D.CUMENT RESUME

01908 - [A1052052]

Security at Nuclear Powerplants, at Best, Inadequate. EMD-77-32; B-127945. April 7, 1977. 25 pp.

Report to the Congress; by Robert F. Keller, Acting Comptroller General.

Issue Area: Energy (1600).
Contact: Energy and Minerals Div.
Budget Function: Natural Resources, Environment, and Energy: Energy (305).
Organization Concerned: Nuclear Regulatory Commission.
Congressional Relevance: Congress.
Authority: Energy Reorganization Act of 1974 (42 U.S.C. 5876).

Six nuclear powerplants were visited to observe security systems and evaluate their effectiveness. Findings/Conclusions: The Nuclear Regulatory Commission (NRC), which is responsible for assuring security from sabotage, had not operated decisively. Security systems at all plants visited could be inadequate to withstand sabotage attempts. NRC's failure to define the level of threat and to establish specific requirements have allowed inconsistencies in security systems from plant to plant. Regulations proposed in 1974 would improve security, but as their implementation will take time, precautionary measures must be taken for plants now operating. Recommendations: The Chairman of the NRC should: (1) establish criteria for judging acceptability of alternative protective systems; (2) establish and implement improved inspection procedures; (3) upgrade guard forces; and (4) increase interim protection at operating plants. (Author/HTW)

REPORT TO THE CONGRESS

BY THE COMPTROLLER GENERAL OF THE UNITED STATES

Security At Nuclear Powerplants--At Best, Inadequate

Nuclear Regulatory Commission

The Nuclear Regulatory Commission is responsible for assuring that commercial nuclear powerplants have adequate security systems to protect against sabotage. Successful sabotage could present a significant hazard.

The Commission's failure to define the level of threat to protect against and to establish specific requirements have allowed inconsistencies in security systems from plant to plant. GAO and the Commission believe the resulting array of security systems is inadequate. Moreover, the guard forces at these powerplants were generally ineffective and inefficient.

The implementation of recently adopted security regulations should improve nuclear powerplant security.

EMD-77-32

APRIL 7, 1977

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-127945

To the President of the Senate and the
Speaker of the House of Representatives

This report discusses the Nuclear Regulatory Commission's approval and inspection of physical security at nuclear powerplants.

This review was conducted as a part of our evaluation of the effectiveness of the Commission's regulatory activities, as required by the Energy Reorganization Act of 1974 (42 U.S.C. 5876).

We are sending a copy of this report to the Chairman, Nuclear Regulatory Commission.

Sincerely yours,

ACTING Comptroller General
of the United States

COMPTROLLER GENERAL'S
REPORT TO THE CONGRESS

SECURITY AT NUCLEAR POWERPLANTS--AT BEST, INADEQUATE
Nuclear Regulatory Commission

D I G E S T

Nuclear powerplants, in the highly unlikely event of a serious accident, could present a very significant hazard. The consequences of a successful sabotage could be similar--perhaps identical--to those resulting from a serious accident. (See p. 1.)

The Nuclear Regulatory Commission is responsible for assuring that commercial nuclear powerplants have adequate security systems to protect against sabotage. To gain firsthand knowledge of the adequacy of security systems, GAO went to six nuclear powerplants and found (1) vast differences in the degree of protection at these powerplants and (2) shortcomings in guard forces at the plants generally reduced their effectiveness. (See p. 3.)

In discussions of security and sabotage at powerplants, questions on the probability or likelihood of sabotage attempts are often raised. This review was not aimed at answering these questions. Instead, it focused on the vulnerability of powerplants to sabotage and the effectiveness of the Commission's system for making sure that powerplants would be able to withstand a sabotage attempt--regardless of its likelihood. The answer is that the Commission has not operated 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 by threats that are now considered minimum by the Commission. (See p. 17.)

One site GAO visited was protected by

--magnetic alarms on area gates which alarm the guard house if they are disturbed,

--an infrared alarm system along the perimeter of the plant which alarms the guard house if any of the beams are broken,

--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 monitors and records the opening and closing of the doors, and

EMD-77-32

--an attack-resistant guard house with bullet-resistant glass, steel plated ceilings and dual electrical systems.

By contrast, at another site, there were

--no sensitized fences or gates,

--no infrared alarm system,

--no closed circuit television system, and

--a guard house which was not attack resistant.

The primary security device at this latter site was an 8-foot fence topped with barbed wire. (See pp. 3 and 4.)

Regarding the guard forces at these sites, GAO found (1) recruits were given as little as 4 hours training before they were used as guards, (2) annual turnover rates were as high as 48 percent, and (3) the guards' performance was poor in several drills run during GAO's visits. (See pp. 7 and 8.)

Studies done for the Commission, as well as a special inspection the Commission made in 1976, support GAO's views on the inadequacy of security and security guards at nuclear powerplants. In fact, these studies conclude that security at nuclear powerplants could not counter sabotage forces of several individuals that were armed and had knowledge of the plant. Gaining this knowledge is easier than one might imagine. (See pp. 4 to 11.)

The primary cause for the current inadequacies in security has been the Commission's failure to define minimum threat levels upon which utilities could build their security systems. In the absence of such definition, utilities were given great latitude in establishing the security requirements in which they would abide. The inconsistencies that now exist from plant to plant in security systems resulted.

These inconsistencies also result in inequitable dealings with utilities. This is illustrated by the fact that a utility has been cited by the Commission--which can lead to a fine--because one of its security cameras was not working, while at the same time, many powerplants are not required to be equipped with cameras. (See pp. 13 and 14.)

