PNNL-17802

Security during the Construction of New Nuclear Power Plants: Technical Basis for Access Authorization and Fitness-for-Duty Requirements

KM Branch
KA Baker

September 2009

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Disclaimer

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America
Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov

online ordering: http://www.ntis.gov/ordering.htm

Security during the Construction of New Nuclear Power Plants: Technical Basis for Access Authorization and Fitness-for-Duty Requirements

Kristi M. Branch

Kathryn A. Baker

Pacific Northwest National Laboratory

September 2009

Prepared for the U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research
Division of Risk Analysis
Human Factors and Reliability Branch

ABSTRACT

This report presents information gathered and analyzed in support of the U.S. Nuclear Regulatory Commission's (NRC's) rulemaking efforts regarding new nuclear reactor construction. Following the terrorist attacks on the United States in 2001, greater attention has been given to security of the nation's critical infrastructure, including nuclear power plants. The report summarizes information obtained from a review of literature, discussions with a variety of security and construction experts from across the different critical infrastructure sectors, and participation in a workshop on construction security hosted by The Infrastructure Security Partnership that focused particularly on the nuclear sector. It discusses the need for, status of, and issues associated with security during the construction phase of U.S. critical infrastructure. It applies a vulnerability assessment framework to examine potential threats, identify standard practice, and evaluate the need for enhanced protective measures. It concludes that there is a basis for personnel security requirements during construction.

EXECUTIVE SUMMARY

This report describes the technical basis for U.S. Nuclear Regulatory Commission (NRC) personnel security requirements during the construction phase of new nuclear power plants (NPPs). It presents the results of a study of how security is being addressed in the construction phase of U.S. critical infrastructure (CI) sectors in the heightened risk environment following the 2001 terrorist attacks. It also describes how initiatives responding to the post-2001 security context are affecting the technologies, policies, and requirements for U.S. CI protection and security and the standards and expectations of CI stakeholders. Because of the hiatus in building new nuclear power plants in the United States over the past several decades, there was little recent U.S. experience with NPP construction to draw upon for this analysis. This study makes it clear, however, that the terrorist attacks of 2001 and continuing concern about terrorist threats have significantly changed the security context for U.S. NPP construction since the previous wave of NPP construction.

This effort was motivated by questions about whether, when, and to what extent personnel security measures, particularly personnel access authorization (AA) and fitness-for-duty (FFD) programs, both of which are currently deemed necessary and appropriate during NPP operations, and insider mitigation programs should be applied during the construction phase of new NPPs. Personnel access authorization requirements are implemented to protect against threats introduced by individuals, particularly those approved for unescorted access to the site or facility. Fitness-for-duty requirements are implemented to protect against threats created by individuals whose capability to perform their assigned duties is impaired for any reason, including drug or alcohol use, fatigue, or other factors. Insider mitigation programs share the goal of ensuring the trustworthiness and reliability of the workforce with access authorization programs. They typically focus on supplementing access authorization programs but put a greater focus on counterterrorism intelligence, surveillance, and information sharing across agencies and sites. In this report, personnel access authorization, fitness-for-duty, and insider threat mitigation programs are referred to collectively as personnel security requirements. These requirements seek to enhance safety and security through selection, deterrence, detection, and mitigation.

The experts consulted in this study emphasized the importance of considering all the pathways by which personnel with access to or working at a NPP, or other CI, construction site could threaten safety and security, either intentionally or inadvertently. They also stressed the importance of including measures to address both intentional and inadvertent threats in the analysis. The inclusion of measures to address intentional as well as inadvertent behaviors is consistent with recent guidelines on personnel security, particularly those designed to address information security or to qualify personnel for accessing classified or sensitive materials.

Consequently, the personnel security focus of this study includes consideration of both (a) the pathways by which malicious adversaries can threaten the security of a CI facility during construction and its security and safe operation once completed, and (b) the pathways by which other personnel can intentionally or unintentionally increase the vulnerability of the facility to such threats or magnify their potential consequences. Personnel security therefore is concerned about both the trustworthiness and reliability

of individuals, to address intentional actions, and their reliability and fitness-for-duty, to address inadvertent errors, lapses, or failures to reliably and competently perform assigned duties.

Security during construction is important for at least three reasons. First, breaches of security can jeopardize facility safety, which in turn can threaten the safety of not only workers at the site but also, potentially, surrounding populations. Second, for some facilities such as NPPs, security is essential to protect the facility, its contents, and associated technologies and information from being captured or acquired by an adversary. Third, security measures help to ensure continued functionality through protection of the facility and the assets it represents from damage or destruction.

These general considerations resulted in the study exploring four questions:

1. To what extent do threats of concern exist during the construction phase of NPPs?
2. What are current, typical construction practices and do they adequately protect against these potential threats?
3. What, if any, enhanced protective measures do experts recommend?
4. Are the recommended protective measures in use at other CI facilities under construction? Are personnel security requirements warranted and/or justifiable in terms of costs and benefits?

To address these issues, the project team gathered information by reviewing the open literature, benchmarking construction security practices in other CI sectors, interviewing experts across CI sectors and substantive areas of relevance, reviewing governmental initiatives undertaken to enhance the security and resilience of U.S. CI, and participating in a workshop on CI construction security to obtain a broad overview of the issues of relevance to CI and NPP construction security. This study's information, conclusions, recommendations come from these sources.

Discussions of security requirements necessarily include consideration of threats and vulnerabilities. The scope of this project did not include the conduct of threat, vulnerability, or risk assessments for nuclear power plants under construction. Rather, this project's mandate was to draw upon experts who had conducted or were familiar with such assessments and to present conclusions about threats, vulnerabilities, and risk, and, generally, how they would likely be manifest, at a level of generality consistent with public discussion. These experts' views also helped shape the analytical framework and approach for the analysis.

Threats of Concern during the Construction Phase of Nuclear Power Plants

The information gained from the experts interviewed for this project and the relevant literature make it clear that there are several threats of concern during the construction phase of NPPs. These threats fall into three categories:

- Immediate and delayed impact threats;
- Intentional and inadvertently-caused threats;
- Threats caused by insiders, outsiders, and insiders colluding with outsiders.

