121450
~~25600~~

BY THE U.S. GENERAL ACCOUNTING OFFICE

Report To The Chairman, Nuclear Regulatory Commission

Additional Improvements Needed In Physical Security At Nuclear Powerplants

Since the middle 1970's, the Nuclear Regulatory Commission and powerplant operators have taken measures to reduce the vulnerability of powerplants to attempted acts of sabotage. GAO's evaluation disclosed that further improvements can be made by

--screening nuclear plant employees to reduce the number of potential saboteurs and

--strengthening the physical security systems to ensure their compatibility with other plant safety systems.

The Commission has taken two initiatives addressing these improvements. Therefore, GAO is not making recommendations at this time.

121935

GAO/RCED-83-141
JULY 13, 1983

026216

Request for copies of GAO reports should be sent to:

U.S. General Accounting Office
Document Handling and Information
Services Facility
P.O. Box 6015
Gaithersburg, Md. 20760

Telephone (202) 275-6241

The first five copies of individual reports are free of charge. Additional copies of bound audit reports are $3.25 each. Additional copies of unbound report (i.e., letter reports) and most other publications are $1.00 each. There will be a 25% discount on all orders for 100 or more copies mailed to a single address. Sales orders must be prepaid on a cash, check, or money order basis. Check should be made out to the "Superintendent of Documents".

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

RESOURCES, COMMUNITY,
AND ECONOMIC DEVELOPMENT
DIVISION

B-127945

The Honorable Nunzio J. Palladino
Chairman, Nuclear Regulatory Commission

Dear Mr. Chairman:

We recently completed an evaluation of how well the Nuclear Regulatory Commission (NRC) is performing its regulatory responsibilities for assuring the adequacy of physical security at commercial nuclear powerplants. Our review focused on recommendations made in our 1977 report[1] with an overall objective of evaluating the vulnerability of nuclear powerplants to attempted acts of sabotage. We found that many of the weaknesses noted by our 1977 report have been corrected and that physical security systems at commercial nuclear powerplants have been substantially improved.

However, there are areas where further improvements in physical security can be made. The first centers around minimizing the threat of sabotage from internal sources. NRC's regulations require all powerplants to protect against an internal threat but NRC has not established criteria for ensuring the integrity of nuclear powerplant employees.[2] Secondly, some licensees and NRC officials believe that certain physical security requirements are conflicting with the safety of nuclear powerplants.

NRC is in the process of considering actions aimed at addressing both of these areas. The NRC staff is working on a proposed personnel screening requirements rule which is designed to establish a standard on the reliability and trustworthiness of plant employees. NRC also established a Safety/Safeguards Review Committee which addressed the second issue and recently forwarded its findings and recommendations to the Commissioners

---

[1]"Security At Nuclear Powerplants--At Best, Inadequate," EMD-77-32, Apr. 7, 1977.

[2]Plant employees, for the purposes of this report, include all individuals who are allowed unescorted access to the plant site. These individuals include employees who work directly for the NRC licensee or a contractor hired by the licensee.

for review. Based on our visits to 3 nuclear powerplants and discussions with plant officials, the findings and recommendations of the Committee's report appear to be consistent with the results of our review.

Because you and the other Commissioners are considering the proposed personnel screening rule and the recommendations in the Committee's report, we are not at this time making recommendations concerning security at the Nation's nuclear powerplants. We do, however, request to be informed on how the Commission disposes of the recommendations in the Committee's report and your actions with respect to the proposed rule.

- - - -

Although we did not obtain official agency comments on this report, we did provide copies of this report to NRC program officials for their review and comment. They said the report contained no factual errors and in their opinion the statements and findings contained therein were representative of NRC's physical security program. With that exception, we performed our work in accordance with generally accepted government audit standards.

The details of our review are contained in appendices I and II, and the objective, scope, and methodology are contained in appendix III. We are sending copies of this report to the Chairman, Subcommittee on Oversight and Investigations, House Committee on Interior and Insular Affairs, other interested congressional committees, and the Office of Management and Budget. Copies of the report will also be provided to others upon request.