Regulations that call for better security at powerplants and that specify, for the first time, the minimum threat security systems should be able to counter have been under consideration since November 1974--an inexcusably long time. (See p. 13.)

The environment in which the Commission inspectors have operated in the last several years has not been conducive to quality inspections. Specifically, (1) knowing that major differences are permitted in security systems at powerplants and (2) believing that requirements to correct the situation were imminent, has frustrated, confused, and irritated the inspectors. Since inspection efforts are unable to correct the deficiencies in the requirements, security systems remain inadequate. (See p. 17.)

The adoption of the Commission's pending requirements should lead to better security at powerplants. Implementing these requirements will take time, however, which raises the problem of those powerplants--now operating or about to operate--that are vulnerable to minimum threats. GAO believes that interim precautionary measures should be taken. (See p. 18.)

These measures, as well as others GAO believes should be taken, are contained in the following recommendations to the Commission Chairman. The Chairman, Nuclear Regulatory Commission, should:

--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.

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

--Take immediate action to increase interim protection at all operating nuclear powerplants. Such action should include (1) promptly alerting plant management of the serious deficiencies in security systems at existing powerplants, (2) specifying interim measures that powerplant management can take to strengthen security in line with the proposed regulations, (3) improving local law enforcement coordination, and (4) increasing the number of guards.

AGENCY COMMENTS AND RECENT ACTIONS

On February 16, 1977, GAO briefed the Nuclear Regulatory Commission, at its request, on GAO's concerns regarding powerplant security. The Commission solicited GAO's views because it was planning to issue revised security regulations. In fact, an internal memorandum dated February 11, 1977, made the Commission's approval of the proposed regulations contingent upon the GAO briefing. Subsequently, the proposed regulations were published in the Federal Register on February 24, 1977, and became effective on March 28, 1977.

The Nuclear Regulatory Commission agreed with the thrust of GAO's report but disagreed with the recommendation concerning the need to take immediate action to increase interim protection at all operating nuclear powerplants. The Commission stated in a letter to GAO that it considered the publication of the new security regulation which requires the licensees to take certain security actions by May 25, 1977, to be an appropriate interim action. The actions taken to date to improve powerplant security are a step in the right direction.

Nevertheless, the licensees are permitted by the regulations almost 1-1/2 years to comply with several important provisions involving construction or installation of equipment, such as

--detection of penetration or attempts to penetrate the protected area;

--bullet-resistant control room and guardhouses;

--equipment for detecting firearms, explosives, and incendiary devices;

--positive control of all points of personnel and vehicle access into vital areas;

--establishment of microwave or radio communications, in addition to conventional telephone, with local law enforcement authorities; and

--closed circuit television or other means of observing the protected area barriers.

Because of the inadequacies in security systems at nuclear powerplants and because powerplants may have until August 1978 to implement the above provisions, as well as others, GAO believes that the Commission should take immediate steps, as outlined in the report, to increase the interim protection at all operating nuclear powerplants.

C O N T E N T S

		Page
DIGEST		i
CHAPTER		
1	INTRODUCTION	1
2	HOW GOOD IS SECURITY AT NUCLEAR POWERPLANTS?	3
	Quality of security systems	3
	Guards at nuclear powerplants	7
3	WHY HAS THE NRC PROGRAM FOR SECURITY AT NUCLEAR POWERPLANTS FAILED?	12
	Requirements for security	12
	Inspecting security at powerplants	14
4	CONCLUSIONS, OBSERVATIONS, AND RECOMMENDATIONS	17
	Recommendations	18
	Agency comments and recent actions	19
5	SCOPE OF REVIEW	21
APPENDIX		
I	Letter dated March 17, 1977, from the Executive Director for Operations, Nuclear Regulatory Commission	22
II	Principal officials responsible for administering activities discussed in this report	25

ABBREVIATIONS

AEC	Atomic Energy Commission
GAO	General Accounting Office
NRC	Nuclear Regulatory Commission

CHAPTER 1

INTRODUCTION

It now takes about 10 years and a billion dollars to plan, design, and build a nuclear powerplant. Many safety features and systems are built into the plant to protect it, the persons that will operate it, and the public from accidents. Because machines and systems--however carefully designed and built--fail, nuclear powerplants are equipped with backup and redundant systems. The possibility of enough of these systems failing and a serious accident occurring is extremely low. But the consequences of the most serious accident at an operating powerplant would be disastrous. According to a study known as the Rasmussen report, 1/ the consequences of the most serious accident would be 3,300 early fatalities, 1,500 latent cancer deaths per year for 10 to 40 years, and $14 billion of property damage.

Safeguarding nuclear powerplants from sabotage is very important because the consequences of a successful sabotage attempt could be similar--perhaps identical--to those of the most serious nuclear accident. In 1968 the Atomic Energy Commission funded an evaluation of the potential hazard of sabotage to nuclear powerplants. This evaluation reviewed the history of industrial sabotage and examined the motivation and extent of knowledge likely to be possessed by different types of saboteurs. The study concluded that, although sabotage with serious consequences to the public was theoretically possible, the probability was sufficiently low so that no undue risk to the health and safety of the public existed.

Several aspects relating to sabotage of nuclear powerplants have changed since the 1968 evaluation. Public information on, public knowledge of, and public opposition to the operation of nuclear powerplants have increased. Also, incidents of sabotage have increased in number and sophistication, and saboteurs have been attacking a greater variety of more complex targets. In light of these changes, the Federal Government--through the Atomic Energy Commission (AEC) and now the Nuclear Regulatory Commission (NRC)--has been

---

1/ Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, WASH-1400 (NUREG-75/014), October 1975.

increasing its efforts to assure that commercial nuclear powerplants are secure from sabotage.