In the case of immediate threats both the causes and consequences occur during the construction phase; for delayed impact threats the causes may occur during the construction phase but the consequences occur after fuel has been brought onto the NPP construction site or the plant has begun operating. Intentional threats, which are primarily trustworthiness- and reliability-based, can be caused by individuals and groups with the intent to damage, delay, or shut down a CI facility. Vandalism, sabotage, or aid to outsiders by workers who are untrustworthy or unreliable are examples of intentional threats. Inadvertently-caused or unintentional threats, which are primarily fitness- and reliability-based, result from individuals' errors, lapses, or failures to reliably and competently perform assigned duties. The potential for both intentional and inadvertently-caused threats is furthered by the open and large-scale nature of NPP construction sites and by the number and variability of workers, activities, materials, and equipment over the construction life cycle. Likewise, the demonstrated high tendency of construction workers to use drugs and abuse alcohol relative to other worker categories tends to increase the potential for both types of threats. The third threat category, threats caused by insiders, outsiders, and insiders colluding with outsiders, can be a combination of the first two categories.

This study put great weight on threats that could result in a delayed impact on the plant once it is in operation. Delayed impact threats have the potential for consequences that jeopardize the public health and safety, the common defense and security, and the environment. However, historical evidence demonstrates that threats to the security of the plant while it is under construction should not be dismissed. Such immediate threats can pose a significant risk to (a) public confidence in the safety and security of nuclear power; (b) continuity of operation of nuclear power plants; and (c) the safety and security of workers at the site and its immediate vicinity.

Given the current threat environment in the U.S. and the desirability of NPPs as potential targets, the experts consulted for this project and the relevant literature identified several credible threats of concern during the construction phase of NPPs. These include:

- Direct external attacks;
- Immediate acts of theft, vandalism, or sabotage;
- Hidden explosive devices;
- Compromised critical safety- and security-related SSCs, especially software systems, from sabotage or accumulated errors;
- Compromised or deficient major components or materials from sabotage or accumulated errors;
- Access to and theft of critical information; and
- Caching weapons or explosives for later use.

The consequences of such events or conditions would be of a nature and degree that protection against them falls within the regulatory scope of the NRC.

Adequacy of Current Construction Practices to Protect Against Potential Threats

Typical construction practices; construction industry standards and applicable regulatory requirements governing security, occupational health, safety, and environmental

protection; and normal quality assurance/quality control (QA/QC) practices do not adequately protect against these threats of concern during NPP construction.

This study's investigation of current standard CI construction practices found examples of a wide range of security measures being used but little evidence of a CI-wide standard of security practice existing or being developed by either professionals or industrial sectors. Typical security practices focus on preventing access to the construction site by unauthorized people and vehicles and by workers impaired by drugs or alcohol, keeping contraband items from being brought on site, preventing theft of materials, and controlling movement of workers on site. The lack of any standard approach to security is due to the fact that security measures applied at any particular construction project are determined by the owner of the particular facility being built. Unless the owner imposes security requirements on its construction contractors, security measures are unlikely to be implemented. And, it is cost considerations that dominate facility owners' decisions about implementing security measures in private sector CI construction.

Though not aimed at achieving security, federal and state regulations governing worker health and safety and environmental protection have resulted in widespread adoption of some security-related measures. These regulations include those promulgated by the Occupational Safety and Health Administration and the Environmental Protection Agency. Compliance with such regulations has led to the use of security-related measures such as site access control, badging to identify authorized personnel, and safety and health briefings.

The study experts emphasized the importance of implementing rigorous QA/QC procedures as a means of achieving security. Typical QA/QC practices now include QA/QC procedures and documentation requirements, external QA/QC assurance teams and other related measures. Several of the experts associated with the nuclear industry pointed out that in earlier nuclear plant construction projects, work and material quality deficiencies, combined with deficiencies in QA /QC programs, caused major problems. These quality problems have proven difficult to resolve. Although quality practices have evolved to some extent since the first wave of U.S. NPP construction, recent investigations of safety and QA/QC practices during nuclear construction in other countries indicate that serious issues still exist. Some of the same quality control problems experienced during the construction of the first round of U.S. plants have been identified at the Olkiluoto plant in Finland, at the Rokkasho Reprocessing Plant in Japan, and at the Areva Shaw MOX fabrication facility construction project in South Carolina.

Experienced construction managers among the experts also indicated that, even if construction contracts specify heath, safety, and quality controls, the number of subcontractors and the intensity and complexity of site activities tend to make adequate control and coordination difficult. Experience also indicates that construction managers' inexperience with the particular management and task requirements has been an important source of construction-phase quality problems. Both the literature and experts consulted for the project identified the rapid growth in the number of nuclear power plants that were built during the first phase of NPP construction as a factor that contributed to the quality problems. They warned that these problems could reoccur if this pattern of rapid growth is repeated.

The study found some examples of CI separate-site construction projects at which comprehensive access authorization and fitness-for-duty programs were being implemented. These included off-shore oil drilling, high-tech chemical plant, casino, and government-owned construction projects. When a new facility is being constructed adjacent to an operating facility, that personnel security measures of the operating facility are normally applied to the construction work force. Comprehensive workplace drug and alcohol testing programs typically include provisions for pre-employment, for cause, post-accident, random, and follow-up testing. Both the available literature and the experts consulted indicated that pre-employment, for-cause, and post-accident testing were increasingly common for construction workers in all sectors. Random testing of construction workers was reported to be less common, particularly at projects with a high proportion of temporary workers. Considering the persistent issues of drug and alcohol use and workplace impairment among construction workers and the vulnerabilities created by drug and alcohol addiction, the experts emphasized the importance of keeping impaired workers and addicts off the construction site.

Access authorization measures that are used to some extent in CI construction projects include identity verification and badging, employment history and character reviews, pre-employment fingerprint checks, local criminal history background checks, and the use of the federal government's evolving terrorist screening process. All such measures, if applied in a coordinated and rigorous manner, are proving to be important parts of effective CI construction personnel security programs.

Enhanced Protective Measures Are in Use at Some CI Facility Construction and Their Costs Are Likely to Be Justifiable

The expert opinion and secondary data assembled for this analysis indicate that enhanced security measures are warranted for at least a subset of CIs under construction and that this subset includes NPPs. The experts and relevant literature indicate that the security measures deployed for CIs during construction in many sectors are inadequate to protect against post-2001 threats. Enhanced requirements for security during construction have been established for several CI sectors, including seaports and airports, military bases, foreign embassies, and many federal government facilities. This study's results indicate that enhanced security measures are also warranted for NPPs under construction. The full range of potential security measures are being applied to the construction phase in some sectors and by some facility owners. This demonstrates that these measures can be deployed in a construction setting.

