Physical Security of Nuclear Facilities

Herbert Dixon

In the United States, the Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC) are responsible for providing adequate protection to nuclear facilities, materials, and shipments under civilian control Of the two, DOE's task is somewhat more critical, since generally the nuclear materials it handles can more readily be converted into a nuclear weapon, and it is responsible for nuclear weapons prior to their transfer to military custody

A protection system should be able to deter attacks by making the price of entry too high for all but the most dedicated and determined likely adversaries in terms of personnel, equipment, and skills That security mission has several fundamental elements definition of the threat, design of a security philosophy, identification of the systems and processes to be used to deter, detect, and deny access to intruders, and decisions as to the required training and the tactics that will neutralize the threat.

Defining the Threat

The basis of the security system itself is the potential threat The definition of the threat must go well beyond numbers of adversaries to include detailed characteristics, such as method of attack, armaments, and speed of movement Although it is impossible to protect against all threats, the most likely ones need to be planned for

The intelligence agencies disagree to a considerable extent on whether a credible threat exists to nuclear materials facilities, and there has been little intelligence that provides any guidance In the absence of a clearly identifiable threat, both the DOE and the NRC have had to develop what are called design basis threats, within which context they have also prepared generic security standards that serve as guidelines for the design of security systems at specific nuclear facilities The field offices, aided by security staff from the facilities, conduct site-specific threat analyses and are responsible for converting the generic standards into site-specific performance standards for the security system Implementation of the related security system is put out for competitive bid

The lack of a sufficiently detailed definition of the threat and the ambiguity over the interpretation and implementation of the headquarters' guidelines by the field offices have caused the DOE and the NRC many problems in developing their nuclear protection programs A common all-inclusive threat to all sites could be defined by headquarters, yet this step has not been taken Both the threat parameters and related standards have been vague, and as a result they have permitted different interpretations at the field level For that reason, actual security systems have varying capabilities that may or may not be equivalent to what headquarters intended

There is one comprehensive set of standards at the headquarters level the Inspection and Evaluation Section of the DOE recently completed (after some fourteen years) Draft Inspection Standards Documentation, which staff members use to evaluate security systems at nuclear facilities (In fairness to that unit, its status has been so uncertain over the years that it was unable to fulfill these types of fundamental functions in timely fashion) These standards are not policy, however, and hence cannot be used by plant licensees as the basis for requesting funds to adapt their systems to meet the inspection unit's standards Moreover, because there are conflicts between those standards and what has been put in place at the facilities, the inspection standards may engender controversy Finally, the standards appear in eight different volumes; the one on physical protection and operations alone is 400 pages long

In spite of this facility-based approach to designing security systems, there are some aspects of potential threats that seem to be universal Attackers are likely to be highly mobile, skilled in the operation of electronic security systems, and knowledgeable about security force routines These capabilities would apply to any nuclear facility It is interesting to note, then, that current guidelines call on each facility, in conjunction with law enforcement and intelligence agencies, to do a detailed local threat assessment These types of outside threats are similar across facilities and can be better assessed at the national level Local assessments should focus on what they are best suited to address· insider threats

Evaluating the insider threat requires an assessment of the impact of each employee at a facility in terms of the person's authority, access, job, and relationship within the organization and with the security program Positions that present the best opportunity for successful insider threats should be identified and security measures designed to minimize possible problems

Measures include the two-man rule, rotation of personnel, assignment of new work schedules, and perhaps interplant reassignments, along with more detailed checks on personnel background and strict enforcement of "need to know" and "need to be" regulations

Not enough attention has been paid to defining the insider threat Current specifications require the security system to detect an attempt by an insider to bring explosives or weapons into the plant or to remove nuclear materials illegally from the plant Some parts of the security system are designed to detect an attempt to approach certain critical elements of the nuclear process The problem is that these specifications do not adequately define the insider or certain characteristics of a potential threat, such as the range of speeds and time needed for electrical or mechanical detection, or the quantities and types of explosives an insider might have Yet this information is needed to design an effective and complete security system For example, depending on a sensor settling time after being triggered and its sensitivity, an intruder walking at the right speed could pass undetected through an area covered by a single sensor Adequate protection might require two sensors and a television monitor per zone