The history of sabotage threats and attempts against nuclear powerplants in this country does not present any clear indication of whether the problem has been exaggerated or understated. On one hand, a serious sabotage attempt has never occurred or, at least, has never progressed far enough to present any danger to operating a powerplant in this country. On the other hand, there have been a rather large number of threats made against powerplants. From January 1975 to September 30, 1976, 62 incidents, involving bomb threats, extortion attempts, and actual security breaches, occurred at commercial nuclear powerplants. Most of these incidents involved unidentified callers who made vague threats of bombs located on powerplant property. Others, however, seemed more serious. In one incident, an individual was arrested for attempting to illegally obtain explosives to use in sabotaging a nuclear powerplant.

Nuclear powerplants must be licensed by NRC before they can be constructed and then again before they begin operating. As part of the application for an operating license, NRC requires the utility to submit a security plan describing how it will protect the powerplant from sabotage. NRC is then responsible for reviewing and approving the plan and, once the plant begins to operate, inspecting plant security to assure that the utility is complying with the approved plan.

This report is our evaluation of the NRC program for assuring powerplant security.

CHAPTER 2

HOW GOOD IS SECURITY AT NUCLEAR POWERPLANTS?

To observe firsthand the security systems at commercial powerplants, we accompanied NRC inspectors on their inspections of six nuclear powerplant sites. Our major observations on the security at these sites concerned the (1) vast differences in the degree of protection provided by the security systems and (2) shortcomings in the guard forces at the powerplants. NRC has funded studies and taken other actions which resulted in conclusions similar to ours. NRC has proposed some corrective actions which will improve security systems. Such actions may take as long as 1-1/2 years to fully implement. (See pp. 17 and 18.)

QUALITY OF SECURITY SYSTEMS

The six powerplant sites we visited were protected by security systems of vastly different qualities. For example, one site was protected by

--magnetic alarms on area gates which alarm the guard house if they are disturbed,

--an infrared alarm system along the perimeter of the plant which alarms the guard house if any of the beams are broken,

--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 monitors and records the opening and closing of the doors, and

--an attack-resistant guard house with bullet-resistant glass, steel-plated ceilings, and dual electrical systems.

The security officer for this powerplant worked on security matters full time. He was convinced that good security was necessary and felt that he had been able to convince management of this necessity.

In contrast, the primary security device at another site was an 8-foot fence topped with barbed wire. This plant did not have

--alarmed gates or fences,

--infrared alarm systems,

--closed circuit television,

--door tracking systems, or

--attack-resistant guard houses.

The security officer at this plant devoted only part of his time to security operations.

The quality of security at the other four sites was somewhere in between the above two examples. At all six sites, we were able to identify deficiencies in the security systems which we believed could permit a takeover of the plant and the security system. Moreover, a special NRC inspection and several studies done for NRC support our views.

Special inspections

In February 1976, NRC began to make special inspections of all operating powerplants. These inspections were begun because of the concern and publicity that was generated by an internal NRC memorandum which discussed security and safeguards at nuclear facilities. This memorandum said that while definitions of minimum threat were being formulated, an external force of several persons coupled with one insider should be considered as the minimum threat level to guard against. If this minimum threat could not be countered, then the security system must be presumed inadequate.

To make these special inspections, NRC inspectors visited all of the operating powerplants in the country to identify the changes that would be necessary to upgrade the security systems to meet a minimum threat of several "outsiders" and one "insider."

The inspectors found weaknesses at all 43 sites, but NRC headquarters decided to select only the "worst" sites for corrective action. Nine sites having about 80 specific security weaknesses were selected. NRC headquarters formed a committee to determine which of the 80 security weaknesses should be corrected by the utilities. According to members of this committee, they selected about 50 items which were both significant and easily correctable. NRC later made followup inspections to make sure these weaknesses were corrected.

We have two observations on the special inspections. First, although NRC singled out only 9 sites, NRC officials told us that perhaps all 43 sites could not meet the minimum threat level. Secondly, at the time the followup inspections were made and probably even today, many significant security deficiencies existed both at the 9 sites where some corrections were made and at the remaining 34 sites. These deficiencies include unalarmed protected areas, lack of guard house physical protection, and no coordination with local law enforcement agencies.

Studies done for NRC

The Sandia study

Early in 1974, Sandia Laboratories was given a Federal contract to, among other things,

--evaluate the susceptibility of nuclear plants to sabotage for a broad range of threats and

--determine the consequences of successful sabotage.

The study was made in three parts at a total cost of $830,000. Reports on the first two have been issued, and a report on the third part has been drafted. All three reports have been classified secret.

The first report discusses sabotage in relation to "pressurized" type reactors, 36 of which are now operating commercially in the United States. The second report discusses sabotage in relation to "boiling water" type reactors, 25 of which are now operating. The draft report on the third part is a summary analysis of possible sabotage on both kinds of reactors.

Sandia concluded that present protection at many commercial powerplants "would be inadequate against a sophisticated sabotage attack." The Sandia report went on to say that:

> "* * * sabotage which might endanger the public could only be carried out by knowledgeable, capable personnel having a high degree of technical competence. Such an attack would require thorough planning in order to mount an effort coordinated to bypass the plant security system and to disable or destroy elements of several plant systems in the multiple plant defenses against a radioactive release."

