POST 9-11 SECURITY ISSUES FOR NON-POWER REACTOR FACILITIES

P.J. Zaffuts
Morgan Lewis & Bockius LLP
1111 Pennsylvania Avenue, NW, Washington, DC 20004

ABSTRACT

This paper addresses the legal and practical issues arising out of the design and implementation of a security-enhancement program for non power reactor nuclear facilities. The security enhancements discussed are derived from the commercial nuclear power industry’s approach to security. The nuclear power industry’s long and successful experience with protecting highly sensitive assets provides a wealth of information and lessons that should be examined by other industries contemplating security improvements, including, but not limited to facilities using or disposing of nuclear materials. This paper describes the nuclear industry’s approach to security, the advantages and disadvantages of its constituent elements, and the legal issues that facilities will need to address when adopting some or all of these elements in the absence of statutory or regulatory requirements to do so.

INTRODUCTION

In the wake of the terrorist attacks on September 11, the federal government has introduced or passed a host of proposals to study, evaluate, and strengthen the security of facilities considered to be part of the nation’s critical infrastructure, including electric power, chemicals, petroleum refining, oil and gas transportation, and communications. A few examples include the National Energy Infrastructure Security Program Establishment Act (S. 1529), the Homeland Security Act of 2002, the Critical Infrastructure Information Security Act of 2001, the Pipeline Safety Improvement Act, the Energy Policy Act of 2002 (S. 1766), and the Chemical Security Act of 2002.

Further, there is a recognition, whether accurate or not, that certain radioactive source material is not subject to adequate accountability and security measures. Moreover, concern over a so-called dirty bomb has prompted Congressional bills (e.g., Dirty Bomb Prevention Act of 2002), an NRC-led effort to determine whether additional controls are appropriate, as well as international efforts (e.g., International Convention on Radiological Dispersal Devices, March 2003.)

A number of industries have, or are considering, adopting voluntary guidelines regarding security enhancements. For example, on June 14, 2002, the North American Electric Reliability Council (NERC) (which had been identified by the Department of Energy as the Sector Coordinator for Electricity Security) issued the “Security Guidelines for the Electricity Sector.” The NERC standards address areas such as vulnerability and risk assessment, threat response capability, emergency management, continuity of business processes, communications, physical security, information technology / cyber security, employment screening, and protecting potentially sensitive information. ¹
Similarly, the Chemical industry has adopted a set of security standards under their “Responsible Care” program. These standards address such things as risk assessment, employee and contractor training, physical security, access control, emergency preparedness and response, and cyber security.2

Common among these voluntary standards is their lack of implementation guidelines. Accordingly, these industries are left with the flexibility (and responsibility) to create and tailor their own security programs based on their unique circumstances. Accordingly, companies in these industries, as well as companies in the host of industries without any security standards at all, are still faced with the following daunting questions: (1) what are the particular elements of an effective (or enhanced) security program; (2) which of these elements should be implemented at any particular facility; and (3) are there any legal issues associated with implementing elements not mandated by federal regulations or in a manner not specified by such regulations?

Beyond the enhanced security standards, many industries are, or will need to, consider security in many areas of their daily business activities. For example, personnel policies, facility siting and capital improvements, and public relations should all be influenced by security considerations. Although the purpose of this paper is not to answer these questions, an examination of the nuclear security model may provide a rational basis for beginning to address these questions.

THE NUCLEAR SECURITY MODEL

Commercial nuclear power plants are the most secure industrial facilities in the United States. As Nuclear Regulatory Commission (NRC) Commissioner Edward McGaffigan said, in 1999, “there are threats to the nation. But outside the military, [the nuclear energy] industry is probably the best at protecting its assets.” This opinion was echoed by the Director General of the International Atomic Energy Agency who said on September 28, 2001, “[w]e should not lose sight of the fact that nuclear power plants are among the most secure and robust industrial facilities in the world.”