The outsider threat is even harder to design against Will the intruder use armor-piercing bullets, a shaped charge explosive, or something else? These questions should be addressed, although they can be unending, and a limit will have to be imposed In some cases, a capability will be considered unlikely enough that it will not be addressed or will be put aside for monetary or other reasons A good general basis for a security philosophy is the statement, "The security system must defeat the terrorist who will be armed with automatic weapons, possess explosives, and be highly trained and dedicated "

Once the fundamental threat parameters are established, more precise data can be developed, such as the speed of the intruder, different positions he or she may assume when moving, and minimum height and weight This type of information should be common to all facilities That is, the threat characteristics should not be site specific for the purpose of preparing system technical performance standards When local conditions are used to define a quantitative generic threat further, systems of varying performance capabilities among the facilities will result

Operational requirements and technical specifications should be defined for both the insider threat and some outsider ones The requirements and the specifications should address each segment of the detection and verification subsystems Only then can the security system designer provide the functional requirements to the producers of the hardware and software In addition, some common standard of security will be present at all nuclear facilities

Security Philosophies

The DOE and the NRC follow two basic security philosophies graded security and power block security Both philosophies are predicated on the idea that physical barriers, armed guards, and electronic devices will deter most would-be intruders Should deterrence fail, however, the objective is to provide means of detecting the intruder(s) and to aid the security forces in denying them access to the protected materials

The graded security philosophy is based on the premise that the security system should become more difficult to resist the nearer the intruder gets to the asset being protected Traditionally the first grade of defense has been perimeter fences with barbed wire on top; the second grade is a combination of electronic components to detect attempted intrusions and response forces to intercept the intruders Locks, vaults, steel doors, and concrete walls, along with inside and outside law enforcement personnel, are the last grade This philosophy is akin to DOD's "defense in depth" approach to protecting nuclear weapons storage sites

The power block security philosophy presumes that the intruder will be successful in arriving at the buildings that house the reactors and other power generation equipment Thus although the system includes perimeter security fences, they serve only as a barrier to keep out animals and casual passers-by and are not colocated with electronic detection and surveillance equipment The strategy is to deny attackers entry into the buildings through a circled wagon approach Vehicles and people are controlled by security guards ouside the power block areas, more sophisticated electronic equipment, including detection and verification devices, are found at the power block facilities.

Elements of a Security System

A discussion of the different segments of a security system is useful in understanding how the system as a whole deters, detects, and denies access The discussion also highlights the need for detailed operational requirements, technical specifications, and threat definitions so the system designers can select the best equipment and configurations of components and measures The elements of a security system addressed here are barriers, lighting, exterior sensors, interior sensors, alarm assessment equipment, and command and control devices Examples of some of the equipment standards published by the DOE are used to illustrate their weaknesses

Deterrence

Lighting and physical barriers such as fences, walls, and doors are used to deter and impede access to secure areas The barrier standards for civilian nuclear facilities cover such features as the height of wires and the thickness of doors The specifications yield some but not total uniformity of protection across all facilities Perhaps more important, neither the DOE nor the NRC standards address other important barrier problems, such as protecting against penetration by a high-speed land or aerial vehicle

As a further deterrent, entrance to protected areas by personnel and vehicles is controlled, for example, by steel turnstiles for people, as well as metal detectors and, in some instances, explosive and radiation detectors, and searches for vehicles, using mirrors to check underneath them Television cameras usually track all searches An elaborate system of badges ensures that only authorized people are admitted to a facility. Upon arrival at the actual plant, an individual turns in one badge and gets another that authorizes further specified access In some instances, access is possible only with a specially coded card inserted into an electronic card reader These readers are connected to a computer that can track individuals wherever they go in the facility