It is our observation nonetheless that it is easier to gain the required technical information on nuclear powerplants than one might imagine. A lot of information is publicly available which saboteurs could use to gain detailed knowledge of the operation of powerplants in general and even on particular powerplants. Information published by NRC discusses the most severe accidents that could occur and describes in detail the backup or redundant systems needed to prevent these serious accidents. This information, along with detailed drawings of all powerplant structures, equipment and systems (except for the security system) is maintained for public use at a designated library or facility near each commercial nuclear powerplant. At four libraries we visited, no records were kept on the use, dissemination, or reproduction of this information. Also, some plants have visitor information centers which show the basic plant layout and provide telescopic viewing devices which visitors can use to view much of the plant in detail.

Regarding the consequences of a successful sabotage attempt, the Sandia study points out that the consequences produced by a core meltdown due to sabotage could not exceed the largest consequences predicted for the worst accident. (These are the same consequences mentioned on page 1--namely, 3,300 early fatalities, 1,500 latent cancer deaths per year for 10 to 40 years, and $14 billion of property damage.) The Sandia reports point out that it is extremely unlikely (about 30 to 1) that any early fatalities would occur from a successful sabotage attempt. It also points out that there is a 50 percent chance that cancer deaths would increase by no more than 60 cases per year and offsite property damage might not exceed $2.5 billion.

Lawrence Livermore Laboratory study

Lawrence Livermore Laboratory made an analysis of various security force concepts against sabotage for NRC. To make the study, six commercial nuclear powerplants were visited as well as other types of nuclear facilities. The study concluded, in an October 1975 report, that

> "* * * the combination of guard forces and physical security systems presently used at nuclear facilities was found to be unable to counter the three levels of sophisticated threats postulated for this study."

The lowest of these threats was an external force of several armed individuals. The report stated that guard

forces would have to be augmented in numbers, training, and equipment, and that the physical security systems would have to be upgraded to be able to counter the threat.

GUARDS AT NUCLEAR POWERPLANTS

Guards at nuclear powerplants are either employees of the utility (so-called proprietary guards) or employees of a private security firm under contract to the utility.

In our visits to the six powerplant sites, we observed situations and developed information which indicated major weaknesses in the guard forces. Five of the six guard forces were contract services and the sixth was a proprietary force. Most of the guards were recruited through classified ads and referrals. The selection criteria varied, but as a minimum, included a physical examination and educational requirements.

The background investigations required for some guard forces were much more stringent than for others. Some required employment histories, references, and police checks, and one gave applicants psychological tests. Another facility only checked with the person's former employer. The amount of training necessary before a recruit could begin working ranged from 120 hours for two guard forces to 4 hours training for one guard force. All guard forces were required to have both firearms training and general training.

Perhaps the most disturbing information we obtained concerned the annual turnover rate. As the table below shows, three powerplant sites were protected by guard forces that have experienced annual turnover rates of 35 to 48 percent. The information that most of these guards possess about the powerplant and its security system could be valuable to a potential saboteur.

Information on Guard Forces (note a)

Powerplant site	Total guards	Average age	Annual turnover rate (percent)	Salary (per hour)
A	27	38	48	$3.50 to $4.30
B	34	37	41	2.95 to 4.00
C	70	45	35	3.20 to 4.10
D	25	32	4	Not available
E	25	Not available	Not available	Not available
F	21	29	Not available	5.30

a/Information furnished by NRC.

During our visits, the NRC inspectors sometimes tested the guards' knowledge of procedures to be followed in responding to certain situations. In several of these tests, the guards' performance was poor. For example, we accompanied an NRC inspector to one powerplant at night. The inspector asked a guard manning the guard house to aim a closed circuit television camera on a particular spot. The guard tried but was unable to work the system. The inspector opened a door which rang an alarm in the guard house. After waiting several minutes, the guard house was called to find out why no one responded to the alarm. A guard in the guardhouse answered that all of the available guards were too busy.

At yet another site, we asked a guard about the locations of certain critical systems of the plant, including the control room. He told us that the guard force knew nothing about the location of any of these systems because the guards were not allowed inside the powerplant.

NRC study on need for a Federal guard force

The Energy Reorganization Act of 1974, which established NRC, directed it to assess the need for and feasibility of

establishing a security agency within NRC to perform safeguard functions. This requirement had its origin in several earlier studies and in congressional hearings in which questions about the adequacy of safeguards were raised. During these hearings it was suggested that the importance of the public interest involved might call for direct Federal involvement in security forces.

In February 1975, the NRC Commissioners established the broad objectives and scope for this assessment. They called for a conceptual analysis and comparison of a Federal guard force and a totally private force.

For this study, NRC contracted with five private organizations and numerous consultants to supply information at a total cost of about $419,000. Four of the five study reports by these organizations related to security at facilities while the fifth discussed transportation of nuclear materials.

The first study was done by the United States Marshals Service. Based upon research, discussions with private security officials, and visits to three nuclear sites, the report, dated October 1975, noted that guard forces at commercial nuclear facilities had

--weak allegiance,

--high turnover rate,

--poor background checks,

--poor supervision,

--inferior equipment,

--weak legal authority,

--poor rapport with local police,

--poor mobility,

--no uniform standards for physical fitness,

--low public confidence, and

--little training.