It should be noted at the outset that security at commercial nuclear power plants is neither intended nor designed to preclude any possible harm to the facility. Rather, security at these facilities is intended: (1) to prevent sabotage that could lead to the release of radiation injurious to the public; (2) to prevent the theft or diversion of radiological material; and (3) to provide an effective response to emergencies. Security at commercial nuclear power plants is comprised of four components or elements: (1) A reference or “design basis” threat; (2) physical security; (3) internal security; and (4) emergency preparedness and response. Each of these elements, which are discussed in further detail below, is subject to stringent NRC regulation and oversight.
Design Basis Threat

Operators of commercial nuclear power plants are not responsible for establishing the threat against which they must protect. Rather, the threat is defined by the government and is referred to as the “design basis threat.” The design basis threat is not a “risk assessment,” but defines the actual threat to the facility. It is established in NRC regulations as a “determined, violent external assault, attack by stealth, or deceptive actions.” The assault is carried out “by up to two small teams,” all members of which have “specific skills and weaponry.” In addition, the threat includes “a knowledgeable insider” who assists the teams in carrying out their mission.

The design basis threat provides a uniform basis for security requirements at all commercial nuclear power plants. Just as important, it provides a bright line demarcation between the security responsibility of the plant operator, and that of the federal, state, or local government.

Physical Security

“Physical security” is the more traditional concept of security at an industrial facility. This includes physical elements such as vehicle barriers, fences, walls, etc.; a security or guard force; surveillance and other electronic measures to detect intrusions; and other intrinsic physical elements of a facility that contribute to security. Physical security is considered the primary protection against facility damage that could result in the release of radioactivity as a result of an external assault.

For purposes of physical protection of a nuclear power plant, the NRC divides sites into three concentric rings: (1) the center or “vital area”, which indicates the nuclear reactor; (2) the middle or “protected area”; and (3) the outer “owner-controlled area.” Not surprisingly, physical security requirements become more stringent the closer one gets to the center or vital area. The “owner-controlled area” includes all property associated with or surrounding the plant. This area is generally patrolled by site security personnel and vehicle access is controlled (e.g. by checking identification and looking into vehicles coming into the parking lot). The “protected area” is an area that can be entered only by those having pre-approved access and includes the majority of the nuclear plant buildings and facilities. Personnel cleared under the plant’s access authorization program and issued an “Access Badge” (see infra, section II.D.), may enter the protected area without an escort. Visitors must be escorted by an authorized employee at all times. The “vital area” contains the equipment essential for operating the plant (and shutting down the reactor in the case of an emergency) and has an additional level of access restrictions.

Nuclear power plant physical security includes a lighted, fenced, “protected area” perimeter, as well as vehicle barriers, and a remotely monitored isolation zone immediately inside the protected area. Security teams periodically patrol the perimeter, the "owner-controlled" area and vehicle access controls. Access control should include personnel access to protected area only via controlled checkpoints, site-specific photo identification for all personnel having unescorted access to protected area, detection of firearms, explosives, and incendiary devices through use of metal and explosive detectors, searches of all vehicles and hand-carried packages and radiation monitoring at portals upon exit. The Physical Security Organization is
responsible for responding to the design basis threat and for calling-in to law enforcement if necessary. Federal law authorizes the use of firearms for physical protection. Personnel must pass NRC-approved initial and annual qualification programs, including firearms training and personnel must participate in NRC-organized “force-on-force” security exercises.

Internal Security

“Internal security” consists of those programs whose goal is to prevent or protect against the “insider threat.” Internal security consists of two complementary programs: (1) access authorization; and (2) “fitness-for-duty.” The access authorization program is equivalent to a security clearance process for nuclear workers. Workers who have access are permitted to enter the nuclear power plant’s “protected area” without an escort. To obtain and maintain such access, the NRC requires that operators or owners of nuclear power plants take reasonable measures to assure that the individual be “trustworthy,” “reliable,” and “not an unreasonable risk.”

Granting and maintaining access to the protected area is a three-step process: (1) the background investigation; (2) the psychological assessment; and (3) the continual behavior observation program. The first two steps are applicable to the initial step of granting access, while the third step applies to individuals already granted access. The nuclear power plant operator (or designated contractor) conducts a background investigation of each worker seeking access which consists of a verification of the individual's education, work and military history, and credit check. The investigator will also contact a number of personal references in order to evaluate the individual’s character. The psychological assessment consists of a standardized personality test, and, if necessary, a follow-up interview with a licensed psychologist. Finally, all management at nuclear power plants (supervisors and above) are trained on spotting.