This study found that enhanced security measures are generally implemented only in response to regulation, as with casinos and ports, or as a consequence of owner specifications. The experts warned that cost and schedule pressures, along with how risks incurred during the construction process are allocated among contractors and owners, often lead owners to accept higher risks than may be in the public interest. Regulatory and cost/benefit analyses of alternative requirements were beyond the scope of the study. However, expert opinion is that the consequences of inadequate security during construction could be extremely high, and that enhanced security measures

would have ancillary safety and efficiency benefits that may partially offset the costs of implementation. In addition, measures taken during the design and siting phases could reduce the need for or cost of security measures during construction.

Protective Measures to Achieve Personnel Security Are Available

Personnel security is one of the types of security measures that can be employed during NPP construction to protect against the threats identified in this study. Personnel security can be achieved through hiring competent, reliable, and trustworthy workers, training and supervising them effectively, and implementing measures to prevent, deter, detect, and mitigate careless, impaired, untrustworthy, malicious, or malevolent behaviors thereby reducing the potential for the pathways through which workers inadvertently cause or intentionally implement threats. The following table summarizes these factors, their causes or indicators, and typical measures used to prevent, deter, detect, or mitigate them. It illustrates that a range of personnel security measures has been established as effective and appropriate for addressing the pathways through which workers can threaten the safety and security of the facility and the construction site.

Worker Attributes, Causes or Indicators, and Typical Protection Measures

Worker Attribute	Causes/Indicators	Typical Measures Used to Prevent, Deter, Detect, Mitigate
True identity	➢ Physical features/biometrics ➢ Documents ➢ Knowledge	➢ Pre-employment identity verification and screening ➢ Fingerprinting ➢ Other biometric measures (iris, hand, face) ➢ Official identification documents (birth certificates, drivers' licenses, passports, military papers, social security card) ➢ Passwords
Authorization for site/work place access	➢ Badge ➢ Escort requirement	➢ Badge issuance and control procedures ➢ Entry/exit access control limited to badged or escorted workers ➢ Personnel and vehicle checks/searches/ surveillance ➢ Escort requirements ➢ Peer-checking/ 2-person rules ➢ Smart badges to document site access/egress/

Worker Attribute	Causes/Indicators	Typical Measures Used to Prevent, Deter, Detect, Mitigate
		movement and location on site ➢ Safety/security training
Impairment due to drug or alcohol consumption or abuse	➢ Drug use ➢ Alcohol use ➢ Drug or alcohol possession on site ➢ Drug sales	➢ Pre-employment and pre-assignment drug and alcohol testing ➢ For cause drug and alcohol testing ➢ Random drug testing ➢ Behavioral observation by co-workers and supervisors ➢ Self-reporting of medications ➢ Employee assistance programs
Fatigue	➢ Lack of adequate rest	➢ Shift scheduling ➢ Fatigue self-reporting
Mental instability	➢ Stress ➢ Mental illness ➢ Poor employment and credit histories ➢ Poor social relationships	➢ Psychological testing and interviews ➢ Life stress surveys and self-assessments ➢ Self-reporting ➢ Employment history review ➢ Credit history review ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Employee assistance programs
Vulnerability to pressure, coercion, exploitation, or duress	➢ Weak character ➢ Engagement in illicit activities, including drug use and drug sales ➢ Financial duress ➢ Criminal or terrorist networks ➢ Bringing contraband onto the site ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Pre-Employment and pre-assignment drug and alcohol testing ➢ Random drug testing ➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Employee assistance programs
Criminal or weak character	➢ Criminal record	➢ Pre-Employment and pre-

Worker Attribute	Causes/Indicators	Typical Measures Used to Prevent, Deter, Detect, Mitigate
	➢ Poor job history ➢ Criminal or terrorist network ➢ Poor credit history; fraud ➢ Poor social relationships ➢ Bringing contraband onto the site ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	assignment drug and alcohol testing ➢ Random drug testing ➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Employee assistance programs
Conflicting allegiances	➢ Stated allegiances ➢ Memberships in organizations ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews
Malevolent intent	➢ Statements of intent or desire ➢ Antagonistic or aggressive behavior ➢ Bringing contraband onto the site ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Red-teams ➢ Security-oriented QA/QC ➢ Insider threat mitigation programs
Inattention to or unawareness of security requirements	➢ Lack of knowledge ➢ Absence of security orientation	➢ Awareness and training programs ➢ Responsibility assignment

Typically, access authorization, fitness-for-duty, and insider mitigation programs are designed to implement the measures listed in this table. Access authorization programs normally focus on ensuring that only authorized persons are allowed onto the site or into controlled areas, and that those authorized for access are trustworthy and reliable. Their principal focus is on preventing insider threats. Recently, considerable attention has been given to access authorization for internal information systems, in addition to physical access to buildings and sites.

Fitness-for-duty programs typically focus on providing reasonable assurance that:

- Individuals are trustworthy and reliable as demonstrated by the avoidance of substance abuse and are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause, which in any way adversely affects their ability to safely and competently perform their duties;
- Individuals who are not fit to perform the duties that require them to be subject to the FFD program are detected early and prevented from performing those duties;
- Workplaces subject to FFD requirements are free from the presence and effects of illegal drugs and alcohol; and
- The effects of fatigue and degraded alertness on individuals' abilities to safely and competently perform their duties are managed commensurate with maintaining public health and safety.

Insider mitigation programs share the goal of ensuring the trustworthiness and reliability of the workforce with the AA programs. They typically focus on supplementing the measures implemented by AA programs but with a greater focus on counterterrorism intelligence, surveillance, and information sharing across agencies and sites.

These measures can be tailored to be commensurate with the threat and need.

ACKNOWLEDGEMENTS

This study could not have been completed without the generous contributions of the many experts throughout the critical infrastructure sectors who patiently explored the issue of construction security with us. We thank them. We also thank the NRC project manager, Ms. Niav Hughes, and the technical advisors, Dr. Valerie Barnes and Dr. Julius Persensky, who worked with us to shape and revise the report as the dimensions of the issue and framework of the analysis emerged. We also wish to express our appreciation to Mr. Perry Fowler from The Infrastructure Security Partnership for hosting the TISP workshop and to the numerous participants in the workshop. We learned much from the exchange of views and information that occurred at this event. Mr. Burk Dowell and Ms. Sadie Johnson provided much appreciated support and assistance in preparing the graphics for the report and assisting with report production. Mr. Thomas Grant provided invaluable help structuring the report and clarifying the presentation and we want to express our appreciation and respect for his ability to provide this assistance with such patience, good humor, and skill.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Access: Access means a determination that an employee requires access to a particular level of information or location in order to perform or assist in an assigned task.