The second study was done by the International Research and Technology Corporation. In its report dated July, 1975, it concluded that nine guards would be needed to counter an attempted sabotage by several outside individuals with no

inside help. This conclusion was based on the premise that the facility employed certain protective system equipment. Several of the facilities we visited were protected by this type of equipment but none was required to keep nine guards on at all times.

The third study was done by the International Association of Chiefs of Police, Inc. Its objective was to assess the capability of State and local law enforcement agencies to respond to certain hypothetical attacks and other criminal incidents throughout the United States. The study assessed the response capability of law enforcement agencies at 17 nuclear powerplants and concluded that State and local law enforcement agencies can supply sufficient manpower, but that deployment of manpower would be uncoordinated due to the lack of formal agreements between responding agencies. The study also concluded that most agencies lacked well-trained tactical teams and the necessary equipment (automatic weapons, long guns, body armor, etc.).

The fourth report on guard forces was the Lawrence Livermore Laboratory study we mentioned on page 6. This report concluded that guard forces would have to be augmented in numbers, training, and equipment to be able to counter a threat level of several individuals.

In spite of all the evidence from the four studies that existing guard forces were inadequate, the NRC study concluded in its August 1976 report to the Congress, that:

> "* * * creation of a Federal guard force for maintaining security in the nuclear industry would not result in a higher degree of guard force effectiveness than can be achieved by the use of private guards, properly qualified, trained and certified by NRC."
>
> * * * * *
>
> "* * * can fulfill its responsibilities to assure adequate physical protection of licensed facilities and materials through stringently enforced regulations."

Security guards have limited authority for using firearms

NRC has not clearly defined the authority of private guards for using firearms to protect powerplants. The lack of specific firearm instructions is due, in part, to the local laws which place heavy restrictions on the use of

weapons by private guard forces. For the most part, local laws allow the use of deadly force only in cases of self-defense or in the defense of others. These laws do not allow the use of deadly force to protect property. The rights of guards in this matter are generally no greater than those of private citizens.

The problems associated with the use of private guards has been recognized for several years. For example, an AEC memorandum in March 1974, stated, in part:

> "The Office of General Counsel has researched the point extensively and has taken the position that it will not press licensees to give directions to employees regarding the use of firearms which are inconsistent with State law. * * * In short, the AEC's official position should be to take a soft line regarding the use of firearms. This should turn into a nonissue * * *."

In January 1975, a Committee on Safeguards Policy of the Atomic Industrial Forum, Inc., also envisioned problems with private guards. Accordingly, they told NRC

> "A dominant question relates to the right of guards to use firearms for the protection of property in the absence of a clearly defined threat to life. * * * It is necessary that NRC establish the authority and the circumstances under which a guard should be instructed to discharge firearms at others."

According to NRC's Office of the Executive Legal Director and the Law Enforcement Assistance Administration in the Department of Justice, there are no Federal laws governing the actions of private guards in this regard.

The problems of private guards and the use of firearms is not restricted to powerplants but extends to privately owned facilities that possess quantities of so-called special nuclear material (types of material which can be used to make nuclear weapons). As part of another assignment we are addressing, among other things, problems arising in the use of firearms at different types of nuclear facilities. We expect to issue a report on the subject shortly.

CHAPTER 3

WHY HAS THE NRC PROGRAM FOR SECURITY AT NUCLEAR POWERPLANTS FAILED?

NRC has a two-pronged approach to assuring powerplant security. The first part is to require utilities to prepare plans which describe how the powerplants are to be protected. The second part is to inspect the powerplants to see that the security systems used are in compliance with the security plans.

REQUIREMENTS FOR SECURITY

The first and most important assumption that requirements should be based on is the level and type of threat that powerplants are expected to protect against. That is, how many individuals armed with what weapons and knowledge should the security system be able to successfully counter.

NRC has not made this assumption. Instead, NRC has suggested that utilities consult two documents 1/ which NRC believes provide an adequate basis for a physical security plan. These documents contain general advice on how to detect, deter, and protect a powerplant against intrusion by using armed guard forces, protective barriers, intrusion detection systems, and liaison with local law enforcement agencies. They do not specify any minimum threat level.

Because these documents are general and do not specify a specific threat level, the utilities must exercise a lot of judgment in deciding on the characteristics and performance level of security systems. This decision is based in large part on how much importance the utility attaches to the issue of sabotage. At the powerplant which had a rather extensive security system, the security officer there said he had been able to convince management of the necessity for good security.

1/Regulatory Guide 1.17, "Protection of Nuclear Power Plants Against Industrial Sabotage" and "Industrial Security of Nuclear Power Plants" published by the American National Standards Institute.

NRC, of course, must review and approve these security plans. This approval is made by four individuals with backgrounds in engineering or physics; most are not trained in security. Moreover, there is no documentation supporting the basis for their approval of the security plans. The reviewers are not given any criteria or guidance for determining the acceptability of the plan, nor have they obtained any expertise from outside NRC. Moreover, these reviewers seldom visit the powerplant to see the security system or devices or to note any unique features of the powerplant and its surroundings.

Because of NRC's failure to specify the minimum threat level or to give utilities and the reviewers any other guidance, approved security plans call for protection of vastly different degrees. NRC officials recognize these differences and blame the current general requirements for the situation.

NRC is well aware of the need for improvements to the security requirements. In an October 16, 1974, report to AEC we concluded that (1) utilities needed specific guidance on the level of threat that their security systems must be prepared to handle and (2) performance criteria should be established for security systems. In an October 31, 1974, response, AEC said that our report did not reflect the impact of proposed regulations that were then under consideration.