Other deterrents are the high visibility of the forces, loud sirens, and armaments When properly configured, these devices and measures can deter most thieves and vandals and protect the outermost perimeter and interior facilities of a nuclear facility against a low-level threat For better preparedness, security forces engage in mock responses to alarms

Detection

Should deterrence fail, the next element in the security system is detection, which relies on exterior sensors, interior sensors, and alarm assessment equipment

If a ground-based intrusion is attempted from outside the facility at other than an entrance, electronic detection sensors and a closed circuit television system at the exterior fence should pick it up There is also a possibility that the guards will detect intruders while still outside the fence, using standard military devices for nightsighting

At present, the only requirement at civilian facilities is for a human detection capability to sight adversaries before they reach the perimeter fence or within sight of a perimeter-viewing closed-circuit television camera When early detection is based on human capabilities, many factors must be considered· artificial and natural light levels, weather conditions, dress of the intruder, and the ability of the intruder to stop the human detector without alerting other security forces or the electronic and video systems The DOE, NRC, and Department of Defense (DOD) have assessed the capabilities and accuracy of humans (and animals) as detectors extensively In all instances, they were found to be poor detectors The probability is therefore very high that an intruder at most civil nuclear facilities would not be detected by a human before reaching the perimeter fence, where there has to be an electronic security system

Exterior Detection Sensors. Most nuclear facilities use two sensors, each directed toward a different phenomenon, at the perimeters A fence detection sensor is usually mounted on the innermost fence A second sensor, which may consist of electric field fences, buried magnetic field metal detectors, buried seismic motion detectors, electric cable, or microwave or infrared beams, is installed between the two fences Because physical and environmental conditions can significantly affect exterior detection systems, their selection and installation are critical, particularly since each site is unique

All types of electric security sensors are subject to false and nuisance alarms, both of which have generally accepted definitions, although they may vary somewhat across agencies In general, a false alarm is system generated, a nuisance alarm is a response to a nonthreatening stimulus To deal with nuisance alarms, the sensitivity is adjusted while still maintaining an acceptable probability of detection. To permit a higher sensitivity setting, some nuclear facilities have integrated a form of combination logic into the system's software Selected sensors must activate in a prescribed sequence and within a preset time frame, or the system will conclude that a nuisance alarm has occurred The software must also allow for activation in reverse sequence and for overlapping zones, so that a person leaving the facility by climbing over the fence may be detected Clearly security of and access to the software and its documentation are critical with this type of system

In the absence of combination logic software, maintenance personnel tend to overadjust fence-mounted sensors, and console operators tend to become conditioned to repeated false alarms Another problem in designing adequate sensor systems is the absence of performance standards The threat must be defined in such terms as minimum weight and speed of the intruder, wind velocities, snow density, rainfall, and grass height Detailed specifications for all security equipment are especially important since each field office can approve substitute equipment Further, the DOE and NRC need to specify three performance probabilities that must be met or exceeded that the sensor will detect anomalies, that the sensor will work, and that the system will indicate what a sensor picks up

Present DOE standards do not address exterior intrusion detection systems, and what standards the DOE and NRC use for system probability are unclear At this time, the exterior (beyond the fence) detection capability at some nuclear facilities, because it relies on humans, does not provide sufficient time for security forces to intercept intruders before they get through the perimeter fences

Other departments of the federal government have developed standards, specifications, and operational requirements for security sensors Unfortunately, there is inadequate sharing of information and R&D efforts For example, the DOD has foliage-penetrating infantry radars that might be applicable to civil nuclear facilities Greater sharing of equipment and other cooperation in security matters would produce greater efficiency and economy