Access National Agency Check and Inquiry (ANACI): ANACI means a National Agency Check (NAC) and employment, education, residence, reference, and law enforcement agency checks.

Access Authorization: Access authorization means that an entity with the appropriate authority has determined that an individual has met the requirements to be granted or certified to receive and/or maintain a specific type of access (e.g., unescorted) to a facility or portion of a facility and/or to perform specified duties.

Authorized Person: An authorized person means, in this report, an individual who has met the requirements and received authorization from an entity with the appropriate authority to access a specified site, or portion thereof, and perform assigned duties.

Automated Fingerprint Identification System (AFIS): An automated system that enables searching of fingerprint files and transmitting of fingerprint images. The system uses information technology to automate file searching and transmit "digital fingerprint images," thus increasing speed and reducing personnel demands on fingerprint checking. Systems are operated by state agencies and the Federal Bureau of Investigation's Bureau of Justice Statistics.

Background Investigation: A background investigation means the examination of elements of an individual's history to screen out individuals who, based on their past history or other relevant information, are found unsuitable for the position to which they have applied or in which they are employed. Background investigations may include personal interviews with the individual and other sources and credit, law enforcement, past residences, and employment checks. A background check may include a criminal history check with local law enforcement entities, the FBI, and/or a screening by the Terrorist Screening Center. In the NRC, a background check includes a criminal history check, verification of true identity, employment verification with suitable inquiry (includes education in lieu of employment and military service as employment), credit check, and character and reputation determination.

Cascading Event: Cascading event means an event whose occurrence causes another event.

Cleanup System: Cleanup system means a system used for continuously filtering and demineralizing a reactor coolant system to reduce contamination levels and to minimize corrosion.

Common Node: Common node means a junction or connection point (for example a computer, hub, switch, conduit) that is common to multiple systems or networks and that creates the potential for one event to cause multiple systems to fail.

Constructing or Construction Activities: Constructing or construction activities mean the tasks involved in building a facility, e.g., a nuclear power plant (NPP), that are performed at the location where the facility will be constructed and operated. At NPPs, these tasks include fabricating, erecting, integrating, and testing safety- and security-related structures, systems, and components (SSR-SSCs), and the installation of their foundations, including the placement of concrete.

Critical Infrastructures and Key Assets (CIs): Critical infrastructures and key assets (CI) mean systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[*] CI includes, but is not limited to; energy, transportation, water, public health, telecommunication, banking and finance facilities and systems; software systems and electronic data repositories; and iconic buildings.

Critical Node: Critical node means an element in a network whose damage or destruction has the potential to affect the efficiency or capacity of the entire system.

Delayed-Impact Threats: Delayed impact threat means threats whose consequences are intended to occur after a delay in time, in this report typically after construction is completed and the facility is in operation.

Design Basis Threat (DBT): Design basis threat means a profile of the type, composition, and capabilities of an adversary. The NRC and its licensees use the design-basis threat (DBT) as a basis for designing safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. The DBT is described in detail in Title 10, Section 73.1(a), of the Code of Federal Regulations [10 CFR 73.1(a)]. This term is applied to clearly identify for a licensee the required capability of its facility to withstand a threat. The NRC revised the DBT following 9/11.

Detection: Detection means measures used to discover, identify, and recognize security threats, and is part of an integrated defense-in-depth security strategy.

Deterrence: Deterrence means measures used to discourage undesirable or threatening actions and decrease their probability, for example by imposing barriers or increasing the likelihood of detection, and is part of an integrated defense-in-depth security strategy.

Devious Dan Program: Devious Dan programs mean programs designed to enhance safety and security by having randomly selected persons assigned to do things intentionally to test the performance of various aspects of the protection program.

Directing: Directing means exercising control over a work activity by an individual who is directly involved in the execution of the work and either makes technical decisions without subsequent technical review or is ultimately responsible for the correct performance.

Emergency Core Cooling Systems: Emergency core cooling systems (ECCS) mean reactor system components (pumps, valves, heat exchangers, tanks, and piping) that are specifically designed to remove residual heat from the reactor should the normal core cooling system fail or be disconnected.

FBI Criminal Record: An FBI criminal record is a listing of information on individuals collected and submitted with fingerprints by agencies with criminal justice responsibilities, such as descriptions of arrests, detentions, or other formal criminal charges and any dispositions of the charges, such as dismissal, acquittal, conviction, sentencing, correctional supervision, release, and

[*] Definition from the U.S. Patriot Act, Public Law 107.56 Sec. 1016(e)) as cited in Moteff and Parfomak (2004: 7).

expungement or sealing orders. The record includes the name of the agency that submitted the fingerprints to the FBI, the date of arrest, the arrest charge, and the disposition of the arrest, if known to the FBI.

Graded Approach: Graded approach means an approach in which protective measures are applied to or removed from individuals, areas, or tasks, or made more or less stringent to address different threat levels, depending upon the specific circumstances. Grading may be temporal, spatial, and/or task-based. Grading is often accompanied by an assessment of positions to categorize them according to their potential to affect public health and safety and the common defense and security and their potential to affect the integrity and efficiency of the organization or project. The process for identifying and categorizing "trust positions" within the federal government and its contractors is a component of a graded approach (see for example, 5 CFR 731.106).

Immediate Threats: Immediate threats are threats whose consequences occur immediately or within a short time interval and during the same life-cycle phase.

Insider Mitigation Program (IMP): An insider mitigation program is a program designed to prevent insiders from taking actions that jeopardize security by using measures to detect, deter, delay, and deny such actions, in part by monitoring their initial and continuing trustworthiness and reliability.

Intent: Intent means the desire or motivation of an adversary to attack a target and cause adverse consequences.

National Agency Check (NAC): [DHS] A NAC consists of records searches in the Office of Personnel Management Security/Suitability Investigations Index (SII); FBI Identification Division/Headquarters Investigation Files; FBI National Criminal History Fingerprint File; Defense Clearance and Investigations Index (DCII); and other sources, as necessary, to cover specific areas of a subject's background.

National Agency Check and Inquiries (NACI): [DHS] An NACI consists of a NAC, and employment, education, law enforcement agency, and personal reference checks. NACI is the minimum investigative standard for DHS employees.