In November 1974, the proposed regulations for powerplant security were published for public comment. But as of February 1, 1977, they had still not been adopted. NRC told us that internal problems such as reorganizations and higher priority work had caused the delay.

The proposed regulations are an improvement over the current situation because they would set a minimum sabotage threat level. That is, they are intended to require the security necessary to counter a sabotage force of (1) a determined, violent, external assault or attack by stealth of several persons that are well armed and well trained, and one knowledgeable insider and (2) an internal threat by an insider including an employee in any position.

The proposed regulations also are more specific as to the types of security systems that should be provided. However, proposed regulations give the utilities latitude with regard to the security systems that should be installed. The regulations reserve for NRC the right to approve "measures for protection against industrial sabotage other than those required by this section if the applicant or licensee

demonstrates that the overall level of system performance provides protection against industrial sabotage equivalent to that which would be provided by"--the proposed regulations. That is, the utilities may substitute their own security systems for those called for by the new regulations, as long as NRC believes the substitute provides equal security.

With regard to upgrading security guards, the proposed regulations essentially call for guards to be "properly trained and qualified", without specifying how that should be accomplished.

INSPECTING SECURITY AT POWERPLANTS

NRC has five regional offices which inspect many different aspects of commercial nuclear powerplants as they progress from construction through operation. In each office, one or more inspectors are designated to visit at least once each year all of the powerplants in that region to see if the security systems comply with the plans. The requirements the inspectors check against, then, change from powerplant to powerplant. If the utility's security system is not consistent with the approved plan, the inspector can cite the utility for noncompliance, which could lead to a fine. Having different requirements for each powerplant can and has led to inequitable--and even ridiculous--situations. For example, a utility has been cited for noncompliance because cameras in its closed circuit television system were not working. But other utilities don't even have closed circuit television or comparable systems. In another case, a utility was cited by NRC because its alarmed fences were not as sensitive as required by its plan. Yet, other facilities don't have such alarmed fences.

We accompanied inspectors from three NRC regional offices on inspections of security systems at six sites. All of these inspections were unannounced--that is, the utility did not know the inspectors were coming. Following are our analyses of deficiencies in inspection practices we observed during these visits.

Inspections should be unannounced

The unannounced nature of inspections is intended to give the inspectors a chance to observe the utility's security system in its normal state. Such things as locked doors, lighting, number and conduct of guards, and operability of various systems can best be checked when the inspector "surprises" the utility and the security system.

Some inspectors take precautions so that their inspections are, indeed, unannounced. For example, one inspector we accompanied did not make any advance reservations at the motel he stayed in near the powerplant because of the possibility of a motel employee informing the utility of the inspector's expected arrival. Another arrived at the powerplant at night. He began his inspection that night and immediately checked those security items he had found to be deficient on his last visit.

In contrast, another inspector arrived at a powerplant in the afternoon, met with plant management officials, and told them he would be checking the locked and alarmed doors and the perimeter fence--starting the next morning.

Differences in aggressiveness

Some inspectors were very aggressive in dealing with the utility personnel and in checking the security systems. For example, some inspectors, when checking the alarmed fences, shook each fence section to see if the alarm rang as it should. Other inspectors tried picking locks, crawling under or climbing over fences, or crawling under the infrared beams, and opening alarmed doors to check the time it took guards to respond to the alarm. Several inspectors quizzed the plant security force to determine if they understood their mission and the plant's security system.

On the other hand, some inspectors merely determined that a particular device was in place and did nothing to find out whether the device worked at all or whether it worked effectively. For example, on one visit, the inspector simply walked along the fence and observed that the sensitivity device was attached. He tested only 3 of 17 alarmed sections to determine if the device worked.

On another visit, an inspector observed that doors were locked as they should be but did not make even simple tests of the lock's effectiveness. Our auditors were able to pick the locks and open several doors to vital areas of this plant by using a screwdriver or a piece of wire we found on the ground near the door. After witnessing this, the NRC inspector and a security guard agreed that all similarly locked doors could be opened.

The inadequacies of these locks was brought to the attention of NRC headquarters. NRC prepared a directive instructing utilities with similar locks to replace them. This directive was issued March 17, 1977.

Need for inspectors' authority to go beyond security plans

At several powerplants, the NRC inspectors pointed out rather serious weaknesses in security which were not provided for by the security plans for those plants. Because the inspectors are limited to looking for noncompliance with the approved security plans, the inspector was unable to cite the utilities. Instead, he could either discuss the weaknesses with utility officials and encourage them to take corrective action and/or he could communicate the weaknesses to NRC headquarters with the intent of upgrading the security plan. We noted one case where the inspector was successful in getting a utility to correct a weakness. But we noted several cases where the inspector reported weaknesses to the utility and nothing was done. For example, during our site visits in September and October 1976, inspectors observed such weaknesses as guards not responding to an alarm and an unlocked exterior door which permitted unrestricted access to the control room. The inspectors orally reported these weaknesses to the utility. We also noted several instances where inspectors reported weaknesses to NRC headquarters. These weaknesses included a reactor control room that was unalarmed and unlocked. As of February 1977, neither the utilities nor NRC had taken action to correct the above weaknesses.

CHAPTER 4

CONCLUSIONS, OBSERVATIONS, AND RECOMMENDATIONS

In discussions of security and sabotage at powerplants, questions on the probability or likelihood of sabotage attempts are often raised. Our review was not aimed at answering these questions. Instead, we focused on the vulnerability of powerplants to sabotage and the effectiveness of NRC's system for making sure that powerplants would be able to withstand a sabotage attempt--regardless of its likelihood. The answer is that NRC has not operated 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 by threats that are now considered minimum by NRC.

