notice of final rulemaking for the miscellaneous amendments acknowledged this confusion and deleted those portions of the rule that referred to "vital islands" and "independent vital islands." In the Federal Register notice publishing the final rule, the Commission noted that the regulations did not preclude the consolidation of one or more vital areas into a single vital area if approved by the staff. Currently, there is a wide variation in licensee vital area configurations, including varying degrees of both compartmentalization and vital islands.

Criminal History Checks

Section 606 of Pub. L. 99-399, "The Omnibus Diplomatic Security and Anti-Terrorism Act of 1986," required nuclear power reactor licensees and applicants to conduct criminal history checks for individuals granted unescorted access to nuclear power facilities through the use of FBI criminal history data. On November 7, 1986, the NRC published a proposed rule requiring that these criminal history checks be done. The final rule was published on March 2, 1987. The rule requires licensees to take fingerprints of individuals requiring unescorted access and obtain, via the NRC, criminal history data from the FBI. Access decisions based upon information received from the FBI rests with licensees and is not formally reviewed by the Commission.

Fitness-for-Duty Programs

In recognition of the increasing number of reported drug incidents and the potential impact of drug related problems on power reactor

operations, a broad non-prescriptive proposed rule on fitness for duty was prepared and published on August 5, 1982. Subsequently, in recognition of initiatives and commitments made by the industry to develop and self-manage fitness-for-duty programs, the Commission decided to defer implementation of the rule, to issue a policy statement to further encourage such self-improvement, and to reconsider the need for rulemaking after evaluating the experience gained under the industry program. In December 1987, the staff was directed to prepare a rule requiring power reactor licensees to have a fitness-for-duty program. The final rule was published on June 7, 1989. Although related to the efforts to develop suitable measures for protection against the insider, fitness-for-duty programs, which are primarily a measure of current trustworthiness, were never an integral part of access authorization rulemaking.

Access Authorization Programs

Rulemaking for access authorization programs was first proposed to the Commission in 1977. On August 1, 1984 (49 FR 30726), a proposed rule was published that would require an access authorization program at nuclear power plants. As an alternative to rulemaking, a proposed policy statement was developed and issued for comment on March 9, 1988 (53 FR 7534). However, the Commission decided to proceed with rulemaking. As directed by a Commission memorandum dated April 19, 1989, the staff developed a final rule on access authorization programs for nuclear power plants which was published in the Federal Register on April 25, 1991, with implementation required by April 27, 1992. The rule requires that licensees assure that persons granted unescorted access to nuclear power plants are reliable and trustworthy by conducting a background investigation and a psychological assessment before granting unescorted access. After unescorted access has been granted, the rule requires the licensee to conduct an ongoing behavioral observation program to assure continued reliability and trustworthiness. The staff is developing an inspection plan to assess licensee implementation of their access authorization programs.

B. Safety/Safeguards Impact

Most security measures, consistent with their function, provide controls or restrictions on personnel movement and, therefore, have a potential for adverse impact on safety. The impact of security measures on safe plant operation was one factor considered in the initial development of security regulations for power reactors. Experience with implementation of the security measures has resulted in further considerations of the impact of security on plant safety. Attachment 2 provides a chronology of regulatory activities associated with considerations and review of the potential adverse impact of security measures on safe plant operations.

Soon after 10 CFR 73.55 was initially published in 1977, IE Bulletin 77-08, "Assurance of Safety and Safeguards During an Emergency - Locking Systems" (IEB 77-08), was issued. IEB 77-08, which was issued in

response to several events and inspection findings, required licensees to take actions to assure that security hardware and systems did not impede prompt emergency ingress and egress.

In October 1982, the NRC Executive Director for Operations appointed a five-member committee to review the impact of security requirements on operational safety. The results of the Committee's findings are documented in NUREG-0992, "Report of the Committee to Review Safeguards Requirements at Power Reactors," dated May 1983. Overall, the Committee did not identify any clear operational safety problems associated with implementation of the NRC's security requirements. However, the Committee did find that the potential for safety problems existed, to varying degrees, at licensed facilities. In many cases the Committee found the potential concerns to be caused by licensee-specific decisions and not by security requirements. The Committee's report contained a number of recommendations intended to minimize the potential impact of security on safety. These recommendations included informing licensees of the study's findings, addressing the need for prompt access in ongoing insider safeguards rulemaking (access authorization and miscellaneous amendments, and protected area search requirements), and developing inspection and licensing review initiatives. Most of the Committee's recommendations were implemented.

During two reactor events in 1985, site operations necessary to control the events were hampered or potentially hampered by features designed to control access to areas or equipment. As a result, IE Information Notice No. 86-55, "Delayed Access to Safety-Related Areas and Equipment During Plant Emergencies," was issued to alert recipients of a potentially significant problem concerning the ability to reach and operate essential equipment during an emergency. Although the limited access in the events was not solely due to safeguards measures (some was for administrative or radiological controls), these events represented continuing problems with access to equipment due to locked doors.

Miscellaneous amendments concerning physical protection of nuclear power plants were published on August 4, 1986. These amendments included a number of changes as a result of the special review committee's findings. The changes included specific requirements to accommodate rapid ingress or egress during emergency situations and provided authority [(50.54 (x) and (y)] to suspend safeguards measures during emergencies.

C. Practices and Experiences of Other Agencies

In November 1991, an Interagency Symposium was hosted by DOE entitled "The Insider Threat." A summary of topics discussed can best be portrayed by excerpts from several of the presentations.

Remarks provided by Mr. Glenn S. Podonsky, Director, Office of Security Evaluations, DOE;

...there is a growing realization that greater attention and emphasis must be given to protecting against potential internal acts of espionage, sabotage, and theft of valuable materials or sensitive information by trusted employees. This attention is warranted, not only from concern about hostile acts such as terrorism, but also over concerns about drug and alcohol abuse that are becoming problems in this nation. Personnel who at one time were steadfastly loyal employees may be radically changing both their personal and professional lives through economic difficulties as well as substance abuse. We must consider these vulnerabilities when addressing the insider threat.

Remarks provided by Mr. John Tuck, Under Secretary of Energy, DOE;

...we must anticipate a significant increase in security threats from two areas: 1) more widespread efforts to gain clandestine access to nuclear technologies banned under non-proliferation agreements; and 2) greater attempts at industrial espionage, by governments and private entities, in an effort to gain economic advantage. Such attempts are very likely to target the insider, whether as a willing conspirator or dupe.

While it is extremely difficult for security professionals to identify threats from insiders until <u>after the fact</u>, it is extremely easy for the insider to plan his course of action deliberately and wait patiently for the most opportune time to carry it forward. The insider has the advantage of time and access.

Similarly, it is extremely difficult to prevent insider acts of sabotage against equipment of facilities. We have seen numerous examples in recent years of how vulnerable high-tech facilities are. Employee sabotage was cited as a possible cause of the tragic chemical release at Bhopal, India. A recent event in Chicago involving the disruption and destruction of electronic communications services also demonstrates the vulnerability of a high tech system.

So the insider threat is real: it is likely to grow; and it is extremely difficult to identify before the fact. Moreover, some of the "easier" answers for protecting security may no longer be acceptable because of new sensitivity to employee rights and worker health and safety rules.

First, we must all recognize that there is no single solution -- no silver bullet. Second, we must accept that we will never completely eliminate the insider threat. But through a pooling of resources and a sharing of information and successful experiences, we can reduce the risks of the insider threat to acceptable levels.

> Supervisors are particularly critical; they provide the first line of defense in detecting unstable or aberrant behavior before an employee causes harm to a facility or fellow-employee. Hence, supervisor's training must be expanded and enhanced if we are to minimize the insider threat. We are beginning to work in this area at DOE and would welcome input from others who are also working to develop more effective supervisor training programs.

Mr. Bruce Hoffman, of the Rand Corporation, during the same conference provided the following conclusion regarding the problems related to the insider threat. His findings are based on the review of actual acts committed by insiders in environments similar to nuclear requirements. He characterized the study as a follow up to work done by the NRC in NUREG 0703, "Potential Threat to Licensed Nuclear Activities from Insiders" which is known as the "Insider Study." He stated:

> Insider criminals may be the most difficult and dangerous adversaries to defend against. They may be young or old, long-time or short-time employees. Although financial gain may be the insider's predominant motivation, families, intimate relationships, disillusionment or disgruntlement, misplaced altruism, and ideological allegiances may also play a role in the decision to commit or abet a criminal act against an employer. Insiders can accomplish great damage acting either alone, in cooperation with fellow insiders, or in league with outsiders.

Mr. Hoffman's presentation dealt with several categories of insiders. The following discussions are pertinent to the NRC's design basis insider threat.

> The greatest number of crimes committed for other than financial gain were committed by lone insiders. These individuals, on the whole, appear to be less stable than the others. One-third of them were motivated by emotional disturbance, frustration with their employment, or idiosyncratic factors. Perhaps the most important finding of this study relates to planning and security. Success in most of the incidents examined seemed to depend less on detailed planning or expert execution than on the exploitation of existing security flaws. Indeed, most of these crimes did not require sophisticated planning; they were carried out against targets of opportunity.
>
> Many security directors claim that thorough background checks are more useful than internal procedural controls in preventing insider crimes. (Similarly, periodic background checks of employees might also prove helpful in deterring insider crime by identifying employees with potential financial or psychological problems.) Eleven companies that

were robbed or burgled by insiders working with outsiders had a policy of screening applicants before hiring them, but in six cases this screening involved only a check of the applicant's former employers, and in one case, the screening policy was not carried out.

Continuing supervision, along with periodic screening, including credit checks, might have alerted security personnel to two airline employees, one of whom needed money to cover massive gambling debts; the other used some of his smuggling profits to throw elaborate parties at which cocaine and other drugs were regularly used.

Even if the background check could predict an applicant's tendency to be chronically dishonest, late for work, addicted to drugs or alcohol, or subject to blackmail or financial problems, it could not identify those who will succumb to temptation rather than be honest when the chance arises.

Background checks are also unlikely to uncover characteristics that might lead an employee to join a hostile ideological group or to commit a crime for reasons of principle or personal relationships.

On February 13, 1992, the Federal Aviation Administration published for proposed rulemaking regulations for employment investigations and criminal history records checks for all individuals given access to security areas (areas requiring badging). The U.S. Postal Service is also currently attempting to design a screening program in light of several recent violent incidents involving disgruntled employees. Both of these programs are aimed at "insider" concerns as opposed to the dual nature of the NRC defined threat.

D. Recent Events and Experience

Events Related to Insider Concerns

Revision 17 of NUREG-0525, Safeguard Summary Event List, summarizes events through December 31, 1991. NUREG-0525 breaks the safeguards events into ten categories. Our review for this report focused on five categories which are more directly associated with insider actions. These categories are: (1) Radiological Sabotage, (2) Tampering/Vandalism, (3) Firearms, (4) Arson, and (5) Miscellaneous (any item that does not fit prescribed categories). In these five categories, from 1987 through 1991, there were 106 reactor safeguards events assessed as being potentially associated with utility or contractor employees. There were no Radiological Sabotage events. It should be noted the category of Radiological Sabotage includes only events where a deliberate malevolent act actually endangered the public by exposure to radiation. In the Tampering/Vandalism category, which includes destruction or attempted destruction of property, parts and

equipment which does not directly cause a radiological release, there were 30 events. Of these, the person committing the tampering/vandalism was identified in 4 cases. With respect to the remaining event categories, there was 1 arson event, 106 firearm events (counted if the incident could have provided the insider a weapon), and 29 miscellaneous events (general issues that could aid an insider).