Sincerely yours,

J. Dexter Peach
Director

Contents

		Page
APPENDIX		
I	ADDITIONAL IMPROVEMENTS NEEDED IN PHYSICAL SECURITY AT NUCLEAR POWERPLANTS	1
	NRC is responsible for regulating physical security at nuclear powerplants	1
	Prior GAO report on physical security at nuclear powerplants	2
	Physical security at nuclear powerplants has improved	4
	History of security events shows concern for inside threats	5
	Opportunities exist for minimizing the insider threat	8
	Implementation of physical security systems has caused potential safety problems	9
II	ABNORMAL OCCURRENCE	13
III	OBJECTIVE, SCOPE, AND METHODOLOGY	14

ADDITIONAL IMPROVEMENTS NEEDED IN PHYSICAL SECURITY AT NUCLEAR POWERPLANTS

NRC IS RESPONSIBLE FOR REGULATING PHYSICAL SECURITY AT NUCLEAR POWERPLANTS

The Atomic Energy Act of 1954 and the Energy Reorganization Act of 1974 directed NRC to regulate the physical security provided by its nuclear powerplant licensees. The NRC physical security objective for nuclear powerplants is to develop and require implementation of measures designed to prevent, deter, and respond to acts of radiological sabotage. Radiological sabotage is defined as a deliberate act of destruction, damage, or manipulation of vital equipment[3] which could result in the release, beyond the plant boundary, of sufficient radioactive materials to endanger public health and safety due to radiation exposure. Therefore, physical security systems are primarily designed to prevent someone from destroying or tampering with safety-related equipment which could cause a release of radiation that would endanger public health and safety.

NRC assures the adequacy of physical security systems at nuclear powerplants through its powerplant licensing and inspection programs. All licensees must have security plans that have been reviewed and approved by NRC headquarters before they can be licensed to operate a nuclear powerplant. After the security plan has been approved, NRC, through its inspection program, determines whether or not the licensee's implementing procedures will fulfill the commitments in the licensee's security plan.

Physical security is important because it is another measure, in addition to back-up safety systems, that assures the safe operations of a nuclear powerplant. A physical security system is intended to prevent intentional acts that could lead to the unsafe operation of a powerplant. Therefore, it is incumbent upon the NRC to assure that adequate physical security systems are installed at all operating nuclear powerplants because a serious act of radiological sabotage could have the same effect as a major accident at a nuclear powerplant. The importance of physical security at nuclear powerplants has been

---

[3]Vital equipment means any equipment, system, device, or material whose failure, destruction, or release could directly or indirectly endanger the public health and safety by exposure to radiation.

further demonstrated by the enactment of legislation[4] that makes acts of sabotage against nuclear powerplants Federal crimes punishable by imprisonment or fines, or both.

PRIOR GAO REPORT ON PHYSICAL SECURITY AT NUCLEAR POWERPLANTS

In our 1977 report on physical security at nuclear powerplants, we concluded that NRC had not acted decisively or effectively in the security area and, as a result, security systems at perhaps all powerplants would not be able to withstand sabotage attempts. The primary cause for the inadequacies at the time was the Commission's failure to define minimum threat levels[5] which licensees could use to establish their physical security systems. As a result, we found vast differences in the degree of protection at powerplants.

For example, one plant we visited was protected by magnetic alarms on area gates; an infrared alarm system along the perimeter of the plant; a closed circuit television system which views the perimeter of the fence both day and night; a computerized key-card system for all important doors in the plant that monitored and recorded the opening and closing of the doors; and an attack-resistant guard house with bullet-proof glass, steel-plated ceilings, and dual electrical systems. By contrast, at another plant, the primary security device was an 8-foot fence topped with barbed wire. There were no sensitized fences or gates, no infrared alarm systems, no closed circuit television systems, and a guard house which was not attack-resistant.

The greatest single shortcoming was the quality of the guard forces at nuclear powerplants. There were no specific training or qualification requirements for members of the guard forces and, as a result, we found that the performance of the guard forces was poor. New members of the guard force at one

---

[4]On June 30, 1980, Congress enacted public law 96-295, section 204A (42 U.S.C. section 2284), "Sabotage of Nuclear Facilities or Fuel," which makes it a federal crime to commit acts constituting "sabotage" against nuclear powerplants. In addition, other Federal criminal statutes relating to explosives, bombs, firearms, and extortion can be used to investigate sabotage of electric power systems.