The primary reason for this situation is the failure of NRC, and the AEC before it, to establish the minimum threat levels upon which security systems should be built by the utilities and evaluated by NRC. In the absence of these threats or any compensating guidance, the utilities have been given the latitude to play a major role in establishing the requirements by which they would abide. The vast inconsistencies that now exist from plant to plant resulted.

NRC's inspection program was unable to correct the inadequacies that originated in the security plans and that were extended to actual security at powerplants. In the last several years, the inspectors have had to work in an environment which has not been conducive to quality inspections. Specifically, (1) knowing that differences are permitted in the quality of security systems at powerplants and (2) believing that requirements to correct the situation were imminent, has frustrated, confused, and irritated the inspectors. Nevertheless, methods and procedures need to be implemented which would insure consistency in the aggressiveness and unannounced nature of inspections and encourage the inspectors to go beyond security plans in evaluating security systems.

The proposed regulations, which have been under consideration an inexcusably long time, offer the opportunity for NRC to get its program on the right track. Whether it takes advantage of this opportunity depends, we believe, on how it deals with the following three points.

First, the proposed regulations contain a provision which would permit the utility to substitute security systems completely different from those specified in the regulations

as long as NRC finds the substitute acceptable. This provision would necessitate the reviewers to use discretion and judgment in approving security plans. We believe that their decisions are too important and too far reaching to be made independently and without visiting the powerplant site. Consequently, we believe that the reviewers should visit each powerplant and obtain the comments of the regional inspection office before approving the security plan. Obtaining these comments should lead to greater aggressiveness and a greater sense of responsibility than exists now.

Second, the greatest single shortcoming of powerplant security is the quality of guard forces. Unfortunately, the proposed requirements do not specify any upgrading actions. We believe that NRC must develop, as quickly as possible, methods for making major improvements to guard forces in such areas as turnover rates, use of firearms, and background investigations and must direct the utilities to immediately make such improvements.

Third, inspectors should be authorized and encouraged to go beyond the utilities' plans when looking at security systems and appraise the systems in terms of whether their performance can meet the minimum threat. This would give the NRC program the capability to catch mistakes or oversights in approving the security plan, as well as the ability to evaluate the system in light of changes at the powerplant or in its surroundings. More importantly, it would serve to emphasize to the inspectors the necessity to check the performance and not just the existence of security systems.

The actions discussed above, if implemented, would lead to better security systems. However, their implementation will take time. The problem is what should be done with those powerplants that are about to begin operations or are now operating. Clearly, some powerplants now operating are vulnerable to threats of less than the several outsiders and one insider level NRC considers minimum. Some precautionary measures could be taken immediately. NRC is aware of the "worst" facilities--in terms of security --which are in need of significant improvements immediately.

RECOMMENDATIONS

We recommend that the Chairman of the Nuclear Regulatory Commission:

--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.

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

--Take immediate action to increase interim protection at all operating nuclear powerplants. Such action should include (1) promptly alerting plant management of the serious deficiencies in security systems at existing powerplants, (2) specifying interim measures that powerplant management can take to strengthen security in line with the proposed regulations, (3) improving local law enforcement coordination, and (4) increasing the number of guards.

AGENCY COMMENTS AND RECENT ACTIONS

On February 16, 1977, we briefed NRC, at its request, on our concerns regarding powerplant security. NRC solicited our views because it was planning to issue revised security regulations. In fact, an internal memorandum dated February 11, 1977, made the NRC Commissioners' approval of the proposed regulations contingent upon our briefing. Subsequently, the proposed regulations were published in the Federal Register on February 24, 1977, and became effective on March 28, 1977.

NRC agreed with the thrust of the report, but disagreed with our recommendation concerning the need to take immediate action to increase interim protection at all operating nuclear powerplants. NRC stated in its letter to us that it considered the publication of the new security regulation which requires the licensees to take certain security actions by May 25, 1977,

to be an appropriate interim action. The actions taken to date to improve powerplant security are a step in the right direction.

Nevertheless, the licensees are permitted by the regulations almost 1-1/2 years to comply with several significant provisions involving construction or installation of equipment, such as

--detection of penetration or attempts to penetrate the protected area;

--bullet-resistant control room and guardhouses;

--equipment for detecting firearms, explosives, and incendiary devices;

--positive control of all points of personnel and vehicle access into vital areas;

--establishment of microwave or radio communications, in addition to conventional telephone, with local enforcement authorities; and

--closed circuit television or other means of observing the protected area barriers.

Because of the inadequacies in security systems at nuclear powerplants and because powerplants may have until August 1978 to implement the above provisions, as well as others, we believe that NRC should take immediate steps, as outlined in the report, to increase the interim protection at all operating nuclear powerplants.

CHAPTER 5

SCOPE OF REVIEW

We obtained the information contained in this report by reviewing documents, studies, reports, correspondence, and other records, and by interviewing officials at

--NRC Headquarters, Bethesda, Maryland;

--NRC Region I, Office of Inspection and Enforcement, King of Prussia, Pennsylvania;

--NRC Region II, Office of Inspection and Enforcement, Atlanta, Georgia;

--NRC Region III, Office of Inspection and Enforcement, Glen Ellyn, Illinois; and

--Six nuclear commercial powerplant sites at various locations.