Interior Sensors. Interior sensors are electronic devices that detect unauthorized personnel entering restricted areas such as desks, safes, and rooms Motion sensors such as infrared (passive or active), microwave, or ultrasonic (passive and active) can detect unauthorized personnel Proximity sensors relay an alarm if the protected item is touched In highly sensitive areas, a combination of volumetric detection and proximity sensors with video surveillance is appropriate Here, too, more detailed specifications are necessary, based on a clearly defined threat Without them, uniformity of security across facilities cannot be achieved

Alarm Assessment Capabilities

When a sensor generates an alarm, the cause must be determined Because human assessments are too slow against a fast-moving intruder, electro-optic devices that can view the area in question immediately are necessary Remote-controlled day and night television cameras are a very effective means of verifying alarms and determining the exact nature of the stimulus Each camera covers a particular section of the perimeter, usually 100 meters long

The capabilities of some video systems found at nuclear facilities are limited in some respects One constraint is their inadequate ability to handle multiple alarms in situations where an intruder must be viewed almost instantaneously—perhaps because the number of personnel available to monitor the cameras is insufficient and several cameras therefore have to be viewed through one monitor Although all the cameras tape what they see, this capacity does not help when immediate decisions have to be made

Standards and specifications relating to the performance of the television system are extremely important Lighting specifications in particular have a major impact on the performance of cameras The kinds of lights found at nuclear facilities are mercury vapor, sodium vapor, metal halide, and fluorescent

At present, the performance and technical specifications for video systems, as with electronic equipment, are determined by the field offices, an inefficient approach The final determination as to whether an alarm is real will be made by the system operator, and in most cases it will be based on what the operator can see with the camera In turn, the camera will perform only up to the specifications prepared in the field offices

Command and Control

Command and control must interface with all sensors, assessment equipment, communications systems, and electronic displays Typically the consoles contain visual and audio alarms, panels for directly monitoring protected areas, and communications modes (radio, telephone, intercom, or public address) for contacting security forces and command officials The consoles may also contain switching controls and monitors for viewing information reported by closed circuit television assessment equipment and the electronic access control system The key point here is that the design of command and control equipment must emphasize human engineering and the needs of the security force commander

Several features of some command and control systems at nuclear facilities give cause for concern Some systems can manage only a limited number of alarm and video inputs, and the computers may be subject to failure, although the impact of that problem is greatly reduced by the use of redundant equipment physically separated from the primary system Two omissions in the command and control standards at nuclear facilities are noteworthy The security systems are supposed to protect against electronic devices that collect classified information illegally, such as by eavesdropping. Protection is provided by means of periodic electronic scanning of areas to be used for classified conferences Little attention is paid to eavesdropping on unclassified conversations of key officials in, for example, hallways, from which the best information may be obtained, stationary, fixed equipment is not used

To counter the threat of electronic eavesdropping, one U S government agency uses off-the-shelf surveillance equipment to measure line resistance and other factors that would indicate tapping This equipment alerts the operators to any anomalies and their location The same system also monitors a radio frequency analyzer that constantly samples radio frequency energy and calculates its point of origin, again alerting the operator to anomalies. This type of monitoring equipment is likely to be more effective and efficient than are traveling teams of individuals who periodically perform electronic sweeps of classified areas, the present system

A danger with clandestine listening devices is that they could cause the importance of a position to rise The potential security impact of a low-level employee who may be able to record conversations of key employees is certainly elevated

The second omission is the absence of a requirement that the security system software access other data bases at the facility where important personnel information may be stored. It is easy to determine job by job what the impact would be if an employee were to collaborate with terrorists It is similarly easy to develop software to analyze events and personnel activities to detect suspicious patterns of behavior Information on security forces and technicians who maintain the system is especially important, because these two groups could do the most damage Variables to check are sick days taken, vacation patterns in relation to other employees, and pay advances

At the same time, it is important to be aware that the software used to analyze personnel information can itself be made the villain in the security system At present, the software is maintained by the contractor who installed the security system, in some cases, the nuclear facility does not even get a copy of the software source program There should be a clear requirement that the software be tested independently to ensure that it has not been subverted