Nuclear Steam Supply System: Nuclear steam supply system means the reactor, the reactor coolant pumps, steam generators for a pressurized water reactor, and associated piping in a nuclear power plant used to generate the steam needed to drive the turbine.

Peer Checking: Peer checking, synonymous with 2-person rules and buddy systems, means a system in which workers are assigned to work together and to check one another's work and behaviors.

Personnel Security: Personnel security means the requirements, programs, and measures implemented to provide reasonable assurance that the personnel involved in any phase of a facility or system will perform their assigned duties in a reliable and trustworthy manner, not impaired from any cause that adversely affects their ability to competently perform their duties, and are suitable, in terms of trustworthiness and reliability, to access the workplace and perform their assigned duties without constituting an unreasonable risk to the security of the site, the facility, its systems, or components.

Personnel Security Measures: Personnel security measures mean measures taken to provide reasonable assurance that the personnel involved in any of the life-cycle phases of a facility or system will perform their assigned duties in a reliable and trustworthy manner, not impaired by any cause that adversely affects their ability

to competently perform their duties, and are suitable, in terms of trustworthiness and reliability, to access the workplace and perform their assigned duties without constituting an unreasonable risk to the security of the site, the facility, its systems or components.

Physical Security: Physical security means that part of security concerned with physical measures designed to control access to assets or facilities and protect and safeguard assets or facilities from espionage, theft, fraud, or sabotage by a malevolent human adversary.

Prevention: Prevention means measures used to keep a threat from occurring. Prevention is one aspect of an integrated defense-in-depth security strategy.

Primary System: Primary system means the reactor coolant system that contains radioactively contaminated steam and/or water in a pressurized water reactor.

Protected Area: Protected area has the same meaning as in 10 CFR 73.2(g): An area encompassed by physical barriers and to which access is controlled.

Reactor Coolant System: Reactor coolant system means the system used to remove energy from the reactor core and transfer that energy either directly or indirectly to the steam turbine.

Red Team: Red team means a group of individuals engaged to take on the role of an adversary and to critique, identify weaknesses, and challenge the strategies or defenses of an organization, proposal, or system in order to identify vulnerabilities and ways to improve those strategies or defenses.

Risk: Risk is the product of the probability of an event occurring and the impact of the event; i.e., (probability) X (consequence). In vulnerability assessments, risk is a function of the severity of the consequences of an event, the likelihood of an adversary attack, and the likelihood of adversary success in causing a catastrophic event [DOJ 2002].

Risk Assessment: Risk assessment means the process of characterizing the nature of risks associated with a specific activity and evaluating them, including determining the probability of events and their potential impacts.

Sabotage: Sabotage means a deliberate act designed to damage, destroy, disable, or obstruct the normal operation of a system or facility.

Safety-Related Structures, Systems, and Components (SSCs): Safety-related structures, systems, and components (SSCs) mean, for the purposes of this report, those structures, systems, and components that are relied on to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in 10 CFR 50.34(a)(1).

Scientific Content Analysis (SCAN): Scientific Content Analysis, or scientific analysis of statements, is a variety of techniques used to detect deception by analyzing the statements made by an individual.

Secondary System: Secondary system means the steam generator tubes, steam turbine, condenser, and associated pipes, pumps, and heaters used to convert the heat energy of the reactor coolant system into mechanical energy for electrical generation. Most commonly used in reference to pressurized water reactors.

Security-Related SSCs: Security-related SSCs mean, for the purposes of this report, those structures, systems, and components that are relied upon to implement the physical security and safeguards contingency plans (for example, that are required under Part 73 of this chapter if the licensee is a construction permit applicant or holder or an early site permit holder, as described in Sec. 26.3(c)(3) through (c)(5), respectively, or are included in the licensee's application if the licensee is a combined license applicant or holder, as described in Sec. 26.3(c)(1) and (c)(2), respectively).

Selection: Selection means establishing qualifying criteria and applying a process for identifying and selecting personnel who meet those criteria and rejecting those who do not.

Separate/Greenfield Sites: Separate/greenfield sites mean, for the purposes of this report, sites on which the facility under construction is the only/first facility, i.e., without an existing operating facility of the same type.

Shared Sites: Shared sites mean construction sites at which an operating facility is already present and the facility under construction is being built proximate to or interspersed within the operating facility

Steam Generator: Steam generator means the heat exchanger used in some reactor designs to transfer heat from the primary (reactor coolant) system to the secondary (steam) system. This design permits heat exchange with little or no contamination of the secondary system equipment.

Suitable: Suitable means a determination, based on an individual's identifiable character traits and conduct, that the individual is likely to be able to carry out the duties under consideration with appropriate integrity, efficiency, and effectiveness and is suitable, in terms of trustworthiness and reliability, to access the workplace and perform their assigned duties without constituting an unreasonable risk to the security of the site, the facility, its systems, or components.

Threat Assessment: Threat assessment is the process of formally evaluating the nature, likelihood, and consequences of acts or events that could place assets or safety at risk and is typically conducted in conjunction with vulnerability and risk assessments.

Threat Capability: Threat capability means the ability and capacity of an adversary to attack and cause adverse consequences.

Threat Pathway: Threat pathway means the sequences of events/actions through which a threat results in a consequence (see Nishimura et al. 2004).

Vulnerability: Vulnerability means the attributes of a system (e.g., physical, technical, organizational, social, cultural) that can be exploited by an adversary to harm or damage the system and lead to adverse consequences or that allow errors or inattention to harm or damage the system and lead to adverse consequences.

Vulnerability Assessment: Vulnerability assessment means the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities of a system and is typically conducted in conjunction with a risk and threat assessment and involves identifying, characterizing, and prioritizing assets to be protected.