Attachment 3 presents the yearly number of events from 1987 through 1991 reported for each of the five event categories of interest. The total number of events each year as well as the number for each of the five categories shows no distinct trend, with the possible exception of an increase in the number of firearm events. The increase in firearm events may be attributed to more sophisticated detection equipment and diligence on the part of the licensees to successfully detect the introduction of firearms and ammunition. It should be noted that these firearms events did not involve any malevolent intent but could have provided the potential for such acts. Many firearms incidents are the result of searches conducted of commercial trucks making deliveries to nuclear sites. Typically, the driver had obtained a firearm for protection from highjacking and other assaults common to the trucking profession. Other typical incidents involved the discovery, during access searches, of weapons placed in a purse for offsite protection and then forgotten. Both of the above examples reflect today's social conditions and do not reflect a threat against the nuclear plant. Furthermore, the discovery of these firearms indicates that access control measures by licensees are effective.

Insider acts of tampering/vandalism continue to occur at reactor facilities that could potentially impact the margin of public health and safety, even if the intent was not malicious. Of those events where the individual was identified, the causes are primarily related to disgruntled employees who were already authorized access and not someone who was bent on gaining access for the purpose of damaging a nuclear facility. This points to the importance of behavioral observation programs in identifying and dealing with personnel problems that develop after a person has been granted unescorted access.

Events Related to Safety/Safeguards Interface Problems

A loss of feedwater event at Davis-Besse on June 9, 1985 resulted in an inspection by an investigative team which in its published report (NUREG 1154) noted that security system constraints could (in the Davis Besse event they did not) deny timely access for performing emergency duties. Since the Davis Besse event there has been only one event of note that had safety/safeguards implications. That event occurred at Surry on December 9, 1986, and involved access equipment being disabled by steam released from a ruptured pipe. The concerns were over the safe evacuation of an area by an equipment operator.

Experience With Safety/Safeguards Interface

As part of Regulatory Effectiveness Reviews (RER), Operational Safeguards Response Evaluations (OSRE), and inspections by regions, the staff reviewed the safety/safeguards interface at least once at each power reactor to assure that safeguards measures do not adversely affect the safe operations of the plant. During the RER and OSREs, NRC team members interviewed the security manager, at least one operations shift manager, and at least one auxiliary equipment operator. During these reviews team members made a walking tour of the safety equipment throughout the plant. The objective of the walking tour and discussions are to assure (1) prompt access to and egress from the protected area and vital areas in an emergency situation, and (2) that security radio transmissions would not interfere with plant operations. Since the Miscellaneous Amendments requiring rapid ingress and egress became effective in 1986, RER and OSRE reviews have been completed at 50 sites. Potential safety impacts that warranted licensee attention were identified at only two sites and have been corrected by the licensees.

E. International Perspective

The International Safeguards Branch of the Division of Safeguards and Transportation, Office of Nuclear Material Safety and Safeguards, has participated with the Department of Energy and the Department of Defense on interagency technical exchanges with representatives of foreign governments and power reactors in 13 different countries. While the country-specific information is classified, data about 15 physical protection program elements were extracted from reports from site visits in each country. These security program elements were compared but are not identified as to country of origin. Elements were evaluated and given a subjective, non-specific rating of either "equal to," "less than," or "greater than" requirements implemented in the United States.

The categorization process does not account for social/political influences, the relative significance, or the frequency of occurrence of one element versus another element. Attachment 4 is a bar chart which identifies the specific numbers for each of the 15 elements reviewed. Ten elements relate to the external threat, while five apply to the insider threat.

The general findings are that approximately 65% of the individual elements meet or exceed NRC requirements in a comparison of all elements. Comparing the five insider elements, it appears that 60% of the countries have protective measures against the insider that meet or exceed NRC requirements. The guard force size was assessed as smaller than US guard forces in 60% of the foreign country sites.

Extreme care should be used regarding this data considering the great disparity in social and political environments between countries, making the comparison difficult. It should be noted that the NRC physical protection program, or at least specific elements, has been the model from which many foreign countries have designed their programs.

F. Diversity of Insider Security Measures

The performance effectiveness of security measures employed against an external adversary can be evaluated with reasonable confidence. These measures are heavily interdependent for their overall effectiveness. The effectiveness of the total measures used to protect against the insider are difficult to evaluate, but conversely to the external threat, individual measures are largely independent of the effectiveness of the other measures. To a large extent, staff confidence in the overall effectiveness of programs designed to protect against an insider relies on the diversity and independence of these measures.

Some measures, such as criminal history checks, other background investigations, psychological testing, and pre-employment drug tests protect by excluding individuals with undesirable backgrounds or behavior patterns. This type of information provides a reasonable "picture" of an individual at the time the investigation is completed, with limited value for predicting future behavior. Although such measures are important and effective in their intermediate goal of determing initial access, their contribution to the ultimate goal of protecting against radiological sabotage is also difficult to evaluate. Persons with acceptable characteristics prior to access can develop undesirable characteristics after access is granted. This aberrant behavior may have nothing to do with the work environment. In addition, per with malevolent intent prior to seeking access could potentially circumvent these measures.

Other measures, such as behavioral observation and post-employment drug tests continue where the initial screening process stops and can protect by identifying persons who develop undesirable characteristics subsequent to initial screening. However, their effectiveness is also difficult to evaluate.

Measures such as the use of metal and explosives portal detectors and x-ray machines can make an important contribution by making it difficult for an insider to bring weapons, explosives, or incendiary devices into the protected area to make radiological sabotage easier. However, their contribution to the overall goal of protecting against radiological sabotage is difficult to evaluate because of technological limitations on their effectiveness and because an insider could potentially commit radiological sabotage without the use of such contraband materials.

Other measures such as vital area access controls can contribute to deterring radiological sabotage attempts by providing a record of individual access. Vital area security patrols can contribute by either deterring or detecting a malevolent act. The contributions of these measures to the overall goal are also difficult to evaluate.

It is unlikely that any single type of protective measure against an insider could provide a high degree of assurance by itself. The effectiveness of measures such as background investigations decreases with time. Since confidence in the overall effectiveness of protection

against an insider depends on the diversity of these protective measures, it is unlikely that any individual measure could be totally eliminated without some loss of confidence in our ability to meet our goal of high assurance. However, since no individual type of measure is relied on independent of the others, latitude exists for potentially changing detailed requirements which may contribute marginally to overall effectiveness.

III. ANALYSIS OF INSIDER MEASURES, THEIR EFFECTIVENESS, AND THEIR IMPACT ON SAFE PLANT OPERATION

This section presents an analysis of the effectiveness of safeguards measures to protect against the insider threat and the impact of these measures on safe plant operations.

All safeguards measures required by regulation were reviewed and those requirements that provide physical protection against the insider were specifically identified. Further, safeguards requirements that have a potential impact on safe plant operations, whether or not associated with the insider threat, were also identified. This process eliminated from the analysis a number of safeguards requirements.

The screening of safeguards requirements resulted in the identification of the requirements of interest for this analysis that fall into the following nine areas:

A. Protected Area Perimeter Systems
B. Search Equipment and Protected Area Access Controls
C. Access Authorization Programs
D. Fitness-for-Duty Programs
E. Vital Area Barriers
F. Vital Area Access Controls
G. Vital Island/Compartmentalization
H. Security Patrols and Response to Alarms
I. Safeguards Information

Each of these nine areas is discussed below. Included in the discussion are: (1) a description of the requirements, (2) an evaluation of the effectiveness of the requirements in protecting against the insider, and (3) an evaluation of the impact of the requirements on safe plant operation.

A. Protected Area Perimeter Systems

Description

Power reactor facilities are required to establish certain physical barriers around their sites to protect vital equipment. While utilities usually own large tracts of land (owner controlled areas) where power reactors are located, the first required physical barrier is the "protected area" (PA) barrier. The perimeter of the facility is bounded

by the PA barrier which is required to be a physical barrier such as a chain link fence with clear areas (isolation zones) on either side. At the PA boundary, licensees are required to have a system that provides "detection of penetration (alarm system) to assure adequate response by the security organization." The isolation zones facilitate assessment of PA alarms. To aid in assessment of alarms, the regulations require "illumination sufficient ... to monitor and observe ... the isolation zones and all exterior areas within the PA." Security patrols are required to conduct routine patrols of the PA.

Effectiveness of Measures to Protect Against the Insider

Most of the above mentioned security features were included in the regulations to protect against the external threat. However, the PA barrier provides some measure of protection against the insider because it confines individuals who have been granted unescorted access to the PA and channels personnel though specific PA entrance and exit portals which facilitates identification and control procedures and economizes guard force resources required to control the PA.

Safety/Safeguards Impact of Measures

PA perimeter systems have little or no impact on safe plant operations since these systems do not limit internal facility access or movement.

B. Search Equipment and Protected Area Access Controls

Description

The regulations require that licensees control all points of personnel and vehicle access into a PA. Required personnel controls include identification of the person, verifying that access is authorized, and search for detection of firearms, explosives, and incendiary devices. Individuals authorized unescorted access are required to be issued and display a numbered, picture identification badge. Vehicles and their cargos are required to be searched prior to their being granted access to the PA and the drivers are required to be processed (searched, badged, and escorted) through the entrance facility. Vehicles are usually processed through a vehicle "trap" or "sallyport" immediately adjacent to the personnel entrance facility. Vehicles, except certain designated vehicles which remain in the PA, are required to be escorted by a member of the security organization while in the PA. The regulations exempt vehicles from search while under emergency conditions; however, they must be escorted by a member of the security force.

The regulations require that security officers be processed through electronic search equipment each time they enter the PA. If they leave the PA, even for a short period to conduct official business, they are required to be searched upon re-entering the PA. If carrying a handgun, the officer would be required to remove the weapon while passing through

the metal detector or carry the weapon and, after setting off the metal detector alarm, be subject to a hands-on search.

Effectiveness of Measures to Protect Against the Insider

A primary purpose of PA access search equipment (i.e. metal detectors, explosive detectors, and x-ray machines) is to protect against an insider introducing firearms, explosives, and incendiary devices into the PA. Metal detection equipment has a good performance capability to detect the introduction of weapons. The capability of x-ray machines to detect firearms and explosives is particularly dependent on the quality and maintenance performance capability and calibration of the equipment and the training, experience, and attentiveness of the equipment operators. Explosives detection equipment has technical limitations related to types of explosives capable of being detected. Physical searches are done only for cause, or if electronic search equipment is inoperable. The mere presence of the search equipment provides a deterrent to someone who may be considering introducing contraband into the PA.

Searching of vehicles is very difficult, due to the limitations of portable electronic search equipment and the number of potential areas on a vehicle where contraband can be concealed. Difficulties in vehicle searches are one reason why vehicles are escorted by a security officer, which, in concept, provides additional protection.