Denial

The final step in either the graded or power block philosophy—barriers, walls, doors, and locks notwithstanding—is the use of the security force to deny access. The key to the security equation is denial, and that goal in turn lies almost exclusively with the capability of the on-site security force and the assistance it gets from off-site law enforcement agencies

On-site Security Forces. The quality of the security force is equivalent to the quality of each member in terms of character, training, and equipment The DOD is conducting studies of how people respond under stress in order to quantify the probability that a person will perform as trained, even in life-threatening situations A person's background and its potential influence on behavior are two points to be checked

The greatest point of vulnerability in any security system is the people who operate and repair it Some states, however, limit access to an employee's criminal record This restriction, which affects the NRC more than the DOE, is sufficiently troublesome that Congress passed a law requiring that the FBI help screen people who have access to nuclear facilities and materials and that the criminal records of employees be made available to facility licensees (Section 606 of the Omnibus Diplomatic Security and Antiterrorism Act of 1986, P L. 99-399)

With respect to those who operate or maintain the security system, DOE order 5632 4 of November 4, 1985, says that

> protective force personnel within exclusion areas are required to possess "Q" access authorizations and "L" access authorizations when a confidential matter is involved

> Maintenance personnel are to possess an access authorization equivalent to those levels of classified matter, and/or SNM [special nuclear materials] to which they will have access

The difference in the depth of the investigation for the "Q" and "L" clearances is substantial If their standards were followed to the letter, a portion of both the guard and maintenance crews would not get top security clearances, and the number of personnel with that access would be fewer, a positive change More important, a more stringent clearance requirement reduces the personnel base for rotating assignments, a measure that greatly assists in deterring collusion At the same time, it is prudent to clear all security and maintenance personnel to the highest level of access they may need In crises, an improperly cleared person may be granted access to sensitive material and information because of necessity; it is better to have foreseen this possibility and to have cleared the person in advance Finally, if supervisors are not fully confident of those under them because of a lack of information, their suspicion could be detrimental to the individual and the organization

A critical factor in security investigations is timing It is felt that more frequent reviews would, for example, have uncovered John Walker's spy activities One reason for periodic reviews is that people and the conditions of their lives change, sometimes to the detriment of job loyalty and performance. More frequent investigations should be required for all security and maintenance personnel. A related matter is the need to control the abuse of drugs Some facilities now require random urine samples and undertake routine searches of the premises

Training for the protective forces requires a minimum of eighty hours of introductory work and twenty-four hours of refresher courses each year The material should encompass the required procedures of the organization, individual skills training, and monthly exercises involving security responses to seizure, theft, or sabotage of the facility or materials Special response teams are also legislated, and their training is similar to that required of civilian SWAT teams One potential problem is that some training must sometimes take place during overtime, yet overtime funds are increasingly scarce

The DOE has improved the training of security managers and the readiness of its security forces through several programs They include the Central Training Academy at Albuquerque, New Mexico, and auxiliary protective force training That latter force, which is composed of nonsecurity guard contractor personnel, acts as a home guard The auxiliary force poses severe clearance problems, especially in terms of its being given access to classified material during an emergency

The size of the guard force, clearly an important consideration, must be determined on the basis of different attack scenarios. In general, the number of guards has been judged adequate in terms of the present design basis threat as defined for their facilities The problem is that the design basis threat may not be appropriate As a result, the adequacy of the guard force may not be sufficient to protect nuclear facilities or materials

Another determinant of the size of the guard force is the amount of time required to place security forces in a position to intercept intruders Present guidelines state that "security inspector response time to alarms shall not be more than 5 minutes Alternately, response time shall be less than the delay time that can be demonstrated from alarm activation until intruder could complete their adverse actions "