[5]A minimum threat level describes what powerplants have to protect against. It gives the characteristics (number, training, equipment, etc.) of the potential saboteur(s).

plant were given as little as 4 hours training before they were used as guards. Further, some licensees were not conducting adequate background screening to determine whether a guard had a criminal record or whether there was anything in his background that would cause the licensee concern about his trustworthiness.

Improvements were also needed in NRC's inspections of physical security systems. We found that NRC inspectors were not authorized or encouraged to go beyond the licensee's security plans when looking at security systems. As a result, inspectors were only checking for the existence of physical security systems and commitments in the licensee's security plan but were not checking to see how well the security systems performed in preventing attempts of sabotage.

We made several recommendations to correct the inadequacies in physical security at nuclear powerplants. Specifically, we recommended that NRC

--establish criteria for judging the acceptability of alternative protective devices and systems,

--implement a procedure whereby security plans cannot be approved until a site has been visited by the reviewer and the comments of the regional inspection office have been obtained,

--establish specific and stringent requirements for upgrading guard forces,

--authorize and encourage inspectors to go beyond approved security plans when appraising security systems and implement a timely procedure for correcting deficiencies, and

--develop and implement additional procedures to provide greater assurance that inspectors are consistently thorough and make unannounced inspections.

Based on our review of the actions taken by NRC to the above recommendations, we believe the recommendations have been implemented. Both NRC and industry officials told us that our 1977 report served as a catalyst to upgrade physical security at nuclear powerplants.

PHYSICAL SECURITY AT NUCLEAR POWERPLANTS HAS IMPROVED

Our review found that NRC and powerplant operators have taken measures to improve the level of protection against acts

of sabotage. For example, security guards now have to meet specific training and qualification requirements, security inspections are unannounced, and NRC inspectors are authorized and encouraged to perform independent evaluations in addition to required inspections when appraising security systems. NRC has established procedures for conducting site visits before security plans are approved; these include a survey by the license reviewer and an inspection by the NRC regional office. Some powerplants have had to upgrade their security equipment and related hardware since our 1977 report and, when considered in combination with improvements made in the guard forces, better protection against acts of sabotage now exists.

On February 24, 1977, NRC published in the Federal Register proposed regulations to upgrade physical security at nuclear powerplants. These proposed regulations became effective on March 28, 1977, and licensees had until February 23, 1979, to fully implement them. These new regulations are contained in Title 10 of the Code of Federal Regulations, Part 73, Section 55 (10 C.F.R. 73.55) with appendices. One of the most significant improvements NRC made was to define a physical security performance standard that all commercial nuclear powerplants must meet. This standard defines the "design basis threat" as:

(1) A determined violent external assault, attack by stealth, or deceptive actions, of several persons who are well trained (including military training and skills) and dedicated; have inside assistance which may include a knowledgeable individual; have suitable weapons up to and including hand-held automatic weapons, equipped with silencers; and use explosives, or

(2) a threat by an insider, including an employee in any position.

The regulations governing physical security at nuclear powerplants also require that all licensees have a physical security organization, physical barriers, access control measures, detection aids, communication equipment, response equipment, and sufficient tests to assure that these measures are working. In addition, NRC has established employment suitability and qualifications criteria for security guards, and training requirements in 100 areas of specific knowledge, skills, and abilities dealing with nuclear security. Licensees are required to submit a contingency plan which spells out what a licensee will do in the event of threats, thefts, or radiological sabotage.

To combat radiological sabotage at a nuclear powerplant, a typical protection system is designed to prevent access of unauthorized persons to areas where they could cause a serious release of radiation. Such areas are designated "vital areas"[6] and are protected by at least two concentric circles of barriers and access controls. The outer circle is called the "protected area" and the inner circle is called the "vital area." Individuals entering a powerplant at the protected area entry point are searched for contraband (weapons, explosives, sabotage tools) by electronic equipment and sometimes are given a pat-down search. The protected area is usually monitored by closed circuit television, security guards in bullet-proof towers or patrolling guards to detect attempts at entry through other than designated entry points. The protected area barrier is usually a chain-link fence topped with barbed wire and equipped with electronic intrusion alarms.