Badging individuals who have access to the PA is effective in controlling and limiting access to the protected area to authorized individuals. Badges issued for unescorted access are required to have a photograph of the bearer and usually contain some visual coding indicating PA versus vital area (VA) access levels. Personnel are required to display these badges so that they are readily visible on their upper torso, except when personnel are wearing radiation protection clothing. In addition to the badges' visibility to patrolling guards, any employee can easily observe these badges and challenge anyone whose badge does not authorize access to the area in which observed. Visitors wear distinctive, non-picture badges.

The usefulness of the requirement to search guards, particularly using metal detection, upon their re-entry into the PA after exiting on official business is marginal. This requirement was predicated on the concern that the security officer could be the insider and that no one entering the PA should be given special treatment. However, if the security officer is issued a weapon, the usefulness of checking to assure the officer is not bringing another weapon into the site as an insider would appear to provide little marginal protection.
NOTE: The design basis threat does <u>not</u> include collusion by 2 or more insiders.

Safety/Safeguards Impact of Measures

PA access controls and search equipment have very little impact on safe plant operations since safety and vital equipment are located inside the PA. Also, search equipment and badging should not provide an obstacle for people outside the PA who need access to the site in responding to operational events. 10 CFR Part 50.54 (x) and (y) permit expedited access for personnel and vehicles into the protected area in emergencies. With the authorization of a senior licensed operator or above, the licensee may exercise these provisions and take reasonable action during an emergency to expedite PA access.

C. Access Authorization Programs

Description of Requirements

Power reactor licensees are required by 10 CFR Part 73.56, "Access Authorization Program for Nuclear Power Plants," to have an access authorization program applicable to individuals granted unescorted access to protected and vital areas of licensed facilities. Regulatory Guide 5.66, "Access Authorization Program for Nuclear Power Plants," endorses, with a few exceptions, NUMARC 89-01, "Industry Guidelines For Nuclear Power Plant Access Authorization Programs," as an acceptable method of meeting the requirements of 10 CFR 73.56. The intent of the access authorization program is to verify the trustworthiness and reliability of an individual. The behavioral observation aspect of the program is intended to provide continuing assurance of the individual's trustworthiness and reliability.

10 CFR 73.56, which was published on April 25, 1991, requires licensees to implement by April 27, 1992, an access authorization program that meets the regulation. In general, the rule requires that licensee programs contain the three major program elements of background investigation, psychological evaluation, and behavioral observation. The background investigation element includes checks of an individual's criminal history, including fingerprint checks with FBI records (10 CFR 73.57).

Although power reactor licensees had access authorization programs prior to the issuance of the access authorization rule, the programs varied significantly in their scope, detail, and quality. The rule should provide for more consistent access authorization programs and also facilitate exchange of access status among licensees. The staff intends to assess licensee implementation of these programs through inspections.

Effectiveness of Measures to Protect Against the Insider

If implemented adequately, access authorization programs provide an increased capability to protect against the insider. The program provides for a check of the individual's background, which provides an effective means for detecting past actions that may be indicative of

future reliability. The psychological assessment element of the program provides an additional tool that assesses an individual's present stability and mental health and evaluates any noted psychological characteristics that may have a bearing on trustworthiness and reliability. Both the background check and psychological assessment are accomplished immediately prior to the individual's being granted unescorted access. This information provides a means to evaluate a person's past and present trustworthiness and reliability which is assumed to be a good predictor of demeanor in the near term.

The major purpose of the behavioral observation element of the access authorization program is to detect negative behavioral changes over time (after the initial granting of access) that might lead to acts detrimental to public health and safety. The regulations and guidance for this aspect of access authorization programs are very general, which could lead to a wide variation in their effectiveness in detecting detrimental behavioral changes. If designed and implemented properly, behavioral observation programs can serve to detect and correct problems early on and serve to promote a better working environment for both the employee and employer. Behavioral observation is the responsibility of an individual's supervisor and management.

Safety/Safeguards Impact of Measures

Access authorization program requirements are primarily measures that are required to be completed prior to an individual being granted unescorted access. Therefore, the program contributes to safety and has no negative impact on safe plant operations.

D. Fitness-for-Duty Programs

Description of Requirements

Operating power reactors are required by 10 CFR Part 26, "Fitness for Duty Programs," to implement fitness-for-duty (FFD) programs for persons granted unescorted access to protected areas and persons required to report to the Technical Support Center or Emergency Operations Facility in accordance with the licensee's emergency plans and procedures. These programs are required to include suitable inquiries as to any past evidence of substance abuse by the individual involving illegal drugs or alcohol. The program also includes employee awareness training, supervisory training and drug testing.

Effectiveness of Measures to Protect Against the Insider

Similar to the access authorization program, FFD programs check an important aspect of an individual's personal history that could have a direct bearing on that individual's trustworthiness and reliability. The testing aspects of the FFD program provide measures to identify and screen out individuals who have drug or alcohol problems. Random testing is primarily a deterrent to substance abuse and provides an ongoing measure to detect persons who may have gone undetected during

the pre-access screening test or persons who may have later acquired a drug or alcohol problem.

Safety/Safeguards Impact of Measures

Many of the FFD program requirements, such as a suitable inquiry into any history of substance abuse, pre-access drug testing, and awareness training, are required to be completed prior to an individual's being granted unescorted access and therefore have no negative impact on safety. The program also includes a requirement for random testing of individuals. Individuals selected for testing who are on duty would need to be absent from work, nominally for about 1/2 hour. This process might cause a temporary reduction in staff physically on duty but should have little impact on the licensee's normal operational or emergency response capability, especially since testing would be immediately terminated during an emergency.

Overall, FFD program measures have a very low potential impact on safe plant operations from a safety/safeguards standpoint.

E. Vital Area Barriers

Description

Licensees are required to locate vital equipment within a vital area, which in turn, is located within a PA. The vital area barrier is required to be separate from the protected area barrier, with access of both personnel and vehicles controlled through secured doors. Vital area barriers are required to be of substantial construction, including preclusion of openings where surreptitious entry may occur. Accepted criteria for the penetration resistance (hardness) of barriers generally includes barriers that are difficult to penetrate with common hand tools. For VA barrier penetrations (e.g., pipes, ventilation, etc.), most sites have established a criterion of not allowing a barrier opening of greater than 96 square inches (definition of "man sized" openings). To meet this criterion sites have taken such actions as placing grating at ventilation penetrations and tack-welding manhole covers.

All vital area doors are required (if the space is unoccupied) to be locked, alarmed and have access controlled. Licensees typically meet this requirement using an electronic card reader, or, in special situations, a guard.

Effectiveness of Measures to Protect Against the Insider

Vital area barriers provide a dual role of protecting equipment against both the external and insider threats. Against the external threat, the vital and protected area barriers, in conjunction with PA detection and assessment, delay and as well as detect an adversary and thereby provide sufficient time for interdiction by the licensee's response force. Vital area doors, which generally provide a less substantial barrier to

an external assault than most other types of vital area barriers, are alarmed which would help direct security response to a specific location if the door was subject to forced entry.

Against the insider threat, vital area barriers restrict individuals from gaining access to areas where they are not authorized access. This, in conjunction with control of access to vital areas (see Item F), provides for control and monitoring of individual access. If there are few vital areas (vital island concept) or most persons granted access to the PA are also granted access to all or most vital areas, these barriers are rendered mostly ineffective as a protection against the insider.

Safety/Safeguards Impact Measures

Vital area boundaries principally include walls and structures in place for reasons other than security. Vital area barriers established solely for security reasons include those around vital equipment not located in a building (e.g. tanks, and piping runs) or barriers around equipment (ducting, cable trays, ventilation) in a PA which penetrate a vital area wall. The primary safety/safeguards impact of vital area barriers would be delays caused by gaining access through the controlled access doors, not the barriers themselves (see Item F for discussion on vital area access).

F. Vital Area Access Controls

Description

Licensees are required to limit non-emergency vital area access to individuals who require access in order to perform their duties. Specifically, the regulations require licensees to maintain updated lists (updated and approved by a cognizant manager every 31 days for each vital area) of individuals whose specific duties require their access to a specific vital area. All points of personnel and vehicle access to vital areas are required to be positively controlled, in accordance with the access lists. "Positive control" means an access control system using a card key or other device or measure unique to a specific person. Unoccupied vital areas are to be locked and alarmed. Access control procedures and equipment are designed to accommodate rapid ingress and egress during emergency conditions or situations that could lead to emergency conditions.

Procedures are required for "for cause," involuntary termination of an individual's unescorted access to assure that access is not continued. Prior to or simultaneously upon notification of the individual of his or her access termination, electronic control of access should be revoked and identification badges and entry control devices retrieved.

One unique access control measure applies specifically to access to reactor containment. The regulations require that any time "frequent access is permitted to containment such as during refueling or major

maintenance, positive access control to assure that only authorized personnel and materials are permitted into the containment shall be exercised by the licensee, with a guard or watchman."

Effectiveness of Measures to Protect Against the Insider

Control of access to a facility's vital areas is an attempt to minimize the number of persons with an opportunity to commit sabotage. Also, controlling access may provide accountability of an individual's access which is expected to provide some deterrence from malevolent acts due to the possibility of later detection. Vital area access records allow for the reconstruction of who accessed certain vital areas, which can be beneficial both for facility evacuation for safety reasons and from an investigation perspective.

The effectiveness of vital area access control measures is dependent on many factors such as plant specific facility design and arrangement. For example, the benefit of vital area access accountability would be minimal for facilities having few separate vital areas (vital islands) or authorized access to most persons on site. An important factor is how licensees designate who needs access to vital areas. The NRC has given licensees considerable latitude in their determination of who has a need for access to vital areas. At many sites, most persons granted unescorted access to the site are designated as needing access to all vital areas. Generally, administrative people who work inside the protected area and do not work in the plant are the only individuals who are not granted access to vital areas.

The effectiveness of special access controls required during periods of frequent access to containment are limited. While a watchperson monitoring personnel access may provide some measure of personnel accountability, effective monitoring of materials brought into containment during high traffic periods is difficult because of the quantities and variety of materials that may be introduced. Thorough checking of personnel and materials entering containment could cause significant delays in access.

Safety/Safeguards Impact of Measures

Controlled access to vital areas during plant operations provides limitations on personnel access and potentially could delay movement of personnel. Further, malfunction of access equipment could cause delays in access into a vital area. As discussed in the background section above, concerns about rapid ingress to or egress from vital areas during emergencies have been raised in the past and, as a result, a number of regulatory actions were implemented. Regulatory changes made in 1986 specifically required licensees to ensure prompt ingress and egress during emergencies. A review of the likelihood of an electronic or mechanical failure has been conducted and the probability of such an event was determined to be small, and a failure occurring simultaneously with a safety emergency was considered even less likely. However, there

is a possibility that an accident involving a steam release outside the containment could cause electronic failures.

Actions taken by licensees to assure prompt access include such measures as availability of emergency keys in control rooms and card reader systems that allow vital doors to be unlocked from either of the security alarm stations. As a result, and based on recent observations at licensee facilities during RER's and OSRE's, vital area access controls for personnel responding to operational events and emergencies do not appear to cause a significant impact.

For non-emergency maintenance work, outage work, or other routine activities, vital area access controls could cause personnel access delays. These delays would be caused by the time necessary to process personnel access authorization for individuals to specific vital areas and providing those individuals with properly coded card keys. These delays could be greater for access to containment because of the additional access controls imposed for entry during periods of frequent access.