All personnel with access are also subject to the site’s fitness for duty program. The program provides assurance that personnel previously deemed trustworthy (i.e. having unescorted access) remain fit to perform their assigned duties. The program consists of an initial (pre-access) drug/alcohol test, as well as continuing random drug/alcohol testing and continual behavioral observation. Workers who are judged impaired, or whose fitness-for-duty is otherwise questioned, shall be removed from licensed activities and may be returned only after determined to be fit to safely and competently to perform their assigned responsibilities. Upon finding a first positive, there is an immediate removal from licensed activities for no less than 14 days, referral for assessment and counseling, plans for treatment, follow-up, and future employment. Upon finding a second positive, there is removal from unescorted access and removal from licensed activities for 3 years. Many owners have more stringent policies than those of the NRC, including mandatory termination on a first positive.

Emergency Preparedness and Response

Emergency preparedness and response addresses how to mitigate the consequences of an “accident,” whether it is the result of an unintentional or intentional act. Each nuclear plant must prepare a detailed emergency plan whose purpose is effectively to respond to an incident in which there is a potential for a release of radioactivity. The plan directs the acts of plant
personnel in the event of an emergency including command, control, and communications with local law enforcement, and federal, state and local emergency responders.

The emergency plan has a wide footprint, covering a 10-mile radius with the plant at its center (the so-called “emergency planning zone”). The plan covers procedures for communication with response organizations, emergency personnel and the public, assessment of potential off-site radiation dose consequences, emergency facilities and equipment, training of response personnel, and periodic exercises and drills. The plan is reviewed by the NRC and the Federal Emergency Management Agency (FEMA). Full-scale exercises conducted once every two years, include participation of on-site and off-site emergency response organizations, plant employees, local hospitals, and radiological monitoring teams.

ADVANTAGES OF THE NUCLEAR MODEL

Benefits of the Nuclear Model include: (1) significant assurance that the design basis threat will be averted and that the public will be protected in the event of an attack; (2) heightened awareness of security among site personnel; and (3) consistent industry-wide requirements that foster an environment of sharing of security/emergency lessons learned among nuclear power plant operators.

The design basis threat element of the Nuclear Model provides an unambiguous definition of the threat against which plans to defend need to be made. A well-defined design basis threat is key to an efficient, effective, and reasonable security response. It allows a site operator to target security resources toward the most likely or most significant risks. Another benefit of a government-defined design basis threat is its indirect definition of what the owner is not required to protect against, e.g. suicide bombers, massive assault, etc.

The physical protection provisions provides multiple physical barriers and a well-trained and qualified security force. The internal security element of the physical security program provide access authorization and Fitness-for-Duty that generally ensure a fit, trustworthy, and reliable workforce. Emergency planning and response of the Nuclear Model: (1) minimizes the consequences and liability for all accidents irrespective of cause; (2) fosters public confidence in, and acceptance of, the plant as a responsible corporate citizen; (3) creates a defined, effective relationship with state and local police, fire, and rescue personnel; good relations with local authorities also facilitate assistance in dealing with protests, trespassers, workplace violence, medical emergencies, and other matters; (4) integrates security/emergency with plant operational safety, creating a more robust and effective response organization; and (5) effectively is used in response to natural and other disasters. Many local governments have, in fact, benefited from their role in emergency planning -- nuclear plants have provided significant training, resources, and other assistance to local governments as part of emergency planning and response.

DISADVANTAGES OF THE NUCLEAR MODEL

Disadvantages of the Nuclear Model include: (1) extensive compliance and enforcement relationship with the state or federal government; (2) significant costs associated with the initiation and operation of the various security programs, including those necessary to administer
access authorization and fitness-for-duty programs; and (3) unavoidable reliance on the cooperation of sometimes reluctant outside groups (e.g., local governments) for effective emergency planning.

As inferred in the above description, nuclear power reactors are subject to an intrusive regulatory regime of security regulations. Under the NRC’s requirements, the facility owner or operator must prepare detailed security (including fitness-for-duty and access authorization programs) and emergency plans, all of which are subject to NRC review and approval. In addition, the NRC ensures that these plans are properly and adequately implemented through the use of periodic on-site inspections. Moreover, the NRC expects self-policing, internal compliance audits, and self-reporting of findings and violations. Violations can lead to enforcement actions, monetary penalties, adverse publicity, and in some cases, criminal investigations and prosecution. The legitimate desire of the nation’s critical infrastructure industries is to avoid the imposition of an NRC-like regulatory regime regarding security through the use of voluntary security enhancements.