APPENDIX I

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

March 17, 1977

MEMORANDUM FOR: Thomas J. McTiernan, Director
Office of Inspector and Auditor

FROM: Lee V. Gossick
Office of the Executive Director
for Operations

SUBJECT: COMMENTS ON DRAFT GAO REPORT, "SECURITY AT NUCLEAR POWER PLANTS -- AT BEST, INADEQUATE"

Your February 24, 1977, memorandum forwarded for staff review and comment the subject document.

It was stated in the subject report that inconsistencies in the level of protection presently exist among individual security plans. It was also implied that no remedial action was being taken to eliminate these inconsistencies. We were aware of the inconsistencies and, with the publication of the new physical security rule (73.55), have taken significant action not only to eliminate th inconsistencies but also to provide a high level of protection against industrial sabotage at all nuclear power reactors.

This new rule establishes a performance criterion for the physical protection of nuclear power reactors. This criterion can be stated succinctly as requiring "high assurance protection against industrial sabotage by (1) a determined, well-armed, well-trained team of several outsiders assisted by a single insider or (2) a single insider acting alone." In meeting this general requirement the rule states that the onsite physical protection system and security organization shall include, but not necessarily be limited to, the following capabilities:

1) A physical security organization including armed guards to protect the facility against industrial sabotage.

2) At least two barriers to protect vital equipment, illumination of all outdoor areas, isolation zones extending on both sides of the protected area perimeter to permit observation of activities on both sides of that barrier, and a bullet-resistant reactor control room.

Thomas J. McTiernan

3) Search of all individuals, packages, and vehicles prior to entry into the protected area; escort of all but licensee-designated vehicles while in the protected area; a badge system for identification of the level of plant access authorization; escort of visitors while in the protected area; positive access control of all points of personnel and vehicle vital area access.

4) Intrusion alarms that annunciate in a continuously manned central alarm station and at least one other continuously manned station.

5) Continuous communication capability for on-duty guards with each alarm station; telephone and wireless communication between alarm stations and local law enforcement authorities.

6) A nominal force of ten guards and armed, trained personnel immediately available at the plant to fulfill security contingency response requirements, with a minimum of five guards in this response force.

Revised security plans submitted in response to 73.55 are due on May 25, 1977. These will be reviewed onsite by several teams, each led by an individual from Nuclear Reactor Regulation and including personnel from Inspection and Enforcement (IE). During the review, each plan will be evaluated against standard acceptance criteria, thereby increasing uniformity in the levels of protection required.

To supplement this new rule, the Commission has published for comment a clearance rule for screening individuals permitted unescorted access to protected areas. This clearance rule, if adopted, would provide additional assurance against industrial sabotage involving an insider.

There remain three areas in the report about which we believe specific comments are in order.

The first area contains the GAO staff recommendation that "immediate interim action" should be taken and that plants be placed on "alert". We disagree. By publication of 73.55, with its provisions that call for implementation by May 25, 1977 of the above described capabilities except for any requirement involving construction and installation of

APPENDIX I

Thomas J. McTiernan

equipment not already in place, the staff believes that the necessary action has been taken. We have no information from any intelligence or investigative arm of the government of known groups in this country having the combination of motivation, skill, and resources to attack a nuclear power reactor, and physical security upgrading is underway. Therefore, publication of this rule is, in the staff's view, appropriate interim action and results in the appropriate increased awareness of physical security at nuclear power plants.

The second area concerns statements made on page iii and elsewhere in the document which indicate that GAO believes the level of inspection varied from plant to plant. Variations observed by GAO could have arisen from three basic causes: (1) different commitments and levels of details in each licensee's approved security plan; (2) the fact that only portions of the annual inspection are covered during any one visit and the tasks of successive visits are not required to be repeated except to verify corrective action taken by the licensee; and (3) human factors, which we have attempted to minimize by the establishment of standard inspection procedures.

As described above, the program that will be used to review the licensee's amended security plans will solve the problems associated with different commitments and levels of details. The GAO has suggested that changes are appropriate to minimize the other two causes of variation in the level of inspection. We are continuing to review our inspection program and procedures for upgrading as necessary.

The third area concerns the directive relating to inadequacies of locks. GAO points out that the directive has not yet been issued. A circular addressing locks was forwarded on 17 March 1977 to the regional offices for distribution to licensees.

As you know, the staff has met with GAO staff to discuss several specific points of the report. Several changes were discussed. In addition, GAO staff and Division of Security staff have met to discuss areas which caused some classification concern. I understand that changes have been made in the report and that the Division of Security recommends that the report be published as not classified.

Lee V. Gossick
Office of the Executive Director
for Operations

APPENDIX II

PRINCIPAL OFFICIALS RESPONSIBLE FOR ADMINISTERING ACTIVITIES DISCUSSED IN THIS REPORT

	Tenure of office From	To
NUCLEAR REGULATORY COMMISSION		
CHAIRMAN:		
Marcus A. Rowden	Apr. 1976	Present
William A. Anders	Jan. 1973	Apr. 1976
EXECUTIVE DIRECTOR FOR OPERATIONS:		
Lee V. Gossick	Jan. 1975	Present
DIRECTOR OF NUCLEAR REACTOR REGULATION:		
Ben C. Rusche	Apr. 1975	Present
Edson G. Case (acting)	Jan 1975	Apr. 1975
DIRECTOR OF INSPECTION AND ENFORCEMENT:		
Ernst Volgenau	Apr. 1976	Present
John G. Davis (acting)	Jan. 1976	Apr. 1976
Donald F. Knuth	Jan. 1975	Jan. 1976