

EN-037

NEED FOR IMPROVED SECURITY PROGRAMS AT COMMERCIAL NUCLEAR POWER PLANTS 096730

75-0097



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

RESOURCES AND ECONOMIC DEVELOPMENT DIVISION
B-164105

OCT 16 1974



The Honorable Dixy Lee Ray
Chairman, Atomic Energy Commission

Dear Dr. Ray:

We have surveyed the security systems at commercial nuclear powerplants, and have noted issues which warrant your attention.

As you know, security in the nuclear industry has been a matter of considerable public and congressional concern mostly related to safeguards for preventing the theft of special nuclear materials. Some concern has been expressed about security systems at nuclear powerplants. The consensus of opinion is that security throughout the industry needs to be improved.

We made this survey as a follow-on to our recent work on in-plant and transportation protection of special nuclear material. During the survey, we visited nine nuclear powerplants at five sites. We identified those sites for AEC officials. We also visited local law enforcement agencies. We saw the existing security systems and discussed them with licensee and AEC officials. We also discussed with these officials any planned changes in these areas.

AEC's guidance to licensees for security systems at nuclear powerplants does not specifically define the level of sabotage threats that licensees' security systems must be able to handle, and AEC has not clarified the Government's responsibility for protecting nuclear powerplants against sabotage threats beyond the capabilities of licensees' security systems. Studies AEC is funding should provide a basis for determining credible sabotage threats and for developing performance criteria. However, it will be some time before these studies are completed, performance criteria are developed, and revised security requirements are adopted. The actual or prospective increase in the amounts of highly radioactive used fuel stored at nuclear powerplants would seem to warrant establishing interim additional security requirements as soon as possible.

SECURITY SYSTEMS AT COMMERCIAL NUCLEAR POWERPLANTS

AEC regulations effective November 6, 1973, require licensees to prepare physical security plans for their nuclear powerplants and to submit them to AEC for its approval. To help licensees develop their

REF-75-283

096730
102196

BEST DOCUMENT AVAILABLE

plans, AEC issued Regulatory Guide 1.17, "Protection of Nuclear Power Plants Against Industrial Sabotage." The guide endorses the American National Standards Institute Standard N18.17, "Industrial Security for Nuclear Power Plants." As of September 1, 1974, AEC had reviewed and approved the physical security plans for all nuclear powerplants licensed to operate.

Under the AEC guide and the standard, licensees, to detect, deter, and protect against intrusions, are expected to maintain an armed-guard force, install protective barriers, and provide intrusion detection devices. Licensees are also expected to establish liaison and communications with law enforcement agencies to help the licensees protect their plants against acts of industrial sabotage.

At several plants we visited, we noted unlighted protected-area perimeters, unlocked outside doors, lack of intrusion alarms, and unarmed watchmen. Licensees were planning to correct such weaknesses in their security systems to comply with the AEC guidelines for security at nuclear powerplants.

Are commercial nuclear power reactors
vulnerable to sabotage?

Licensee and AEC officials agreed that a security system at a licensed nuclear powerplant could not prevent a takeover for sabotage by a small number--as few, perhaps, as two or three--of armed individuals. Such a takeover, particularly of a nuclear powerplant near a large metropolitan area, could threaten public health and safety, if radioactive materials were released to the environment as a result of successful sabotage.

Various experts disagree on the vulnerability of nuclear powerplants to sabotage. In an attempt to better define this vulnerability, AEC is funding studies, scheduled for completion by June 1975, to determine the

- potential sources of sabotage threats,
- vulnerability of nuclear power reactors to sabotage,
- resources necessary to carry out successful sabotage, and
- potential consequences of sabotage.

According to AEC and licensee officials, the used-fuel storage facility at a nuclear powerplant is more accessible and vulnerable to sabotage than is the reactor core. Such a storage facility generally is an uncovered pool of water near the reactor. The highly radioactive used fuel does not have the same degree of physical protection as that provided to the reactor core by the reactor containment vessel.