Nonetheless, enhancing a facility’s security is expensive. Physical security measures (e.g., fencing, vehicle barriers, surveillance equipment, security guards and training, metal/explosive detectors, remote surveillance, etc.) require a substantial initial capital expense. Additional staffing is necessary for both security guards and for the development and implementation of enhanced internal security programs. For example, the personal information associated with access authorization and fitness-for-duty programs requires (for the protection of the employer as well as the employee) that such programs be administered to exacting standards. Even the imposition of restrictions to certain areas of a facility can impact productivity, although such impacts can be lessened by limiting the areas requiring heightened security and the number of persons requiring access to these areas.

Finally, many industrial facilities, whether or not they work with nuclear materials, do not enjoy the full support of the local community. However, such support may be a critical and often essential component to an effective emergency plan. In the nuclear industry, such cooperation is necessary in order to satisfy NRC and FEMA (now DHS) requirements. In certain situations, nuclear facility owners have had to engage in quid-pro-quo arrangements with local governments (e.g., new communications equipment for local fire fighters in exchange for local cooperation) to obtain their support and cooperation in emergency planning.

LEGAL ISSUES ASSOCIATED WITH ADOPTING SOME OR ALL OF THE NUCLEAR MODEL

If a company decides to pursue security enhancements in the absence of regulatory requirements to do so, such enhancements should only be adopted after a thorough examination of the legal issues associated with such actions. The following provides a brief summary of a number of such issues.

Certain security enhancements could negatively alter the terms and conditions of a facility’s workers. Examples include: (1) initiating or enhancing personnel surveillance; (2) restricting access to buildings; (3) personnel, vehicle, or hand-carried package searches; (4)
metal detectors; and (5) logging of worker entrances and exists to/from the facility or certain internal areas. Collective bargaining agreements may or may not address these types of changes. For this reason, it is prudent to review any proposed change that could affect represented employees’ terms and conditions of employment against collective bargaining agreements.

In the event that a company decides to hire or enhance a private guard force, State law could limit the scope of authority that can be given to private guards. For example, how much force can be used to respond to threats, what types of weapons or tactics may a guard force use, and under what circumstances may they be used? Any limitation in a guard force’s authority should be specified in contracts with companies supplying such protective services.

Regarding internal security, background investigations implicate the Fair Credit Reporting Act (FCRA), psychological screenings implicate the Americans with Disabilities Act (ADA), and criminal history checks may implicate state law. Additionally, fitness-for-duty provisions implicate the ADA and can create labor relations issues. FCRA considers all background investigations performed by an outside entity a “consumer report” or “investigative consumer report.” One must receive applicant/employee consent before conducting an investigation. If adverse action is predicated on the background information, then the employer must provide the applicant/employee with a copy of the report, and summary of rights five days prior to taking the action.

Under the ADA, psychological/medical screens of applicants are not permitted. Post-offer, pre-employment medical screens are permitted if: (1) required of all applicants; and (2) results are used only for permissible purposes. There may be state law restrictions on what type of information may be asked of an applicant regarding criminal history. Generally, one cannot request applicants to disclose arrests, only convictions. Attempts to verify information may implicate FCRA. Continuous behavioral observation depends on subjectivity, and inherent subjectivity could be problematic. Referrals to the company physician/psychiatrist are held to be an “adverse action” under whistleblower protection statutes. Unlike illegal drugs, alcoholism is not excluded from ADA protections, thus, alcohol testing under the FFD must be exclusively to determine “current use.”

Security measures must also be consistent with requirements imposed under applicable labor and employment laws and good business practices. All employment actions based on security requirements remain subject to challenge under employee protection laws. It is important to adopt clear, defensible policies, make rational, non-discriminatory employment decisions, apply policies consistently, provide training and publicize the workforce. For example, job prerequisites placed on applicants in the name of security (e.g., background checks, psychological assessments, etc.) must be defensible as bona fide occupational qualifications for the position in question. One way of limiting exposure to such issues is to limit the number of persons requiring access to “sensitive” areas, which will, in turn, reduce the number of persons requiring background checks, etc.
CONCLUSION

The nuclear security model is effective and is recognized as such by the U.S. government. The nuclear security model is also very demanding, yet this is primarily a result of the extensive oversight provided by the NRC. Given the legitimacy of this model with lawmakers and the public, industries would be well advised to consider the model as a guide when evaluating options for enhancing security at their facilities.

FOOTNOTES

1. In a somewhat disturbing move, soon after NERC’s voluntary security enhancements were adopted, the Federal Energy Regulatory Commission (FERC) proposed a set of mandatory security enhancements applicable to all “electric market participants. These enhancements had as their primary focus electric systems and personnel, and a secondary focus on physical security.