Each field office decides what constitutes a proper response to an alarm, it can range from simply pushing an acknowledge alarm button to deploying the security forces Moreover, although a five-minute response time is called for, travel times during certain periods of the day at larger nuclear materials facilities can be unpredictable Generally a larger response time than that based simply on the travel time of the intruder is available because of the time it takes to penetrate doors, walls, and fences, given their deterrent characteristics For the most part, penetrability times have been calculated for different threats As long as the capabilities of the attacker do not exceed the parameters on which the calculations were based, it is possible to predict the penetration time quite accurately The preferred size of the guard force is that needed to cope with the worst case situation, but clearly that sort of standard is unrealistic The alternative is for facilities to improve on their early warning and detection capabilities

A key point in this discussion is the speed with which attackers can penetrate a perimeter fence and avoid the detection devices Tests show that it can be done in less than one to four minutes, depending on the distances to be covered, distance being the other determinant of force size The greater the amount of time there is to respond to an attack—and time is a function of the speed at which the attacker must move and the distance to be covered—the smaller the security force can be to protect against penetration of the outer barriers

Facilities that process nuclear materials, as well as the weapons assembly plant (PANTEX), equip their security forces with weapons that should be equal to the firepower that a terrorist group might have They also have night-sighting equipment State-of-the-art body armor and bullet-resistant helmets provide acceptable protection to individual guards against small caliber weapons and, to a lesser extent and depending on the distance, hand grenade fragments

The transportation for moving security forces and special response teams has not always proved reliable Moreover, armored vehicles have tires that are susceptible to light antitank weapons, to which most terrorist groups have access. Those weapons are also capable of destroying guard towers and the hardened portal cubicles Defenders rely on 50-caliber machineguns mounted on some of the armored vehicles as their principal air defense and antivehicular (car or small truck) weapon These weapons are highly effective against a helicopter, hang glider, parachutist, or slow-flying fixed wing aircraft On the other hand, it is well documented that friendly fire from machineguns can exact a high toll on a facility's own forces Some security personnel do not realize the destructive capability of small arms and machinegun bullets With respect to the vehicles, they do provide the necessary high-speed transport capability

In the main, the conclusion reached on the basis of assessments of the type and quantity of weapons, equipment, and vehicles issued to security forces is that they are cost-effective against the quantified design basis threat being used. It has also been concluded that they would be used effectively in an attack On the other hand, these assessments do not assume any degradation of the systems, personnel, and equipment, as they should in order for realistic standards to be set

Off-Site Security Forces. The DOE and the NRC have entered into agreements with local, state, and federal law enforcement agencies for support of facility forces Field offices specify communications checks on assigned radio frequencies and local telephone systems, and the various forces engage in mock exercises annually With respect to the latter, however, funding is often so scarce that less than the full complement participates Moreover, it is unclear what would be the priority for local forces in the event of contemporaneous crises such as an attack on a facility and a natural disaster

Annual mock exercises do not provide sufficient experience to ensure a coordinated response in an actual emergency The movement and use of multiple security forces are a complex command and control matter, as evidenced by the problems encountered in the Grenada exercise Ideally more frequent and fully funded exercises involving both on- and off-site security forces are desirable

Denying access to a protected asset requires an integrated response by all elements of the protective system· equipment, facilities, and people At present, the subsystems and the required integrated response are based on the quantified threat prepared by headquarters, as interpreted, in terms of the detailed specifications and level of capability of the protective systems, by the engineers and security personnel at the field offices and facilities One result of this approach is that security system capabilities vary across facilities

Evaluation of Security Systems

The DOE evaluates security systems against the design basis threat, however, it is unclear what standards are to be used in evaluating capabilities because there are no predefined operational requirements or technical specifications

In the end, it is difficult to say with certainty what the capability of a protective system is with respect to threats of various levels of sophistication For example, the opening and closing of areas by operational personnel in the course of the regular activities is considered a valid test of access alarms However, a terrorist is likely to target the vulnerabilities of a system, not its normal operations Another example is that each field office is permitted to set the sensitivity test levels for sensors What is needed are uniform standards for all sensors and other segments of the total protection system