G. Vital Island/Compartmentalization

Description

Vital Island/Compartmentalization concepts are discussed in the background section above. In theory, compartmentalization (or division of vital equipment into numerous and separate vital areas) could provide greater security from the perspective of both the internal and external threat. With compartmentalized vital areas, an external adversary might have to penetrate several vital area barriers to damage sufficient equipment to cause radiological sabotage. The increased number of barriers required to be penetrated could serve to delay an external adversary and allow more time for response and interdiction. For the insider, numerous compartments for vital equipment could provide for greater control and accountability of personnel access. Numerous vital areas, in conjunction with controls on personnel access to those areas (see above Item F), could serve to restrict individual access and provide a means to monitor an individual's movements in the plant. (For example, in theory, any access by one individual could be limited to a single train of safety equipment.) However, this has not been done in practice because most plants were not built in a manner that would facilitate such a degree of compartmentalization and the negative impact on operational and safety flexibility would outweigh the potential safeguards benefits. Access records have been used by licensees in the past to investigate individual worker access to equipment that has been subject to tampering.

Although the regulations do not specifically address either the vital island or compartmentalization concept, they infer a certain amount of separation with specifications that the control room, central alarm station, and containment be independently controlled vital areas. Further, plant and equipment arrangement dictate the creation of some separate vital areas. For example, at most facilities the service water

system is designed as vital and the intake structure is located in a building separate from the main plant. The greater the number of vital compartments at a facility, the greater the investment in hardware (card readers) and installation costs. The vital island concept requires less hardware and is more forgiving in vital equipment identification since there is no limitation on non-vital equipment being included in vital areas.

Effectiveness of Measures to Protect Against the Insider

The discussion in Section III.F above regarding vital area access controls is closely tied to the concept of compartmentalization in that the degree of selectivity of granting access based on "need" is linked to access to distinct and physically separate areas of the facility. If there are few vital areas and/or most personnel are granted access to all or most areas, the issue of distinct and separate vital areas (with respect to protection against the insider) becomes relatively moot. If a compartmented vital area configuration was used in conjunction with access authorization based upon "need," such a system could potentially provide a measure of protection against individuals granted access to the protected area but not to all vital areas. In practice, that has not occurred and the effectiveness of compartmentalization is limited to potential increase in the deterrent value of access records.
The deterrence value of access records is derived from the ability to reconstruct an individual's location within the plant at any particular time.

Compartmentalization also aids in guard response to alarms and searches associated with those alarms. Accountability, whether it is for incident investigation or safety/emergency evacuation, is also enhanced. With respect to the vital island concept, searching of a large area in response to an alarm is a very difficult task.

Safety/Safeguards Impact of Measures

A greater number of separate vital area compartments results in more controlled access doors a plant operator would have to traverse to accomplish his/her tasks. In theory, the vital island concept has safety advantages over the compartmentalized vital area concept because there could be fewer controlled access doors to negotiate by plant operators. Features discussed in the background section (safety/safeguards interfaces) such as emergency keys and system override commands to open doors have been adopted by licensees to lessen the potential for delays through controlled access doors.

Compartmentalized vital areas provide some safety benefits from an operational perspective. Controlled access to areas of the facility can reduce unnecessary traffic, particularly during maintenance and outages. Reduced traffic lessens the potential for inadvertent equipment operation or damage. Also, use of computer access logs based upon compartmentalized vital areas could aid in locating and evacuating individuals during safety/emergency conditions.

H. Security Patrols and Response to Alarms

Description

Typically, security patrols are conducted at random times using different routes. Patrols not only observe areas for unauthorized personnel and activities, but also look for unauthorized materials and contraband. Patrols carry portable communications to maintain contact with the alarm stations.

Patrols can be used to respond to vital area door alarms. These alarms could be the result of a number of causes, many of which are administrative problems. For example, doors that are held open too long or persons mistakenly attempting to access a door where they have not been granted access may, depending on the access system, cause an alarm. If the specific cause of an alarm cannot be determined, a search of the vital area is required. Also, failure of either the locking or alarm function of a door requires compensatory measures to provide "positive access control." These compensatory measures usually involve the posting of a security officer, with access lists, until the necessary equipment can be returned to service.

Effectiveness of Measures to Protect Against the Insider

Due to their unpredictable nature, random patrols provide some deterrence to anyone considering malevolent acts. Patrols also could detect actions taken by a insider to sabotage a facility. Additionally, operational staff contribute to some extent to the patrol functions by noticing unusual persons and activities. At most facilities, operations staff are trained to identify unfamiliar items and to advise security.

Security officer response to door alarms is effective in assuring proper use of access control systems and providing some deterrent for improper use. However, response is of minimal effectiveness in preventing insider sabotage. The effectiveness of guard response to alarms in protecting against the insider is dependent, to a large extent, on how the vital areas are compartmented and how restrictive the licensee's policy is for granting access to specific vital areas. If a site grants many individuals access to all vital areas and/or there are few compartmented areas, that individual (the insider) would not need to attempt to defeat access control hardware to gain broad access to vital equipment.

Safety/Safeguards Impact of Measures

The presence of security patrols throughout the facility has a positive impact on safety due to the availability of guards to respond to requests for assistance and access. At many sites, guards routinely carry emergency keys to override card reader controlled doors. Patrols also note and report on malfunctioning access control hardware and other security and non-security related equipment failures.

I. Safeguards Information

Description

10 CFR 73.21, "Requirements for the Protection of Safeguards Information," specifies a type of information not otherwise classified as Restricted Data or National Security Information that must be protected against unauthorized disclosure. This requirement lists approximately 13 types of information specifically related to the security programs at power reactor facilities that are not releasable without an established "need to know." Access to this information at reactor sites can only be given to individuals who have had a criminal history check to the extent required by 10 CFR 73.57 and have a "need to know." When not in use, safeguards information must be stored in a locked security container. When in use, safeguards information is required to be under the control of an authorized individual.

Effectiveness of Measures to Protect Against the Insider

Designation and control of certain licensee documents as safeguards information is intended to prevent access to security related information by both the general public and onsite personnel who do not need such information to conduct their business. Controlling access to this information theoretically limits the availability of information that could be of use in sabotaging a facility. However, there is generic information contained in SERs and other documents [e.g., safety (vital) equipment descriptions and locations, and site features] that provides much of the same type of information as that protected as safeguards information. This has the effect of lessening the value of protecting such information as safeguards information.

Safety/Safeguards Impact of Measures

The control of safeguards information has very little direct impact on safety/safeguards issues.

IV. ANALYSIS OF INSIDER REQUIREMENTS IN CONSIDERATION OF FFD AND ACCESS AUTHORIZATION REGULATIONS

Both the recently implemented access authorization and FFD rules apply to persons requiring unescorted access to the protected area of a nuclear power plant. Major purposes of these rules are to assure that individuals granted unescorted access at power reactors are trustworthy and fit to perform required duties. Since 10 CFR 73.55 was put in place in 1977, all sites have had some type of access authorization program of varying quality. Access authorization and FFD programs, if properly implemented, should provide an important element in protection against the insider threat. The following discusses the extent to which the access authorization and FFD programs can supplant the need for other insider protection measures.

Although not specifically addressed in 10 CFR 73.55 in 1977, access authorization was considered an important element of all measures needed to protect against the insider (see discussion in Background section of this paper). Access authorization programs, including FFD aspects, were never intended to be a stand-alone element to protect against the insider. Further, the access authorization programs required by 10 CFR Part 73.56 have not been in place for a sufficient time to fully assess their effectiveness. In the following, the assumption is made that access authorization and FFD programs are effectively implemented.

Implementation of the initial screening aspects of the access authorization and FFD rules can be viewed primarily as a prevention strategy when employed as part of the process for granting unescorted site access. The value of the screening aspect of access authorization and FFD programs as a preventive mechanism diminishes over time unless augmented with some form of investigative update. Screening is a "snapshot" of an individual at the time it is completed, and is immediately thereafter subject to changes over time as related to one's mental, physical and financial health, among other things. Behavioral observation aspects of the access authorization program, if properly implemented, could be a positive, continuing preventive measure and also have a benefit of promoting strong, healthy employee/management relations. Random FFD testing serves as a continuing deterrence and prevention strategy.

Many of the insider protection measures covered in security regulations (as discussed in Section III, above) are both prevention and deterrence strategies. The concept of compartmentalization of vital equipment into vital areas, combined with access controls for those areas, serves as a preventive measure by minimizing the number of employees and contractors with access to specific systems and the opportunity to commit sabotage; the vital area barriers provide resistance to insiders not authorized access to an area. The relative ease with which a response can be made to a specific alarm location and the easier identification of the individual make compartmentalization a good deterrence strategy. Access alarms for doors into vital areas facilitate detection of unauthorized access. Systems that record personnel access provide accountability of individual access, which is expected to deter malevolent acts and aid in the investigation of apparent vandalism or sabotage. Security patrols serve to deter and prevent potential insider acts.

Although each of the methods discussed above provides varying measures of prevention and deterrence, they do so based on different approaches. Assuming that no one method is completely effective, prudence would favor maintaining diversity in deterrence and preventive strategies as long as there are no overriding considerations for not having the measure. As discussed in the above analysis of each of the security measures, none appears to have a significant negative safety/safeguards impact. The measures with the most potential for safety/safeguards impact are vital area access controls and the compartmentalization concept. However, past NRC actions addressing vital area ingress and egress have mitigated the safety/safeguards concerns of these measures. Also, the general movement by licensees away from compartmented vital areas to vital islands has further lessened the safety/safeguards impact for this security measure.

In summary, there does not appear to be a significant safety/safeguards impact from measures in place to protect against the insider threat. Also, while there is a diversity of measures that provide some protection against the insider, none appears to duplicate the goals/objectives of access authorization and FFD programs. From a security perspective, inclusion of multiple measures to protect against the insider provides diversity as well as a balanced security program. However, as discussed above and in the following Findings and Recommendations section, there are several security measures that are marginally effective and therefore may be appropriate for revision or elimination. Properly implemented access authorization and FFD programs will contribute protection against the insider threat and will, with consideration of other measures, help support the elimination of these marginally effective measures.

V. FINDINGS AND RECOMMENDATIONS

A. FINDINGS

The analysis finds that the security measures in place to protect against the insider do not have a significant impact on plant safety. Although not significant, the security measures of vital area barriers (Section III.E), vital area access controls (Section III.F), and compartmented vital area concept (Section III.G) together have the greatest potential for impacting safe plant operations. If a facility were highly compartmentalized, there could be more of a potential for safety impacts due to delays in operator response. However, potential access problems have for the most part been addressed by licensees in response to past NRC concerns and actions. As discussed in the Background Section (safety/safeguards impact), these actions included several alternatives as well as the authority to suspend safeguards measures during emergencies. Additionally, there has been a tendency for those licensees who initially had more compartmentalized vital areas to revise their security programs to decrease the number of separate vital areas. Staff has been receptive to and approved these requests.

Considering the movement by licensees to reduce the number of separate vital compartments and in recognition that at most sites persons granted access to one vital area generally are granted access to all vital areas, the effectiveness of certain vital area access controls has been lessened. For example, the requirement to keep and periodically update lists of personnel requiring access for each vital area, under the above described circumstances, provides little marginal effectiveness in protecting against the insider.