Vital areas are usually compartmentalized within the protected area. They are sometimes enclosed with concrete walls and metal doors. In order to enter a vital area, an individual must first be authorized access by licensee management and receive appropriate credentials. Entry into a vital area is through controlled access points typically equipped with electronic card readers. Vital areas are locked and equipped with alarms that are monitored by two alarm stations manned by the guard force. The alarm stations are equipped with two separate means of communications with local law enforcement authorities.

The guard force at a typical reactor site is armed with handguns and shotguns and is trained in many aspects of nuclear security. Guard forces maintain vigilance over both vital areas and the protected area. They are also augmented by local law enforcement authorities.

HISTORY OF SECURITY EVENTS SHOWS CONCERN FOR INSIDE THREATS

NRC's Safeguards Summary Event List published in February 1983, shows that from 1976 through June 1982, there have been 510 security events at nuclear powerplants. NRC classifies these events as related to bomb threats, intrusion, drug and alcohol, lost and/or allegedly stolen material, vandalism, arson, firearms, radiological sabotage, and miscellaneous.

---

[6]Vital areas contain essential safety-related equipment, systems, devices, or materials whose failure, destruction, or release could directly or indirectly endanger the public health and safety by exposure to radiation.

Three hundred and forty six (68 percent) of these events were bomb threats and only 3 of these were cases where an actual bomb device was found. A breakdown of the 510 security events by year is shown below.

Number of Security Events at Nuclear Powerplants

Category	Number of events by year							
	1976	1977	1978	1979	1980	1981	1982 (note a)	Total
Bomb threat related	52	25	29	92	71	46	31	346
Intrusion	10	2	5	3	14	2	1	37
Drug/alcohol related	0	2	0	1	5	14	13	35
Vandalism	0	0	2	6	8	10	5	31
Firearms	1	2	2	5	4	4	6	24
Arson	0	0	1	0	2	2	2	7
Lost/Stolen	0	0	0	0	3	0	0	3
Misc.(note b)	8	0	2	6	2	7	2	27
Radiological Sabotage	0	0	0	0	0	0	0	0
Totals	71	31	41	113	109	85	60	510

a/Only for first 6 months of 1982.

b/Miscellaneous events are those which NRC says hold some interest to security but which do not fit into any of the previously described categories. For example, a contractor employee who had access to vital areas was arrested by the military police because he was absent without leave from military service.

Source: Safeguards Summary Event List, NUREG-0525, Rev. 6, published February, 1983 and discussions with NRC officials.

NRC records show that there has never been a successful act of radiological sabotage at a nuclear powerplant; however, there were 11 events in the past 3 years (1 in 1980, 4 in 1981, and 6 in 1982) that NRC says may have involved deliberate acts directed against plant equipment in vital areas. NRC considered only 1 of these 11 as serious enough to be reported to the Congress as an abnormal occurrence.[7] (See appendix II for details on this incident). All of the 11 events were classified as vandalism and were apparently committed by plant employees, thus demonstrating that serious sabotage attempts can occur and that plants are to some extent vulnerable to the insider threat.

The 11 incidents of vandalism above include destructive acts against safety-related equipment such as

--cutting electrical cables to safety-related equipment,

--closing water valves to the plants' emergency safety system while the plant was operating, and

--tampering with the diesel generator which would be used in case of power failure.

NRC believes that the individuals committing these acts were disgruntled employees or employees trying to take reprisals during labor contract disputes. For example, four incidents of vandalism occurred in 1982 at one powerplant during a period of labor contract disputes.

An analysis of recent security events shows a trend towards an increase in drug and alcohol-related events. In 1979, there was only one reported event of this kind, while in 1981 there were 14 reported events, and 13 in the first 6 months of 1982. In one such event in 1981, five security personnel resigned and 13 were fired for using marijuana offsite or reporting to work under its influence. In another event at a plant under construction, a quality assurance weld inspector was fired for using drugs. After a reinspection of 187 welds which this employee had inspected, it was determined that some of them were defective.