LIST OF ACRONYMS AND ABBREVIATIONS

AFIS – Automated Fingerprint Identification System
CI – Critical infrastructure
COL – Combined Construction and Operating License
CRS – Congressional Research Service
DBT – Design Basis Threat
DHS – U.S. Department of Homeland Security
DOE – U.S. Department of Energy
DOJ – U.S. Department of Justice
ESP – Early Site Permit
FBI – Federal Bureau of Investigation
FR – *Federal Register*
FIPS 201 Investigative Mandate – Federal Information Processing Standards 201
FIRS – Fingerprint Identification Records System
Form I-9 – Employment Eligibility Verification Form
HHS – U.S. Department of Health and Human Services
IAFIS – Integrated Automated Fingerprint Identification System
IDENT – Automated Biometric Identification System
INEEL – Idaho National Energy and Environmental Laboratory
ITAAC -- Inspections, tests, analyses, and acceptance criteria
NACI – National Agency Check with Written Inquiries
NCIC – National Crime Information Center
NEI – Nuclear Energy Institute
NIST – The National Institute of Standards and Technology
NPP – Nuclear power plant
NRC – U.S. Nuclear Regulatory Commission
OMB – U.S. Office of Management and Budget
PNNL – Pacific Northwest National Laboratory
QA/QC – Quality Assurance/Quality Control
SCAN – Scientific Content Analysis
SSR-SSCs – Safety- and security- related structures, systems, and components
TSC – Terrorist Screening Center
TISP – The Infrastructure Security Partnership
TSRS -- Terrorist Screening Records System
TTIC – Terrorist Threat Integration Center

1. Introduction

1.1 Purpose and Scope

Nuclear power plants (NPPs) constitute an important element of the U.S critical infrastructure (CI), with over 100 operating units supplying approximately 20 percent of U.S. electrical production. In addition to this substantial base of operating facilities, the U.S. is anticipating a potential resurgence of NPP construction. As of May 2008, the U.S. Nuclear Regulatory Commission (NRC), the agency responsible for licensing and regulating NPPs, was expecting to receive over 20 applications for combined construction and operating licenses (COLs) for new NPPs by the end of 2010. This expectation has made addressing security for new facilities and security during NPP construction a particularly urgent concern for the NRC.

The NRC's stated mission is to "license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment." The NRC's *FY 2008-2013 Strategic Plan* identifies twin goals of safety and security, and notes that "[m]aintaining a stable and predictable security environment is one of the NRC's major continuing challenges. It requires ensuring adequate security without unduly limiting the beneficial use of radioactive materials." (U.S. NRC. NUREG-1614, Vol. 4:12). The previous *Strategic Plan* had stated that "[t]he primary challenge facing the NRC in the coming years is to emerge from the period of uncertainty in post-September 11 security requirements; determine what long-term security provisions are necessary; and revise its regulations, orders, and internal procedures as necessary to ensure public health and safety and the common defense and security in an elevated threat environment" (U.S. NRC NUREG-1614, Vol. 3).

These challenges still exist. The new wave of applications follows a nearly complete hiatus in building new nuclear power plants in the United States following the Three Mile Island accident in 1979. Consequently, there is little recent U.S. experience with the construction of NPPs to draw upon to determine what security measures are needed during NPP construction.[1,2,3] The purpose of this report is to examine the technical basis for personnel security requirements during the construction phase of new NPPs within the post-2001security context. For this study, personnel security requirements are defined as requirements for personnel access authorization, fitness-for-duty, and insider threat mitigation programs and measures.

---

[1] Several plants already under construction continued to be built. For example, construction on TVA's Watts-Bar 1 reactor started in 1973, but was completed in 1996 and connected to the grid that same year. For more information, see: http://www.eia.doe.gov/cneaf/nuclear/page/nuc_reactors/operational.xls.

[2] The National Energy Policy (NEP) of 2001, the U.S. Department of Energy's Nuclear Power 2010 program that began in 2002, the Energy Policy Act (EPACT) of 2005, and the Global Nuclear Energy Partnership announced in 2006, have encouraged this revival. The federal government has committed $6 billion in tax credits as incentives for the first companies to build new plants. The Department of Energy has also promised $260 million to offset plant design and application costs of NuStart, a consortium of nuclear operators aiming to demonstrate the process for application and approval for an NRC combined construction and operating license (COL).

[3] Building on past experience, the NRC established a new licensing process in 1989, contained in 10 CFR Part 52, to ensure safety issues would be moved to the forefront in three early life-cycle phases: approval of standard designs, early site permits, and the combined construction and operating license. This new licensing process is designed to help promote a more comprehensive life-cycle view of safety issues.

Literature on security and safety planning emphasizes the importance of systematically assessing threats (including evaluation of both the intentions and capabilities of those posing the threat), vulnerabilities, and risks as the basis for determining the need for, design of, and value from protective measures (see next chapter for references). This project's scope did not include conducting threat, vulnerability, or risk assessments. Rather, our mandate was to draw upon the open literature and experts who have conducted or are familiar with such assessments and to summarize conclusions from these sources about threats, vulnerabilities, and risks, and, generally, how they would likely be manifest, at a level of detail consistent with public discussion. Consultation with these experts was instrumental in informing the framework for and approach to the analysis.

The project team examined the implications of the following threat characteristics and sources:

- Immediate and delayed-impact threats;[4]
- Intentional and inadvertently-caused threats;
- Threats caused by insiders, outsiders, and insiders colluding with outsiders.

To fulfill its mandate, the project team designed an exploratory investigation to answer four questions:

1. To what extent do threats of concern exist during the construction phase of NPPs?
2. What are current, typical construction practices and are they adequate to protect against these potential threats?
3. What, if any, enhanced protective measures do experts recommend?
4. Are personnel security requirements warranted and/or justifiable in terms of costs and benefits? Are the recommended protective measures in use at other CI facilities under construction?

To answer these questions in the absence of recent U.S. NPP construction activity, we:

1. consulted with experts and reviewed the open literature[5] about threats, recommended analytical and conceptual approaches to construction security, and obtained views about the need for, utility of, and cost-benefit balance of particular security measures during CI construction;
2. examined how other U.S. CI sectors are addressing security, particularly personnel security, during facility construction to determine the nature and extent of standard security practices across CI sectors and to understand how knowledgeable individuals in these different sectors are thinking about threats and construction security in the post-2001 context, what analytical approach(es)

[4] Delayed-impact threats are threats whose impact is designed to occur after a delay in time, typically after construction is completed and the facility is in operation.