The trade-off between the low potential safety impact and the potentially marginal safeguards benefit of measures designed to control the movement of authorized personnel into vital areas cannot be quantified. Qualitatively, the security access control measures do not have a significant safety impact. The only significant impact is

administrative. However, there are equipment failures of a known frequency that challenge plant safety systems and require prompt access to that equipment. The recommendations in Part V.B. of this paper should reduce, even more, the existing low safety impact of these security measures.

Although there have been no known attempts to cause radiological sabotage at a licensed nuclear power plant, current safeguards measures may have deterred potential insider threats and a real threat could develop without warning. However, the need to provide prompt access to safety equipment has limited the potential benefit of safeguards measures designed to limit access. Accordingly, for those safeguards measures not important for protection against an external adversary, it appears to be prudent to consider flexibility in vital area safeguards measures if some degree of deterrent value, such as computer records of entires to vital areas, could be maintained.

The analysis also identified a number of other specific security measures that had marginal effectiveness on security against the insider. Many of these measures, while having little if any impact on safety, do cause administrative inconveniences. These measures include the following:

1. Requirement for searching for weapons of security guards (while on duty) each time they re-enter the PA.

2. Requirement for guard to monitor access of personnel and materials entering containment during periods of high traffic.

3. Requirement that all non-designated vehicles (after searching) be escorted by a security guard, even when the driver is authorized unescorted access.

B. RECOMMENDATIONS

The staff recommends making changes to NRC regulations applicable to security requirements in six areas (recommendations 1 - 6). The staff also recommends informing licensees of the NRC's position on (1) the compartmentalization of vital areas, and (2) safeguards information designation. The staff also believes it should closely monitor the effectiveness of the licensees' access authorization programs, with emphasis on the effectiveness of behavioral observation programs to verify the continued trustworthiness and reliability of individuals granted unescorted access. Each of these recommendations and the rationale for the recommendations are discussed below:

Recommendation 1

Revise the regulations to reduce the burden for key controls for vital area locks. Continue to require that doors between protected areas and vital areas remain locked, but permit the licensee to issue keys to any

individual who has unescorted access and who could require emergency access. Specify that the licensee need not take compensatory measures for mechanical lock hardware failure if the access control hardware and alarm are operable. An individual would still be required to use a card key for normal routine access, with metal keys to be used during card key equipment failures. This revision would not apply to locks used as part of the protected area barrier.

Rationale

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 regulations would retain the primary benefit of locking protected area to vital area doors which provides some delay for an external threat.

Remote unlocking of vital area doors is presently permitted by the regulations and has been implemented at many sites. By issuing keys to all individuals requiring emergency access, the licensee could eliminate any remaining concerns regarding emergency access. The threat from the loss of control of vital area keys is smaller and commensurate with lack of resistance to "forced entry" inherent in electrically controlled door strikes that are part of the access control system.

Recommendation 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 list every 31 days.

Rationale

At many sites, most persons granted access to the protected area also have access to most vital areas; at a number of sites, vital areas are not highly compartmented; and at all sites, all personnel granted access to the protected area must meet increased requirements (the FFD and Access Authorization rules) designed to improve the trustworthiness and reliability of workers. Therefore, the licensees derive little benefit from maintaining discrete lists of individuals allowed access to each separate vital area in the facility, and this is a tedious administrative function for many licensees. However, licensees obtain some benefit from restricting access to vital areas for those persons, such as administrative personnel, who are granted access to the protected area and who have no need for access to any vital area.

Recommendation 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. The NRC would still require response to certain alarms or a percentage of alarms.

Rationale

Many current requirements and practices for responding to door alarms and reporting these alarms are of marginal benefit for many of the reasons listed in the rationale section for Recommendation 2. Also, since a person reveals his or her identity when using a card key, persons who improperly use card key(s) can be traced and abuses corrected. There are some types of door alarms (i.e. intrusion alarms) that would still require response and investigation. To assure that access control system failures are corrected in a timely manner, licensees should continue to be required to post security officers as a compensatory measure if the card key system (including alarm) is inoperative.

Recommendation 4

Delete the regulatory 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.

Rationale

During periods when frequent access is permitted to containment, such as during refueling or major maintenance, the number of personnel and materials needing access can be very high. The licensee has difficulty controlling access of materials with a heavy traffic of materials being transported in and out of containment. The NRC has never published guidance defining "acceptable" material, and even certain "authorized" materials could be misused once in containment. Control of personnel and materials into containment is even more difficult in BWR designs because many entrances may have to be controlled and because the reactor building may be the containment boundary when the reactor head is removed. The requirement that access be controlled by a guard or watchperson provides little security since the purpose is to control access and not prevent a forced entry. After containment is secured following periods of heavy access, previous NRC guidance on operational and security walkdown inspections and searches is relevant.

Recommendation 5

Revise the regulations to eliminate the need for armed guards who are exiting and re-entering the protected area on official duty to have to pass through the metal detector. Unarmed guards and watchpersons will continue to meet all search requirements. Guards would still be expected to satisfy the search requirements for explosives.

Rationale

Armed security guards who leave the protected area as part of their duties must be re-searched upon re-entry into the protected area. While searches of packages carried by the guard or explosives detection searches protect against the introduction of contraband, passage of the guard through the metal detector, whose principal purpose is to detect firearms, serves little purpose. The guard either has to remove his or her weapon while passing through the detector, or be subject to a hand search. Either approach makes little sense for the guard who is authorized to carry a weapon on site. Further, removing and handling the guard's weapon could present a personnel safety risk.

Recommendation 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 driven by licensee personnel who have unescorted access. These vehicles while unattended in the protected area would have to remain locked and keys removed. This relaxation would apply to licensee-owned vehicles but not to vendor or contractor vehicles.

Rationale

Vehicles, except certain designated vehicles which remain in the protected area, must be searched upon entry and escorted by a member of the security organization while in the PA. Licensee-owned vehicles driven by permanent licensee employees with unescorted access must be escorted at all times (normal procedure for all non-designated vehicles) while in the protected area. The effectiveness of vehicle escorts was reduced when the NRC reduced the required number of armed escorts for a vehicle from two to one. Presently this requirement does little in protecting against the insider.

Recommendation 7

Inform licensees of the NRC position on the acceptability of reducing the number of separate vital area compartments.

Rationale

Various licensees have evidenced continuing confusion about the NRC's position on allowing them to reduce the number of vital area

compartments. Thus, some licensees considering reducing the number of vital areas, may be reluctant to proceed. The NRC could clarify that a site could remain as configured, if that is the most cost-effective method, or could designate a larger vital island(s).

Recommendation 8

Inform licensees of the NRC position on designating certain types of information as safeguards information.

Rationale

Various licensees and members of the staff have held diverse views as to whether or not certain documents containing lists or locations of certain vital or safety-related equipment should be protected as "Safeguards Information." A conservative approach to designating such documents as Safeguards Information has led, over the years, to assigning too many documents into this category. The NRC should inform licensees of the NRC position on designating as safeguards those documents containing lists or locations of vital equipment. This action should reduce the number of documents determined to be safeguards information.

Recommendation 9

Evaluate the adequacy of the licensee implementation of access authorization programs, including behavioral observation.

Rationale

One premise regarding this study was that access authorization programs are in place and working as intended, providing a significant measure of assurance of the trustworthiness and reliability of persons initially granted unescorted access to a nuclear power plant. To a certain extent this is a valid assumption. All licensees have had in place access authorization programs for a number of years, and many had upgraded those programs prior to the current regulations. NRC inspectors have inspected elements of these programs to varying degrees. Now that all licensees are required to have in place program elements required by the access authorization rule, these programs should be inspected to determine that appropriate elements are being adequately implemented.

The program for observing behavior is one important element of access authorization programs that should be evaluated. While background checks and psychological evaluations may demonstrate the past and present trustworthiness and reliability of individuals being granted unescorted access, the licensee must observe behavior to determine the continued stability of the individual. Actual events have shown that most vandalism and tampering acts at facilities are accomplished by employees granted unescorted access. Behavioral observation programs may spot and deal with employee problems before they reach a condition in which the person may commit such acts. Implementing effective

behavioral observation programs would lessen the need for other measures to address the continuing reliability and trustworthiness of individuals, such as periodically updating or reinvestigating a person's background.

Resource Implications:

The above recommended regulatory changes and restatements of existing guidance should serve to allow licensees to reduce security force manpower at power reactor facilities. 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. These recommendations involve no resource adjustment to the NRC five year plant.

C. STAFF ACTIONS

To implement the first six recommendations, the Office of Nuclear Regulation (NRR) would need to prepare a rule package and forward it to the Office of Nuclear Regulatory Research for processing. The NRR staff would need to prepare Generic correspondence for Recommendations 7 and 8 for transmission to reactor licensees. Recommendation 9 is currently being implemented through development of a Temporary Instruction which will assess licensee implementation of access authorization programs in response to the recent Access Authorization rule.

Attachment 1

SAFEGUARDS INSIDER DOCUMENTATION CHRONOLOGY

(E=EFFECTIVE DATE/P=PUBLISHED DATE/I=IMPLEMENTATION DATE)

02/01/73	FIRST PROPOSED SAFEGUARDS RULE, §50.34
06/00/73	REG GUIDE 1.7, PROTECTION AGAINST INDUSTRIAL SABOTAGE (P)
10/11/74	SECY-R-75-112, POLICY SESSION, PROPOSED AMEND. PART 73
11/13/74	PROPOSED RULE, CREATE A §73.55
02/24/77	FINAL RULE, 10 CFR 73.55 (P)
03/28/77	FINAL RULE, 10 CFR 73.55 (E)
02/28/79	FINAL IMPLEMENTATION OF §73.55 W/COMP MEASURES (I)
07/26/79	IE BULLETIN 79-16, VITAL AREA ACCESS CONTROLS (P)
00/00/80	ATOMIC EN. ACT OF 1954, ADDED SEC 236, MADE SABOTAGE A CRIME (E)
03/12/80	PROPOSED RULE, ACCESS CONTROLS TO VITAL AREAS
07/00/80	NUREG 0703, POTENTIAL THREAT FROM INSIDER (P)
03/10/82	IN 82-05, INCREASING FREQUENCY OF DRUG RELATED INCIDENTS (P)
03/16/82	IN 82-07, INADEQUATE SECURITY SCREENING PROGRAMS (P)
08/05/82	PROPOSED RULE, FITNESS-FOR-DUTY
00/00/83	ATOMIC EN. ACT OF 1954 AMENDED SEC 236, MADE TAMPERING A CRIME (E)
03/23/83	IN 83-15, FALSIFIED PRE-EMPLOYMENT SCREENING RECORDS
05/00/83	NUREG 0992, REPORT OF COMMITTEE TO REVIEW SAFETY/SAFEGUARDS
05/04/83	IN 83-27, OPERATIONAL RESPONSE TO DELIBERATE ACTS
08/01/84	PROPOSED RULE, ACCESS AUTHORIZATION
11/29/85	SECY-85-381, INSIDER SAFEGUARDS RULE