The inspection and evaluation section of the DOE has drafted its own performance criteria, which it uses to pass or fail the systems in place at facilities The problems with these standards have been outlined

Shipments of Nuclear Materials

Interfacility Shipments

The DOE transports nuclear materials and a portion of the nuclear weapons it manufactures for the DOD between its facilities Per year, it makes more than one hundred truck and rail shipments, with the percentage of weapons transfers by truck now increasing

DOE has developed special trucks and railcars for exclusive use in transporting threshold quantities of nuclear materials The trucks, modified tractor-trailers called safe-secure trailers, are armored and contain deterrent and denial devices All weapons-grade plutonium and enriched uranium are moved by truck. Similar safe-secure railcars are used for large-volume rail shipments Both types of vehicles have been tested extensively for their capability to withstand different kinds of terrorist attacks, with close attention to physical protection, communications, denial of access, armor, energy absorption in the event of impact, and personnel safety These vehicles are accompanied by escort and power buffer vehicles that are also specially equipped and protected

The communications system, which involves the transmission of voice and digital data, has been tested extensively as well For example, the feasibility of two-axis inertial attitude reference devices and laser radar and chemical beacon systems for relocating hijacked vehicles was analyzed The resulting communications system is capable of maintaining contact with the special vehicles anywhere in the continental United States

An access denial system for transport vehicles is designed to delay the attackers from reaching the nuclear weapons or materials until other forces arrive at the scene A variety of devices are used, including instant foam, maladorous substances, and some incapacitants It is believed that the various measures provide adequate protection against the defined terrorist threats

The guard forces that accompany the safe-secure vehicles are employees of DOE, they ride in escort vehicles for road transport and escort railcars for rail transport The trucks are also driven by armed couriers All these guards undergo security investigations and an eight-week training course, with refresher courses every three months They receive annual refresher training in radiation monitoring, firearms safety, security, and SWAT team techniques

More likely than a hijacking is an accident, particularly one involving an impact at high velocity It is widely believed that even in that circumstance, detonation of high explosives or plutonium dispersal is almost impossible

The greater danger to the viability of the interfacility transport program is complacency The system was designed to meet a specific terrorist and criminal threat The character of that threat is changing, however, in particular, terrorists seem willing to sacrifice even their lives New analysis of the design basis threat may be in order

Intrafacility Shipments

Special nuclear materials being moved between buildings are usually transported in a sealed, locked van or trailer A shipping custodian schedules authorized shipments with the nuclear materials custodian The shipping custodian also releases the materials from the storage vault to the uranium operations personnel for loading into the sealed van These procedures are all documented. At the destination, the van enters a vehicle trap that has doors at either end, only one of which may be open at any one time At this point, the two-person rule applies An exterior door is raised, and the material handlers back the van up to the loading dock A receiving custodian breaks the seal and inspects the material containers during unloading Both he and the guard verify the shipment and complete the necessary documentation Guards located in hardened cubicles oversee the loading and unloading process

Substantial effort has been expended to design a system that ensures the integrity of the cargo and that accounts for the materials during loading and unloading But the transport system is weak during the period of movement between the loading and unloading sites The current security system and procedures are geared to the skilled, covert, sneaky intruder. The recent helicopter snatch of prisoners from prisons in North Carolina and Paris and the truck bomb incident in Beirut suggest, however, that more violent, overt threats also need to be considered It is advisable to reassess the adequacy of the level of transport vehicle armament and security during the time of movement between buildings in the light of these types of threats Factors that should be addressed are the weight of the vehicle and the nature and number of weapons issued to the transport force

Conclusions and Recommendations

A serious problem with present security systems at nuclear facilities is that the threats and standards prepared by the NRC and DOE are general, and the field offices are required to develop their own local threats and, on that basis, to prepare detailed specifications for security systems at sites in their jurisdicton As a result, the capabilities of the systems vary across facilities