NRC sent an information notice on May 4, 1983 to nuclear powerplant licensees concerning their response to destructive

---

[7]An abnormal occurrence is an unscheduled incident or event at an NRC regulated activity which NRC determines is or could be a major reduction in the degree of protection of the public health and safety. NRC is required by law to report these incidents and events to the Congress.

acts by insiders against plant equipment. The purpose of this notice was to inform the licensees of recent insider events and to encourage licensees to review their operating procedures for responding to them. The notice demonstrates that good coordination between safety and security is needed to mitigate potential safety consequences.

Very few serious security events have involved outsiders, possibly because NRC and licensees have taken many steps in minimizing the outsider threat. Instead, a review shows that the most serious events have been caused by plant employees. Since employees have access to the plant site, we recognize that no security system can guarantee that there will never be a successful act of radiological sabotage. Therefore, NRC should require sufficient measures to minimize the insider threat.

OPPORTUNITIES EXIST FOR MINIMIZING THE INSIDER THREAT

NRC's security regulations require licensees to protect against the insider threat. That means that any employee, be it the plant manager, head of the security force, or a janitor, represents a potential security danger. Plant employees are the most knowledgeable about the location of vital equipment, how it works, and routine operations. Therefore, they could be the most serious source of sabotage because they know the plant's lay-out and have relatively easy access within it. Despite the vulnerability of the plant to insiders and the NRC requirement to protect against them, NRC does not require personnel screening of employees (except for members of the guard force).

The prevailing method of protecting vital equipment at nuclear powerplants is by compartmentalization of that equipment in locked areas of the plant. In an internal memorandum dated January 12, 1982, an NRC official said that "access control measures were never intended to be effective against the insider, and were to be replaced or supplemented with other assurances of personnel integrity." This statement points out the need for a means to ensure that plant employees are reliable and trustworthy.

Magnetic key cards are the primary method that nuclear powerplants use for controlling access to vital areas. The key cards are inserted in a computerized card reader which identifies the individuals, determines whether they have authorized access to the particular area, and if so, it unlocks the door. The system records all individuals who have entered an area, which allows the security organization to identify who has been in a given area. The system also serves as a deterrent for outsiders wanting to sabotage vital equipment.

The insider, however, can circumvent the system. If someone were standing near a person who had been allowed access by the key card system, he could follow immediately behind this person without inserting a key card, a practice commonly called "tailgating." This, combined with the fact that most of the serious security events at nuclear powerplants have been committed by insiders, warrants NRC doing more to minimize the insider threat.

There is strong support among licensees for personnel screening programs that include background investigations, psychological testing, and behavioral observation to assess the reliability and trustworthiness of their employees. Many licensees have some type of background screening program, and some licensees perform psychological testing. However, both the nuclear industry and NRC have identified a lack of uniformity among the licensees' screening programs for plant employees. To correct this problem, NRC's Office of Nuclear Materials Safety and Safeguards has developed the proposed access authorization rule which should promote a uniform screening program and assess the integrity of plant employees.

The proposed access authorization rule would require all licensees to have a screening program that would gather specific information on plant employees to reduce the possibility of malevolent acts endangering the public health and safety. The screening program would include background investigations and continual behavioral observation. Background investigations are designed to determine the individual's trustworthiness through inquiries into his past history (i.e., past employment, education, character, and military and criminal history). Continual behavioral observation is designed to provide increased assurance that personnel remain trustworthy and reliable.

We believe that measures to ensure an employee's trustworthiness represent opportunities for NRC to minimize the insider threat. The proposed access authorization rule appears adequate for upgrading the trustworthiness of plant employees.

IMPLEMENTATION OF PHYSICAL SECURITY SYSTEMS HAS CAUSED POTENTIAL SAFETY PROBLEMS

In addition to the continued problem of dealing with insiders, some licensees and NRC officials expressed concern about the implementation of physical security systems and its effect on plant safety. Security measures by their restrictive nature can interfere with plant operations and safety, if they are not properly implemented. When security restricts plant employees

from promptly responding to emergency situations or situations that could lead to an emergency, plant safety and public health and safety are compromised. Therefore, it is essential that proper attention and coordination be given to the potential conflict between security and safety.