[5] Because the report was to remain unclassified, the team reviewed only open source literature and secondary materials. These included media coverage, professional journals and technical reports, and peer-reviewed articles. The bibliography in Chapter 8 lists the materials reviewed.

they use and recommend, and what conclusions they reach about the basis for security requirements for different types of CI facilities and life-cycle phases;

3. reviewed available information on security issues experienced during the initial NPP construction cycle in the U.S., by other nuclear facilities, and by other CI sectors, and consulted with experts about whether these issues were likely to arise in upcoming NPP construction projects;
4. reviewed the major federal initiatives undertaken following the 2001 terrorist attacks to identify changes in the policies, requirements, and available technologies for U.S. CI protection and security, the rationale for these changes, recommended analytical approaches to evaluate threats and vulnerabilities, and the standards and expectations of CI stakeholders that might affect NPPs under construction; and
5. participated in a workshop hosted by The Infrastructure Security Partnership (TISP) on security during CI construction, in which NPPs under construction were addressed as a particular case in point.[6]

Appendix A lists the experts consulted in the course of this study. They included individuals knowledgeable about the nuclear industry and safeguards; physical security and protection of critical infrastructure; terrorism and counterterrorism; counterintelligence; cyber security; supply chain security; construction planning and management; construction security program development, implementation, and management; personnel security; threat and vulnerability assessment; construction-phase quality assurance; construction safety; and federal initiatives to enhance homeland security and protect U.S. infrastructure, especially from terrorist attacks. The discussions focused on the individuals' (1) views about threats; (2) descriptions of the security measures employed during construction for the projects and sectors with which they were familiar; (3) judgment about the need for enhanced security measures during construction for those projects and in those sectors; (4) opinions about the relative desirability of various types of CI as targets during the construction phase; and (5) assessment of the relative importance of security – particularly personnel security – at NPPs under construction. An outline of the information sought is included in the discussion guide presented in Appendix A.2.

The project team obtained information about current construction security practices for the following CI sectors, key assets, and facilities with special security concerns:[7]

- Aerospace construction facilities;
- Airports;
- Banks and financial data centers;
- Bridges/tunnels;

[6] TISP, a public private partnership established in 2001, focuses on improving the resilience of U.S. critical infrastructure and has a membership with broad expertise in security, emergency preparedness, and response for a wide range of industrial and governmental sectors.

[7] It should be noted that to conform with Office of Management and Budget (OMB) requirements, these consultations were limited in number and did not constitute a survey in which each individual was asked the same questions. Rather the project team used the discussion guide as a basis for providing those consulted with information about the scope and purpose of the study and for organizing the information provided during the consultation. In addition, because the project team inquiry sought to obtain information about a wide range of CI facilities, only a few individuals (often only one) in each sector were consulted.

- Casinos;
- Chemical plants;
- Embassies;
- High-rise commercial buildings;
- Liquefied natural gas facilities;
- Major governmental buildings, including those dealing with classified information;
- Military installations;
- Nuclear power plants and other nuclear facilities;
- Refineries and off-shore oil drilling platforms and infrastructure; and
- Seaports.

The project team also reviewed a variety of literature and secondary source materials. A bibliography of these materials is in Chapter 8.

An important objective of this project was to develop an analytical framework and approach that reflected the advice and experience of experts from a variety of disciplines and topical areas. The approach needed to be sufficiently comprehensive to assure that we did not overlook important considerations or issues. Although the scope of the project did not include assessments of the threats, vulnerabilities, or risks to nuclear power plants, information about them was essential to answering the questions the project was to address. To obtain this information, we drew upon experts who had conducted or were familiar with such assessments. This report contains only information available in the open literature and available to the public. Consequently, the discussion of threats, vulnerabilities, and risks is necessarily general and conclusionary rather than detailed and specific.

1.2 Limitations and Caveats

Following the attacks of 2001, the immediate priority in the U.S. was to secure and protect existing facilities and, to a lesser extent, to design secure facilities for the future. Much effort was directed toward defining, identifying, inventorying, and prioritizing U.S. CI facilities and systems and securing those considered to be the most critical and high-risk targets. In many ways the country's CI and key assets – including but not limited to energy, transportation, water, public health, telecommunication systems, banking and finance, software systems and electronic data repositories, and iconic buildings – have been made less vulnerable as a consequence of these efforts. This progress notwithstanding, there is widespread agreement that the information to characterize current practice – security measures in use – for operating facilities is still under development. As noted by the Defense Science Board Task Force On Critical Infrastructure:

> "Assessments are needed to better understand our progress to date and to assure that further investments will be wisely made…[T]he predominant reliance on guns, guards, and gates for protection of facilities and valuable assets, although expedient, is an expensive approach….[and] most actions have been taken by individual facility and infrastructure owners in a relative vacuum from others in the same or similar situations. Best practices are not widely known and good enough [is] not well understood" (Defense Science

Board 2007:1).

Even fewer data are available about current practices for CI facilities during construction. The project team found little description of security measures employed during the construction phase of projects in the literature or secondary materials. Indeed, many people consulted for this project commented that they had not previously focused on questions of security during the construction phase of projects in their sectors. To date, they reported, the overwhelming focus has been on protecting existing facilities and systems, developing more effective ways to protect them, and designing future facilities and systems that are less vulnerable to threats. Facilities requiring protection from espionage, such as U.S. embassies and buildings in which classified materials and discussions are held, were the principal exception. Experts reported that rigorous security measures are typically applied to these facilities from the earliest planning phases until their decommissioning or demolition. Consequently, the information about security practices and potential threats presented in this report is best viewed as a preliminary and illustrative characterization of construction security practices in CI sectors and the types of threats they may need to address, given the limited sample of facilities and number of informal discussions upon which it is based.

In addition, because the project team was asking the experts to describe practices in use across CI sectors or types of facilities, using specific facility types only as reference points, the information presented in this report is primarily at an overview level of specificity. Where the team obtained more specific information about particular practices, for example about the use of fingerprinting and psychological assessment, it is included in the report. Although the project team was able to clarify that a wide range of personnel security measures are in use at U.S. CI facilities during construction and that, absent regulatory requirements or constraining site conditions, few have become established as industry standards, the experts emphasized that this could change if greater attention were directed to the topic of security during construction. They thought this could occur either through the efforts of the Federal government, organizations such as TISP, or as a consequence of another terrorist event.

An important caveat concerning this report is that it does not reflect a specific threat, vulnerability, or risk assessment for any CI sector or facility. Consequently, the intent is to provide a framework for, and an initial articulation of, experts' opinions and open literature information about (a) the possibility of threats during the construction of U.S. CI in general, and NPPs in particular; (b) the general pathways by which those potential threats might be manifest; and (c) the types of protective measures and security strategies that therefore might warrant detailed evaluation for application during CI facility construction.