A further problem is that no testing is required beyond "alarm"/"no alarm" (which checks whether the sensors will activate the alarms), and there is no definition of what stimulus should set the alarm off Present standards accept the stimulus of routine personnel movements Such an approach to setting standards ignores the probable innovativeness and shrewdness of the likely adversary Another problem caused by the absence of defined performance standards is that there is no good basis for collecting empirical data on the true capability of the security system for any facility

For purposes of inspection and evaluation, the DOE unit in charge of that effort has had to develop its own standards Its standards do not, however, constitute policy to which all parties must adhere, and they differ from those being used in the field As a result, they are likely to engender conflict and controversy Nor can field or facility personnel use them as a basis for requesting funds to bring their systems up to that standard

Other agencies of the federal government have prepared their own security system requirements, standards, and specifications Sharing these data would be useful and cost-effective A new effort is needed to create an administrative process whereby the exchange of information, testing of equipment, and participation in R&D programs are facilitated among all federal agencies

As to the actual performance of systems, it is imperative that they be able to detect intruders sooner than is called for at present DOD has military personnel detecting radars and point sensors that meet the early warning requirements In addition, they reduce the number of human detectors needed Each nuclear facility should assess whether this equipment is cost-effective in terms of potential personnel reductions or possible reassignment to duties to increase overall security

Security guards and maintenance technicians are the potential weak link in the security chain against an insider threat Both groups have access to all parts of a facility and could be called on during an emergency to perform critical tasks Therefore their behavior and background are critical Present standards do not require that these two groups of personnel receive the highest security clearances, with their all-important comprehensive background check It is imperative that the relatively small amount of funds required to conduct background investigations of all security guards, maintenance technicians, and other critical personnel be made available In addition, it is important to conduct reinvestigations of key personnel frequently enough to identify adverse change in individuals and their circumstances.

The vehicles used for intrafacility shipment of nuclear materials are vulnerable to small arms fire, are relatively light in weight, and can be entered easily using handguns or small explosive charges. The entire physical arrangement of this transport system should be reviewed to determine its vulnerability to new types of threats, particularly a helicopter intrusion or a high-speed truck bomb, and other violent and overt attacks. Physical security must be as thorough as that found at the loading and unloading stages.

The physical protection systems of civilian nuclear facilities appear to approach the generic standards established by headquarters, however, the standards are vague and have left a lot of room for interpretation at lower levels. Moreover, there is a serious question as to whether the defined design basis threats remain appropriate. As to their implementation, the personnel security investigation stops short of a reasonable goal, and the lack of coordination among and use of equipment from all government agencies is economically wasteful. When a security system at a nuclear facility is tested by a smart adversary, as it will be, his or her probability of success should be predefined and acceptable to headquarters, field offices, and facility managers. It should not be an unknown because the systems were designed around vague and incomplete standards.

Five steps in particular are strongly recommended at this time.

First, those agencies responsible for civil nuclear facilities should jointly prepare detailed threat definitions, operational requirements, and equipment specifications to protect generic nuclear facilities, and these matters should be issued as policy. The agencies should provide sufficient detail to guide the design of specific security systems and to identify candidate components.

Second, the DOE, NRC, and DOD should explain to Congress why government-developed security and other military equipment are not used to upgrade existing security systems and to stock future ones.

Third, each DOE and NRC facility should be assessed to determine the impact on the size of the guard force and on warning time when personnel-detecting radars and ground point sensors are installed.

Fourth, all security guards and technicians should be investigated for the highest security clearance, with reinvestigations every four years.

Finally, the processes and vehicles used in intrafacility transport of nuclear materials should be evaluated against a range of threats and attack scenarios, including violent air and vehicle assaults.

All of these recommendations are feasible and cost-effective. The appropriate congressional subcommittees should direct that they be implemented as soon as possible.