04/21/86	IN 86-27, ACCESS CONTROLS AT NUCLEAR FACILITIES (P)
06/25/86	COMM. DIRECTS CO-AUTHORSHIP OF POLICY STATE. ACCESS AUTH.
08/04/86	POLICY STATEMENT, FITNESS-FOR-DUTY
09/00/86	REGULATORY GUIDE 5.65, MISC. AMEND. IMPLEMENTATION (P)
09/03/86	FINAL RULES, MISC. AMENDMENTS & SEARCH REQUIREMENTS (E)
09/19/86	IN 86-83, UNDERGROUND PATHWAYS INTO PAs, VAs, & CCAs (P)
11/03/86	IN 86-91, LIMITING ACCESS AUTHORIZATIONS (P)
11/07/86	PROPOSED RULE, CRIMINAL HISTORY CHECKS, FINGERPRINTS (P)
02/12/87	GENERIC LETTER 87-04, EXEMPTION FROM FINGERPRINTS (P)
02/13/87	IN 87-11, ENCLOSURE OF VITAL EQUIP. WITHIN VAs (P)
04/16/87	FINAL RULE, MISC. AMEND, CORRECTIONS (E)
04/01/87	FINAL RULE, CRIMINAL HISTORY CHECKS (E)
05/11/87	GENERIC LETTER 87-08, MISC. AMEND. & SEARCH (P)
06/12/87	GENERIC LETTER 87-10, IMPLEMENTATION OF FINGERPRINTS (P)
02/00/88	NUREG 1178, VITAL EQUIP./AREA GUIDELINE STUDY (P)
03/09/88	POLICY STATEMENT ENDORSING NUMARC INDUSTRY GUIDELINES FOR ACCESS AUTHORIZATION, REV 8
05/16/88	IN 88-26, FALSIFIED PRE-EMPLOYMENT SCREENING RECORDS (P)
07/18/88	IN 88-49, WORKING WITH SAFEGUARDS INFORMATION (P)
09/22/88	PROPOSED RULE, FITNESS-FOR-DUTY
11/22/88	IN 88-91, IMPROPER ADMIN & CONTROL OF PSYCHOLOGICAL TESTS
12/00/88	GAO/RECD-89-41, GAO REPORT RECOMMENDING IMPROVED SCREENING
03/27/89	SECY-89-098, ACCESS AUTHORIZATION, RULE OR POLICY STATEMENT
04/19/89	CHILK TO STELLO, COMMISSION DIRECTS STAFF TO PREPARE GENERAL ACCESS AUTHORIZATION RULE AND ENDORSE NUMARC GUIDELINES IN REG GUIDE
06/07/89	FINAL RULE, FITNESS FOR DUTY, PART 26 (P)

09/00/89	NUREG 1267. TECHNICAL RESOLUTION OF GENERIC SAFETY ISSUE A-29
01/03/90	FINAL RULE, FITNESS FOR DUTY, PART 26 (I)
02/05/91	SECY-91-029, ACCESS AUTH. APPROVAL FOR RULEMAKING (P)
04/25/91	FINAL RULE, ACCESS AUTHORIZATION (P)
09/23/91	IN 91-53, PROBLEMS WITH ACCESS AUTHORIZATION PROGRAMS (P)
04/25/92	FINAL RULE, ACCESS AUTHORIZATION (I)

Attachment 2

SAFETY/SAFEGUARDS DOCUMENT CHRONOLOGY

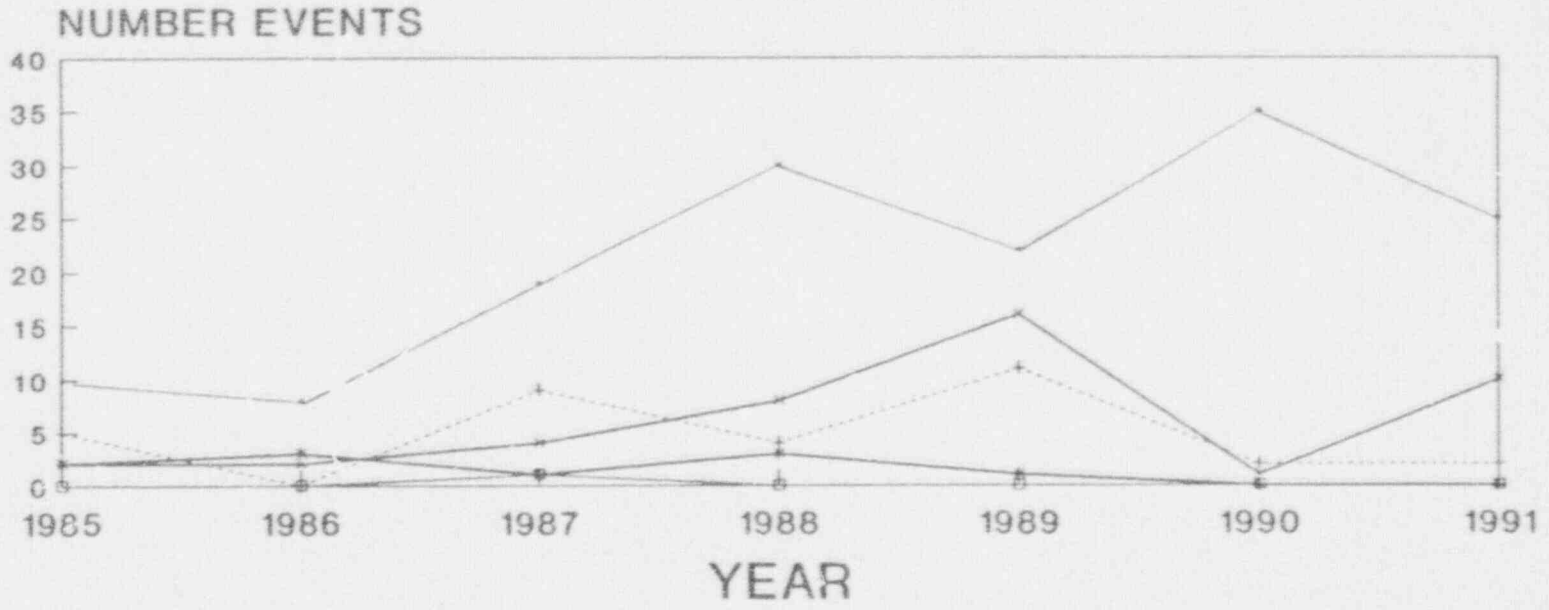
(E=EFFECTIVE DATE/P=PUBLISHED DATE/I=IMPLEMENTATION DATE)

02/01/73	FIRST PROPOSED SAFEGUARDS RULE, §50.34
11/13/74	PROPOSED RULE, 10 CFR 73.55
02/24/77	FINAL RULE, 10 CFR 73.55 (P)
03/28/77	FINAL RULE, 10 CFR 73.55 (E)
01/00/78	NUREG 0416, SECURITY PLAN EVALUATION REPORT WORKBOOK (P)
01/19/78	IE BULLETIN 77-08, ASSURANCE OF SAFETY/SAFEGUARDS DURING EMERGENCY, LOCKING SYSTEMS
02/28/79 03/12/80	IMPLEMENTATION OF 10 CFR 73.55 W/ COMPENSATORY MEASURES PROPOSED RULE, ACCESS CONTROLS TO VITAL AREAS
08/00/82	NUREG 0908, ACCEPTANCE CRITERION FOR SECURITY PLANS (P)
05/00/83	NUREG 0992, REPORT OF THE COMMITTEE TO REVIEW SAFEGUARDS REQUIREMENTS AT POWER REACTORS (P)
06/09/83	IN 83-36, IMPACT OF SEC. PRACTICES ON SAFE OPERATIONS (P)
12/19/83	IN 83-83, PORTABLE RADIO USE AT NUCLEAR PLANTS (P)
08/01/84	PROPOSED RULE, MISCELLANEOUS AMENDMENTS
10/19/84	GENERIC ISSUE 81, IMPACT OF LOCKED DOORS & BARRIERS (P)
12/31/84	GENERIC ISSUE 81, REV ONE, ISSUE DROPPED (P)
03/00/85	NUREG/CR 4093, SAFETY/SAFEGUARDS INTERACTION DURING SAFETY EMERGENCIES
07/10/86	IN 86-55, DELAYED ACCESS DURING PLANT OPERATIONS (P)
09/00/86	REGULATORY GUIDE 5.65, MISCELLANEOUS AMENDMENTS IMPLEMENTATION (P)
09/03/86	FINAL RULES, MISC. AMENDMENTS & SEARCH REQUIREMENTS (E)
00/00/87	GENERIC ISSUE 81, PRIORITY RAISED TO LOW
05/11/87	GENERIC LETTER 87-08, MISC. AMEND. & SEARCH (P)

INSIDER RELATED EVENTS

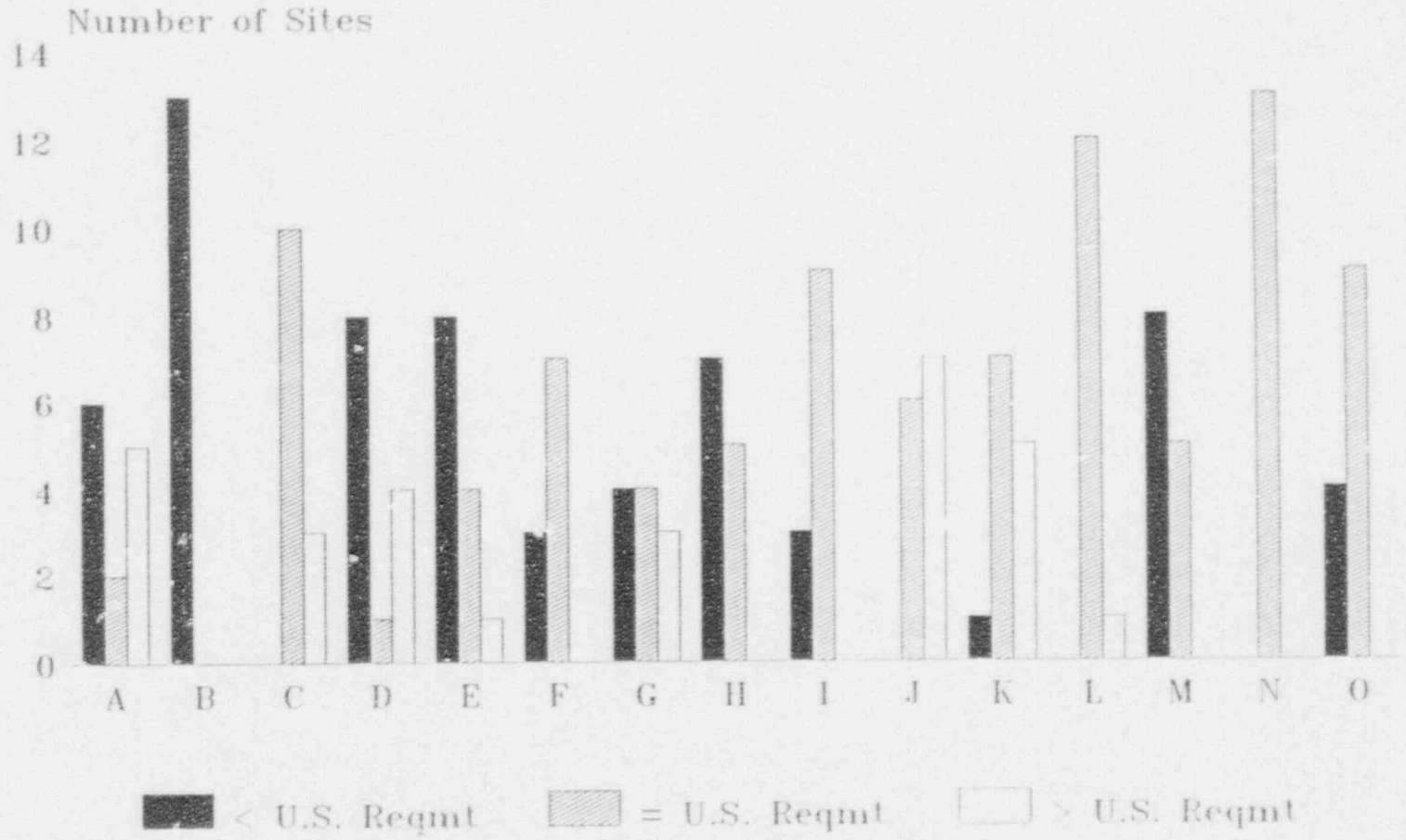
(Total of 245 Out of 568)