The used fuel is stored on site for cooling. After cooling it is packaged and shipped to a commercial fuel-reprocessing plant. Fuel-reprocessing plants have large storage capacities and have been storing used fuel. However, these plants are not expected to be in operation until 1976 or later and their storage areas are rapidly being filled. AEC has recognized this problem and is considering allowing AEC facilities to store used fuel from commercial nuclear powerplants.

The dwindling commercial storage capacity has already resulted in some nuclear powerplants' keeping more used fuel on land than they normally would. This situation increases the potential consequences of successful sabotage of the used-fuel storage facilities at such plants.

Need for improved security requirements

Standard N18.17 states that the security system it outlines is designed to protect against a wide variety of potential threats, including a "small group of discordant individuals." The standard specifically excludes protection against "deliberate assaults by trained para-military groups," stating that such protection is the Government's responsibility.

Licensees have not been given specific guidance on the difference between threats posed by small groups of discordant individuals and those posed by trained paramilitary groups. Therefore the level of threats that licensees' security systems must be able to protect against is unclear.

AEC's review and approval of licensees' proposed security systems are not based on specific performance criteria. Without such criteria there is no way to measure the effectiveness of licensees' total security systems --their onsite security system and assist agencies' response capabilities.

AEC officials told us that there had been no specific coordination with other Federal agencies, such as the Department of Defense and the Federal Bureau of Investigation, to protect against or respond to attacks by paramilitary groups. These officials said that local law enforcement assist agencies would be expected to respond to such attacks. However, AEC guidance to licensees does not provide for making such assist agencies aware that they would be expected to carry out the Government's responsibility to counter attacks by paramilitary groups against commercial nuclear power reactors.

The need to give licensees specific guidance on the level of threats their security systems must be prepared to handle and on the Government agencies which must be contacted for assistance and to provide for evaluating the response capabilities of assist agencies, has been recognized within AEC. During a recent review of an applicant's security system, AEC's

B-164105

Atomic Safety and Licensing Board said that, since the applicant depends on the assist agencies to handle situations beyond the onsite capabilities, their abilities to respond should be tested.

In a later comment on that same security system, AEC's Atomic Safety and Licensing Appeal Board recommended that the AEC Regulatory staff make sure that requirements for security plans "prescribe precisely the 'design basis threat' that the applicant itself must be prepared to meet." The Appeal Board further said that the AEC Regulatory staff should make sure that those requirements specify "the governmental authorities which an applicant must contact for assistance" to counter threats beyond its own capabilities. AEC Regulatory officials told us that these recommendations were advisory and they did not plan to take any specific action on them.

In addition, the need for increased security is being advocated from within AEC. AEC's Advisory Committee on Reactor Safeguards, which independently reviews all applications for construction permits and operating licenses for nuclear power reactors, recently recommended to AEC, as a result of its analysis of a construction permit application, that more attention be given to reactor design features which "prevent or mitigate the consequences of acts of sabotage." Furthermore, an AEC Commissioner recently noted that the use of built-in protective devices, such as incapacitating gas in critical areas of reactors, would help provide greater insurance against sabotage.

CONCLUSIONS

AEC needs to (1) give licensees more specific guidance on the level of threats their security systems must be prepared to handle by clarifying the differences between assaults by small groups of discordant individuals and by paramilitary groups, (2) clarify the Government's responsibility for protecting nuclear powerplants against sabotage by paramilitary groups, and (3) establish performance criteria for licensees' total security systems.

After AEC gives licensees better guidance on what their security systems are expected to protect against and clarifies the Government's responsibility for protecting nuclear powerplants against sabotage by paramilitary groups, licensees will know more precisely what their security systems must be designed to do and AEC will be better able to judge this capability.

The studies AEC is funding should provide a basis for determining credible sabotage threats and for developing performance criteria. However, it will be some time before these studies are completed, performance criteria are developed, and revised security requirements are adopted.