One plant manager we spoke with felt that security could compromise plant safety. He said he did not want his plant operators worrying about punching in and out of doors during an emergency. He provided the following illustration. The control room is a vital area, and plant operators have to insert their key cards to enter it. Once the operator has entered, the computer access control system knows that the operator is there and will not allow him access to another vital area until he punches out. The manager said that if an emergency occurs and the operator leaves the control room to search for equipment elsewhere but forgets to punch out, he cannot gain access to another vital area, because the computer thinks he is still in the control room. Neither will his card let him back in the control room because, as far as the computer knows, he is still there. This wastes critical time and slows response.

In March 1982, an NRC regional office established a task force to review the security and safety programs at a particular nuclear powerplant. The objective of this task force was to determine whether security measures in effect at this plant could inhibit the ability of operational or health physicist personnel to move about the plant in a timely manner in response to emergency situations. This study was initiated because NRC inspectors in this regional office felt that there may be a common problem at nuclear powerplants where the safety of these plants was being compromised by security requirements. They also indicated that NRC had not evaluated the effect of security requirements on plant safety.

The regional task force identified several problems with the NRC rules and regulations. The problems included: (1) the rules and regulations do not address how security should function in an operational emergency or prompt response situations when a potential hazard to the public health and safety exists; (2) the generality of physical security regulations has led to inconsistent interpretations by license reviewers at NRC headquarters; (3) there is no statement in the physical security regulations which requires licensees' security plans to evaluate and describe the impact of security on prompt response to emergency operations; (4) there are no NRC inspections to assure safety and emergency response actions are not inhibited by the security program; (5) the lack of an NRC-sponsored vital area

analysis and an anticipated rule change regarding compartmentalization have resulted in variations in NRC headquarters' licensing policies and confusion on the part of the licensees as to vital area design requirements; and (6) NRC's regulations do not require that security guards be trained to interrelate with operational emergencies or prompt response situations.

NRC headquarters was informed of the findings of the regional task force study and was advised that the situation may prevail throughout the industry. On August 16, 1982, the Chairman, NRC directed the staff to review NRC's physical security requirements with particular emphasis on whether security procedures were detracting from plant safety. The Executive Director for Operations established a Safety/Safeguards Review Committee and the Committee issued a report on February 28, 1983. The Committee's report did not identify specific safety problems caused by security requirements, although it reported that the potential does exist for security procedures to jeopardize plant safety. The Review Committee attributed this potential to site-specific implementing procedures rather than to NRC regulations.

The Committee also noted that inadequate coordination during the implementation of security plans, operating plans, and emergency preparedness plans was causing potential interface problems. The Committee pointed out that NRC did not require licensees to assure that these plans were compatible with each other or for them to assess the impact of security procedures on plant safety.

The Committee recommended that the following requirements be incorporated in NRC's security regulations:

--Require that licensees review security plans, contingency plans, and procedures to evaluate their potential impact on plant and personnel safety;

--Require licensees to provide reasonable assurance of prompt operator access to vital areas and equipment;

--Incorporate provisions for pre-employment psychological testing;

--Describe the extent to which routine security practices may be relaxed during abnormal and emergency situations; and

--Maintain present requirements for electronic search of all personnel entering protected areas.

The Committee also recommended among other things that (1) all power reactor licensees be informed of NRC's concern about the potential impact of security requirements on operational safety; (2) regulatory effectiveness reviews of the safety/security interface be conducted for newly licensed plants; (3) the NRC staff assure that licensees' security contingency plans are consistent with emergency plans; and (4) NRC inspection procedures ascertain whether security practices significantly impede plant employees during emergency situations.