(Potentially Exploitable or Exploited)



Attachment 3

INTERNATIONAL PROGRAM ELEMENT COMPARED TO U. S. ELEMENTS



A:	*	Design Basis Threat	F:		Security Training Exercises	K:		Intrusion Detection Systems
B:		Truck Bomb Contingency	G:		Offsite Response Force	L:		Assessment
C:		Guard Type	H:	*	Personnel B I Screening	M:	*	Alarm Stations
D:		Armed Guards	I:		Deadly Force	N:	*	Access Control
E:		Guard Force Size	J:		Barriers (PA)	O:	*	Access Search

* Insider Elements

Attachment 4

Enclosure 2

NUMARC LETTER TO B. K. GRIMES
DATED JUNE 24, 1992

Enclosure 2

NUCLEAR MANAGEMENT AND RESOURCES COUNCIL

1776 Eye Street, N.W. • Suite 300 • Washington, DC 20006-2496
(202) 872-1280

June 24, 1992

Mr. Brian K. Grimes
Director
Division of Reactor Inspection
and Safeguards
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Dear Mr. Grimes:

The purpose of this letter is to transmit a NUMARC paper, "NUMARC Protective Measures Requirements Re-evaluation" to the NRC. It addresses areas where security resources can be redirected without a reduction in the level of security effectiveness. The paper is the result of efforts by the NUMARC Security Working Group and reflects comments from the industry. NUMARC personnel have met with your staff on two occasions to advise them of the working group's activities. At those meetings we learned of a related effort by the NRC staff in response to a Commission directive. This paper is offered for use in the staff's response to the Commission.

We believe that the fitness-for-duty (10 CFR 26) and access authorization (10 CFR 73.56 and 73.57) programs are providing a trustworthy nuclear power workforce. This belief is the basis for the recommendations contained in the paper.

If you have any questions on this material, or if we can be of further assistance in this matter, please call Rich Enkeboll or me.

Sincerely,

Robert N. Whitesel
Manager
Operations, Management
and Support Services Division

RNW/REE:ldl
Enclosure

Protective Measures Requirements Re-evaluation

June 1992

Nuclear Management and
Resources Council, Inc.
1776 Eye Street, N.W.
Washington, D.C. 20006-3706

NUMARC PROTECTIVE MEASURES REQUIREMENTS RE-EVALUATION

INTRODUCTION

NUMARC established a Security Working Group in 1990 to focus on industry concerns about nuclear plant security. This paper has been developed by NUMARC with the guidance of the Security Working Group. NUMARC staff members were assisted in this endeavor by an Ad Hoc Advisory Committee (AHAC) of several industry security managers. This paper addresses four specific issues that resulted from an industry re-evaluation of current protective measure requirements. The primary issue, vital area security requirements, is addressed in several places in 10 CFR 73.55, paragraphs (b) through (h). There are three other industry concerns addressed in that part of the regulations, and they have been included in this paper as well. The paper presents recommendations for changes allowing security resources to be redirected without a reduction in the level of security effectiveness. Commensurate revisions in nuclear power reactor site physical security plans are also discussed in general terms.

This paper is divided into three parts. Part I provides background information on the thought process which led to the re-evaluation of current security regulations and their effectiveness in today's power reactor security environment. Part II contains a description of industry conclusions with regard to protection against a potential insider in today's environment. This viewpoint is called the Alternative Protection Strategy (APS). When appropriate credit is allowed for the APS, the industry believes it will provide a high level of security effectiveness, equivalent to but different from the controls specified in 10 CFR 73.55 (b)-(h) for the issues covered in this paper. Part III describes the four security issues in more detail, provides applicable citations from § 73.55, makes recommendations for each issue and includes the associated rationale.

PART I

BACKGROUND

Within the past few years the NRC has promulgated, and all licensees have implemented, regulations that require extensive personnel screening programs (fitness-for-duty and access authorization including FBI criminal history) for unescorted access to protected areas of nuclear power plants. Although all utilities had personnel screening programs in place, and many had implemented fitness-for-duty programs prior to the regulations, implementation of these requirements has resulted in more uniformity in programs across the industry. The access authorization requirements of 10 CFR 73.56, the fitness-for-duty requirements of 10 CFR 26, the continual behavioral observation programs and industry professionalism programs have enhanced the trustworthiness of the cadre of licensee and contractor personnel that make up the workforce which has unescorted access to nuclear reactor plant protected areas. Confidence in workforce trustworthiness is reinforced by training programs designed to increase worker understanding as well as supervisory sensitivity to conditions that could undercut someone's trustworthiness.

The passage of time and the new, more stringent unescorted access requirements have provided the opportunity to review the protective measures established more than a decade ago in a time of unsettled world security conditions. It is now possible to refocus security activities without reducing security effectiveness. The industry believes that these access programs, taken as a whole, constitute an Alternative Protection Strategy (APS) that will accomplish that objective. The four areas included in this re-evaluation and described in more detail in Part III are:

- Security requirements for vital areas;
- Posting a security guard at containment;
- Vehicle escort requirements; and
- Re-searching on-duty armed security guards.

The basis for applying the APS is found in § 73.55 (a):

"The Commission may authorize an applicant or licensee to provide measures for protection against radiological sabotage other than those required by this section if the applicant or licensee demonstrates that the measures have the same high assurance objective as specified in this paragraph and that the overall level of system performance provides protection against radiological sabotage equivalent to that which would be provided by paragraphs (b) through (h) of this section and meets the general performance requirements of this section."

The industry believes that the APS described in Part II meets this assurance objective. Licensees could choose this alternative or continue to meet the applicable requirements of 10 CFR 73.55 (b)-(h) by making specific commitments in their Physical Security Plans.

PART II

ALTERNATIVE PROTECTION STRATEGY

Each licensee authorized to operate a nuclear power reactor must submit for NRC approval a physical security plan that meets the general performance objective and requirements of 10 CFR 73.55 (a). *"The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in § 73.1(a). To achieve this general performance objective, the on-site physical protection system and security organization must include, but not necessarily be limited to, the capabilities to meet the specific requirements contained in paragraphs (b) through (h) of this section."* The APS is an equivalent alternative that licensees could implement in lieu of the cited sections of 73.55 (See Part III). The APS addresses the insider element of the design basis threat (DBT) as described in 10 CFR 73.1(a)(1). It recognizes that personnel screening programs work in concert with plant hardware to protect the health and safety of site personnel and the general public from radiological sabotage. Radiological sabotage is defined as a malevolent act within the protected area that would cause a radiological (fission product) release in excess of that specified in 10 CFR Part 100.11.

A. Protection from the Insider Element

The APS addresses the insider threat by providing high assurance that personnel granted unescorted access to the protected area are trustworthy, reliable and not likely to become involved in causing radiological sabotage. To achieve this, several major programs have been implemented and are applicable to all individuals granted unescorted access. Programs designed to directly minimize the insider threat include:

1. Access Authorization Program - A program that conforms with 10 CFR Part 73.56, "Access Authorization to Commercial Nuclear Power Plants" as implemented by Regulatory Guide 5.66, "Access Authorization Programs for Nuclear Power Plants." Such a program assures that individuals granted unescorted access to protected and vital areas have trustworthy backgrounds, stable psychological profiles and reliable behavior consistent with the safe operation of the facility. It provides high assurance that individuals granted unescorted access are trustworthy and reliable, and do not constitute an unreasonable risk to the health and safety of the public including a credible potential to commit radiological sabotage.

2. Criminal History Check - The Criminal History Check Program is an integral part of the Access Authorization Program and conforms

with the requirements of 10 CFR 73.57, " Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information by power reactor licensees." The purpose of the program is to ensure that proper consideration is given to an individual's past criminal activities prior to granting permanent unescorted access.

3. Fitness-For-Duty Program - The Fitness-For-Duty Program conforms with the requirements of 10 CFR 26. This program provides reasonable assurance that personnel granted unescorted access to the protected area are reliable, trustworthy and physically able (specifically, drug and alcohol free) to safely and competently perform their duties. The program provides reasonable measures for the early detection of persons who should not be allowed access to the protected area. Results experienced to date from licensee fitness-for-duty programs show that program objectives are being achieved.

4. Continual Behavioral Observation Program - The Continual Behavioral Observation Program is a key element of the APS and conforms with the provisions of Regulatory Guide 5.66. Each individual granted unescorted access is subject to the Continual Behavioral Observation Program. Management and supervisory personnel are responsible for observing personnel for behavioral traits and patterns that may reflect adversely on their trustworthiness or reliability and reporting those observations to appropriate utility management. The core of the program is the specific training which provides reasonable assurance that management and supervisory personnel have the awareness and sensitivity to detect and report changes in behavior, including suspected alcohol and drug abuse, which adversely reflects upon the individual's trustworthiness or reliability, and then to have the judgment to refer these persons for appropriate evaluation and follow-up action.

5. Law Enforcement Intelligence Network - Federal, State and local law enforcement agencies, in concert with the intelligence community, have significant capabilities to detect the planning activities of individuals who are intent on performing acts of radiological sabotage. Points of contact and lines of communication have been established to ensure the timely flow of significant information. The FBI Key Asset Protection Program is able to provide federal liaison with local law enforcement agencies (LLEA).

B. Programs Supporting Protection from the Insider Element

In addition to the direct programs for minimizing the insider threat there are several supporting programs that provide internal checks and balances that ensure they are functioning properly. These include:

1. Industry Professionalism Programs - These programs are fostered by the industry for the express purpose of setting professionalism standards and ensuring the highest levels of knowledge and personal character for the nuclear worker. Many of these programs encourage the concept of "employee involvement" whereby personnel bring excellence not only to their own specific job but to the entire work environment. These programs are designed to improve the effectiveness of all facets of nuclear plant operations and maintenance, including physical security and safeguards by facilitating a culture of professionalism in how staff and management approach their job. Important to security is the focus of this culture to greatly increase employee awareness of their work environment and to create incentive for improvement.

2. Systems Operations - Plant operations are conducted and controlled in accordance with strict Technical Specifications and plant licensing requirements. Operators are subject to rigorous training and qualification requirements. Responsibility and authorization for operating actions are rigidly controlled. This level of professionalism and control are key elements in protecting the public health and safety.

3. Quality Assurance (QA) Programs - Quality assurance programs, comprised of plans, procedures, training programs, directives, and instructions, represent a major management system which provides internal checks and balances and assurance of the reliability of redundant safety systems. QA programs include surveillances, inspections and other activities which provide active oversight of plant operations, radiological protection, emergency preparedness, fitness-for-duty, testing and maintenance and other programs which collectively provide high assurance that an individual could not successfully commit an act of radiological sabotage leading to a significant off-site release of radiation.

In summary, these programs result in an attitude in the work place which would preclude or expose individuals intent on acts of radiological sabotage. Thus, the programs provide high assurance that personnel granted unescorted access represent a high standard of trustworthiness and of the reliability.

C. Programs that Indirectly Enhance Plant Protection

Programs that indirectly enhance the effectiveness of the APS include:

1. Plant Design and Operation - The complexity of nuclear power plant systems and the defense-in-depth philosophy, i.e., component redundancy and multiple barriers to the release of fission products, make radiological sabotage difficult. Successfully reaching critical plant areas or systems does not automatically

translate into successful radiological sabotage. Factors such as current plant operations, fuel life, engineered safety systems, and operator mitigating actions, all come into play when determining if the malevolent acts are going to be successful in producing radiological sabotage.

2. Surveillance and Maintenance Programs - Surveillance programs provide continuous verification of the ability of plant systems to meet design requirements, under specified environmental, chemical, and/or operating conditions. When surveillances reveal that a system does not satisfy strict requirements, the necessary corrective action is taken to restore the system to a state of readiness. A program of scheduled preventive maintenance is designed to minimize failures.

3. Emergency Preparedness and Response Programs - Comprehensive Emergency Plans and casualty procedure programs are found at all licensed nuclear generating plants. These include on-site and off-site emergency facilities, highly trained licensee and state, local, and Federal government response organizations, and ongoing drills and exercises, employing a full spectrum of challenging scenarios, including biennial NRC/FEMA graded exercises. These elements combine to provide high assurance of the ability to prevent, mitigate and/or minimize the effects of an act of radiological sabotage.

D. Protection from the Outsider Element

In addition to the insider threat, nuclear power plant licensees also have in place detailed security measures to counter threats from external assaults by preventing the outsider from gaining the ability to sabotage critical plant systems that could lead directly to a fission product release in excess of that specified in 10 CFR 100.11. These measures are summarized here for completeness; they do not change as a result of the APS:

1. A physical protection system which protects against the threat of radiological sabotage, including:

   - Perimeter physical protection barriers and illuminated isolation zones;
   - Surveillance and patrols of the perimeter barriers;
   - Perimeter intrusion detection systems;
   - Alarm assessment (e.g., closed-circuit television, visual, etc.);
   - Response force; and
   - Penetration-resistant barriers at strategic points.

2. A physical security organization with appropriately trained personnel capable of carrying out the NRC-approved Physical Security Plan provisions.

3. Access controls for personnel and vehicles that include the positive identification of persons and the searching of vehicles and personnel.

4. The capability to execute safeguards contingency plans for dealing with threats which are to be countered with well-trained, well-equipped personnel who collectively determine a threat's existence, assess its magnitude and are able to act promptly to neutralize it.

5. The availability of local law enforcement agency support through mutual aid response agreements.

In summary, the above protection elements continue to be in place to neutralize the outsider element by detection, assessment and interdiction. The APS described above provides the same high assurance objectives as the level of protection afforded by vital area controls. Development of the APS has been enabled by the significant additional regulatory requirements addressing fitness-for-duty, unescorted access authorization, and continual behavioral observation programs.

PART III

ALTERNATIVE PROTECTION STRATEGY EQUIVALENCIES (CITED FROM 10 CFR 73.55)

The APS described in Part II provides security effectiveness with the same assurance objectives as the level of protection afforded by the vital area controls specified in 10 CFR 73.55 and the various programs which support it. The objective of the APS is to ensure that security resources are not spent on areas which provide little or no real protection. The stringent access authorization process minimizes the potential that an unescorted employee/contractor would become an "insider" who would commit an act of radiological sabotage or assist terrorists in such sabotage. As such, certain specific protective measures requirements have been re-evaluated and the following describes where security resources can be redirected without decreasing safeguards effectiveness.

A. Security requirements for vital areas.

1. Issue: Responding to vital area door alarms has been demonstrated to be of little or no security benefit. The NRC's Regulatory Effectiveness Review (RER) drills have shown that vital area doors are of minimal value as an obstacle to would-be saboteurs. By acknowledging that locked vital area doors and their key card access systems are no longer effective for safeguards and security purposes, resources could be released for more meaningful activities. Using the current door control systems for administrative purposes would then be a licensee management option.

2. Regulatory citations: Several regulations pertain to the vital area door issue:

a. 73.55(c) Physical barriers.

> *"(1) The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements of paragraph (a) of this section. More than one vital area may be located within single protected area."*

b. 73.55(d) Access Requirements.

"(7) The licensee shall:
(i) Establish an access authorization system to limit unescorted access to vital areas during nonemergency conditions to individuals who require access in order to perform their duties. To achieve this, the licensee shall:"

"(A) Establish current authorization access lists for each vital area. The access lists must be updated and reapproved by the cognizant licensee manager or supervisor at least once every 31 days. The licensee shall include on the access list only individuals whose specific duties require access to vital areas during nonemergency conditions."

"(B) Positively control, in accordance with the access list established pursuant to paragraph (d)(7)(i) of this section, all points of personnel and vehicle access to vital areas."

"(D) Lock and protect by an activated intrusion alarm system all unoccupied vital areas."

"(9) All keys, locks, combinations, and related access control devices used to control access to protected areas and vital areas must be controlled to reduce the probability of compromise."

3. Recommendation: Accept the fact that the APS provides the necessary plant security. Either modify affected regulation or issue a generic letter that accepts the APS as an alternative to the associated vital area requirements of 10 CFR 73.55, paragraphs (b)-(h).

4. Rationale: When the cited regulatory provisions were incorporated into NRC requirements, world security conditions were different, and current programs to ensure trustworthiness of workers were not in place. The access authorization, fitness-for-duty, employee training programs and continual behavioral observation programs have significantly enhanced a licensee's security posture in regards to the potential insider. In view of RER findings that vital area doors provide no significant protection against the DBT external threat and because the APS provides licensees with reasonable assurance that the insider threat is being adequately addressed, vital area access controls are no longer effective for safeguards and security purposes. Physical Security Plans can therefore be modified to implement the APS option and refocus security resources in other, more effective ways.

B. Posting a security guard at containment.

1. Issue: A security guard is the wrong individual to control access of personnel and materials entering containment; this is an operations/maintenance function. Personnel security checks have been accomplished prior to anyone gaining unescorted access to the protected area.

2. Regulatory citation: § 73.55(d)(8) states: *"Any time frequent access is permitted to containment such as during refueling or major maintenance, positive access control to assure that only authorized personnel and materials are permitted into containment shall be exercised by the licensee, with a guard or watchmen."*

3. Recommendation: Either remove the citation from security regulation or delete the requirement for "a guard or watchmen." A generic letter could be used to state the expectation for containment access controls pending permanent rule change.

4. Rationale: While good management practices during outages frequently require control of tools and/or combustible materials entering or leaving containment, stationing a security guard at this access point is unnecessary for safeguards and security purposes. Introduction of contraband into containment is already addressed by the aforementioned programs to ensure personnel integrity. Tool/combustible material control is a function accomplished by operations/maintenance personnel. This responsibility should not be the province of the security force.

   Licensees who apply the APS will have fulfilled the requirements of this section. In addition to the trustworthiness and reliability of individuals entering containment, personnel and material would have previously been searched in accordance with 73.55(d)(2), (3) & (4). Entry control for security purposes at the containment access point is redundant, unnecessary, and ineffective.

C. Vehicle escort requirement.

1. Issue: Current regulation, § 73.55(d)(4), requires an escort for each vehicle entering the protection area even though the driver may be badged for unescorted access.

2. Regulatory citation: § 73.55(d)(4) specifies: *"All vehicles, except designated licensee vehicles, requiring entry into the protected area shall be escorted by a member of the security organization while within the protected area..."*

3. Recommendation: Modify § 73.55(d)(4) to add the following after the third sentence: "The escort requirement is waived for vehicles whose drivers have been badged for unescorted access to the protected area." Alternatively, such a position could be included in the generic letter suggested above.

4. Rationale: Utilities have been escorting vehicles to comply with the requirements of § 73.55(d)(4) even though it is unnecessary with current access controls. This same regulation requires a thorough search of the vehicle prior to its being allowed into the protected area. The drivers of such vehicles frequently have unescorted access authorization to the plant. From a security standpoint, there is no logical reason why a searched vehicle with a driver who has been granted unescorted access needs to be escorted. As with any other individual who has been granted unescorted access, no escort is needed.

   Licensees who apply the APS will have fulfilled this requirement if individuals with unescorted access are driving searched vehicles. Based on the stringent access authorization requirements which must be met before an individual is granted unescorted access, the training and implementation of continual behavioral observation and the vehicle search requirements of this section, the additional protection afforded by an escort from a member of the security organization is neither cost effective nor an efficient use of security resources.

D. Re-searching on-duty armed security guards.

1. Issue: Generic Letter 87-08 explains the § 73.55(d)(1) requirement that security guards re-entering the protected area after completing assigned duties outside of the protected area must pass through the metal detectors. If the detectors alarm, the guard must be patted-down to detect the presence of one or more firearms.

2. Regulatory citation: § 73.55(d)(1) specifies: *"The licensee must subject all persons except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry into a protected area."*

3. Recommendation: Remove the distinction between law enforcement officers cited in § 73.55(d)(1) and licensee security personnel. One way of accomplishing this is to modify the answer to Question 11 of Generic Letter 87-08, "Implementation of 10 CFR 73.55 Miscellaneous Amendments and Search Requirements," to read: "Members of the security force must be equipment searched on their initial entry to the PA at the beginning of their work shift. If

these individuals leave the PA to perform official duties subsequent to this initial search, they need not be searched prior to re-entry into the PA." The remainder of the answer is deleted to resolve the issue.

4. Rationale: The distinction between law enforcement officers and licensee security personnel is unwarranted. The visiting law enforcement officers will, for the most part, be under continual escort while inside 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 personnel are more trustworthy than screened security officers. The benefits of removing this unwarranted distinction are the elimination of:

- Those requirements that do not enhance security;
- The unnecessary removal of the officer's weapon which is a personnel safety hazard; and
- The current implication that security force personnel are not as trustworthy as other law enforcement officers.

Licensees who apply the APS will have fulfilled this requirement for armed security officers during the daily course of their duties after an initial search when reporting for work. Additional searches when these officers move through the guardhouse or protected area boundary would not be performed. Since all employees with unescorted access authorization, including the guard force, meet the requirements of the access authorization program, the security officers deserve the same trustworthiness recognition granted to fellow employees.

SUMMARY

This re-evaluation of protective measures at nuclear power plants shows that four current NRC requirements provide little or no contribution to plant security. Access authorization, fitness-for-duty, continual behavioral observation and industry professionalism programs are in place to minimize the threat from insiders. Accordingly, the requirements for vital area door security (including compensatory measures), posting security officers at containment access, escorting cleared vehicles driven by cleared individuals, and re-searching on-duty armed security officers should be deleted.