ABNORMAL OCCURRENCE

On June 5, 1981, during a routine operator tour at a nuclear powerplant, the valves to three Auxiliary Feedwater Pumps were found unchained and unlocked, a violation of the licensee's technical specification requirements. The valves, however, had not been tampered with. On the following day, a manual valve was found shut in the High Head Safety Injection Pumps' system during a routine operator tour and was immediately reopened. The chains and locks that normally secured this valve in the open position and those that secured the Auxiliary Feedwater Pumps' suction valves were not found. Although the event did not harm the health of the public or licensee personnel, it did seriously compromise essential safety-related equipment designed to mitigate the consequences of a major occurrence such as a loss of coolant accident.

NRC reported the incident to the Congress as an abnormal occurrence. The licensee, NRC, and FBI investigated the incident and determined that the intent of the probable perpetrator was to harass or embarrass the licensee rather than to commit radiological sabotage. On June 9, 1981, the NRC issued an immediate action letter confirming the licensee's commitment to strengthen controls over and surveillance of essential safety-related equipment. Based upon the results of an on-site assessment conducted in August 1981, the NRC staff has approved a partial relaxation of these stringent interim commitments.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our review was to follow up on recommendations in our 1977 report and determine whether or not physical security at nuclear powerplants has improved since that time. Our review focused on the actions taken by NRC to implement recommendations in our 1977 report and actions taken by licensees in response to NRC requirements.

We conducted our work primarily at NRC headquarters in Washington, D.C., and at three of its regional offices in King of Prussia, Pennsylvania; Glen Ellyn, Illinois; and Walnut Creek, California. We interviewed NRC officials responsible for carrying out the physical security program at both NRC headquarters and the regional offices. We also contacted officials at the Federal Bureau of Investigation, Department of Justice to discuss the feasibility of their providing licensees with national criminal history information about plant employees.

To determine whether or not physical security at nuclear powerplants has improved, we visited 3 nuclear powerplants to observe the security systems installed. At two plants, we accompanied NRC security inspectors on unannounced inspections which lasted 1 week each. At the third plant, we were given a tour of the plant to observe the security systems in place and the interaction between the guard force and plant employees. During one of the inspection visits, we accompanied the NRC inspector on a review at night to see how well the plant was guarded at that time and whether the licensee met NRC's lighting requirements. These requirements specify that all outside areas within the protected area be sufficiently illuminated. Our visits allowed us also to observe how NRC conducted security inspections.

We interviewed the NRC resident inspectors at the plants and licensee personnel to get information on how well the security inspections are conducted and how plant employees interacted with the security systems. We attended a licensee class designed to train its management personnel in detecting plant employees who may be abusing drugs or alcohol or have personal problems that could affect the safe performance of their jobs. This class was conducted by a Drug Enforcement Administration agent and a member from the local Sheriff's Department. We also met with a local Deputy Sheriff who is responsible for assisting the plant's guard force in cases of local disturbances or acts of sabotage.

During the visits to the powerplants, we interviewed members of the guard forces and the licensee's plant management and operational personnel to determine the interaction between

plant safety and security. We observed how offsite vehicles are searched and guarded while on the plant grounds and how individuals are searched before entering or leaving the plant. While at one plant, we observed along with an NRC inspector a simulated emergency drill in which it was hypothesized that a bomb had been placed somewhere within the plant.

To determine the types of security events that have occurred at nuclear powerplants, we reviewed NRC records and documentation at NRC headquarters. We also interviewed officials and reviewed records at NRC headquarters pertaining to future initiatives by NRC to address personnel screening of plant employees and the potential conflict between safety and security. We attended a physical security coordinating group meeting which had security representatives from over 30 utilities operating nuclear powerplants. At this meeting we heard their concerns regarding NRC's physical security requirements, and we also talked with an official from the Edison Electric Institute to discuss personnel screening of plant employees.

Although we did not obtain official agency comments on this report, we did provide copies of this report to NRC program officials for their review and comment. They said the report contained no factual errors and in their opinion the statements and findings contained therein were representative of NRC's physical security program. With that exception, we performed our work in accordance with generally accepted government audit standards.

(301592)

25800

AN EQUAL OPPORTUNITY EMPLOYER

UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE,$300

POSTAGE AND FEES PAID
U. S. GENERAL ACCOUNTING OFFICE

THIRD CLASS