1.3 Structure of the Report

The report has eight chapters and three appendices. Following this introduction, Chapter 2 describes the analytical approach and framework used in this study. Chapter 3 presents information about facility characteristics and characteristics of the construction phase of a facility's life cycle important to an assessment of construction security issues and considerations. Chapter 4 discusses threats to CI facilities during construction and summarizes the experts' views about potential threats. Chapter 5 describes types of protective measures, summarizes the benchmarking information

about standard protective measures in use for U.S. CI facilities during construction, and presents experts' views about their effectiveness and benefit-cost balance. Chapter 6 presents the conclusions of the study concerning construction security strategy and the basis for personnel security requirements during NPP construction and Chapter 7 suggests potential next steps. Chapter 8 presents a bibliography that includes the references cited in the report.

Appendix A presents the list of individuals consulted for the project, the individuals who participated in the TISP workshop, and the discussion guide used by the project team to organize the discussions and the information obtained from them. Appendix B provides an overview of recent or on-going Federal initiatives to enhance the security and resilience of U.S. CI, many of which have the potential to change the regulatory, technological, and acceptability landscape in the U.S. concerning personnel security measures. Appendix C presents a summary of the TISP workshop, including copies of the materials distributed to workshop participants. The workshop discussions informed the substance of the report.

2. The Study's Analytical Approach to Construction Security

2.1 Overview of the Chapter

This chapter describes the analytic approach taken in this study. It starts by briefly describing the systems-based life-cycle approach with a cost-benefit orientation that provides the overall framework and analytic perspective for the study and an anchor for the study's focus on the construction phase of U.S. CI facilities, particularly NPPs. It then presents an overview of a vulnerability assessment framework. This framework guided this inquiry and its six elements provide the structure of the report.[8] The chapter concludes with a definition and discussion of personnel security, the other particular focus of this study.

2.2 The Broad Perspective: A Systems-Based Life-Cycle Approach with Cost-Benefit Orientation

Systems-Based Life-Cycle Approach

The experts consulted during the initial stage of this project advised the project team that a study of security during the construction phase of CI, and particularly NPPs, should take a systems-based life-cycle approach. They recommended a systems perspective because of the technical and organizational complexity of NPPs and the challenges of addressing a construction process that requires integration of the numerous complex and inter-related systems that comprise an NPP. They pointed out that planning for and managing the construction process of an NPP requires attention to each of the plant's systems (for example the nuclear island, reactor cooling, steam generator, electrical, turbine, condenser, emergency, and safety systems), and, often, to the subsystems that make up those systems. They noted that assessing security needs and evaluating the effectiveness of potential security measures requires analysis of vulnerabilities and consequences at both individual and integrated system levels. Information about when and how those systems will be built and where they will be located on the site is needed to do this effectively. They argued that a systems-based approach is important to provide an appropriate conceptual perspective, even if the project does not require analysis at the individual system level, and that it encourages a systematic, comprehensive, and integrated approach to security. They also pointed out that regulators often structure safety and security regulations to address particular systems or the integration of systems. The literature reinforced this expert view (see, for example, Aguilar 1973; IAEA 2000; Holmgren 2005; Mannisto 2005; McDonald 2001; Patterson and Apostolakis 2007; Stasinopoulos et al. 2009; U.S. NRC 2006d).

The experts also pointed out that a systems-based approach would facilitate identification of aspects of the construction process important to security but that extend beyond the immediate construction site. They noted that a systems-based approach would help structure and provide a basis for considering the security implications of the streams of material objects and workers coming onto the construction site to build the various plant systems. It would also help frame consideration of how these streams are

[8] Two of these six elements are analysis of threats and analysis of risks and vulnerabilities remaining after applying standard protective measures to address those threats. The discussion of these two elements is combined in Chapter 4.

organized, selected, screened, and monitored, and thereby help identify and evaluate potential threat pathways and protective options.

Although this project focuses on one phase of the life cycle, the construction phase, both the experts consulted and the literature reviewed emphasized the value of a life-cycle perspective. A life-cycle perspective encourages consideration of the temporal progression of project-related activities and facilitates consideration of impacts that carry over from one life-cycle phase to another. It also allows consideration, as in this project, of distinctive regulatory implications of different life-cycle phases.

The experts noted that inattention to adequate security measures during early life-cycle phases could threaten the security of the facility during subsequent phases. To illustrate this point, they described how failure to impose document control on early design and planning documents could lead to their distribution or exposure to unauthorized personnel (which could be either on-site personnel or personnel elsewhere in the supply chain). Likewise, they emphasized that decisions made in one phase could impact, or be impacted by, decisions made in another phase. For example, a security breach during the construction phase could introduce a threat whose consequences occur during facility operation. Similarly, decisions made during reactor design, including supply chain and workforce decisions, could impact plant design, construction, operation, and decommissioning.

While conceding that most CI facility planners have generally not used a life-cycle approach to CI project planning in the past, the experts did note that this approach is being used in some sectors. For example, they cited its use in planning for some high-security government facilities and, to a somewhat lesser extent, for casinos. Several experts also noted that some security consulting firms are starting to provide integrated security planning and implementation services to construction projects. These firms are applying a life-cycle perspective and vulnerability assessment process to facility security planning along the lines of the planning approach described here.

Several of the experts recounted actual examples of plant design and siting decisions that did not adequately take security considerations of later life-cycle phases into account, thus affecting the protective measures needed in subsequent phases. Examples included cooling water intake and outfalls that were located without consideration of the need to protect them over the course of the facility's life cycle. These design decisions significantly increased both the facility's potential vulnerabilities and its long-term security program costs, as additional security personnel and equipment had to be deployed throughout subsequent life-cycle phases. They also cited personal experience with expensive retrofit requirements needed to meet security specifications that were either not clearly delineated before the early life-cycle phases were complete, or were not adequately reflected in the planning and design process.

NPPs have a life cycle that is typically delineated into reactor design, plant siting, plant design, construction (or build), operation, and decommissioning phases. Each of these phases can be further disaggregated into sub-phases to articulate the major activities and progression of system development within that phase. This disaggregation can be important to the analysis of security needs and effectiveness as it provides threat analysts and security planners greater specificity about, for example, the timing and

location of particular steps in the process, the number and types of personnel involved, and duties being performed.

The transition from one life-cycle phase or sub-phase to another may be more or less distinct. Different systems may transition through the life-cycle phases on different schedules. As with their recommendation to apply a systems-based approach, the experts emphasized that a life-cycle approach would provide considerable conceptual value to the study, even though a full life-cycle examination was beyond the scope of the effort. Figure 2.1 illustrates the systems-based life-cycle approach and Appendix C.4 further discusses this approach.[9]

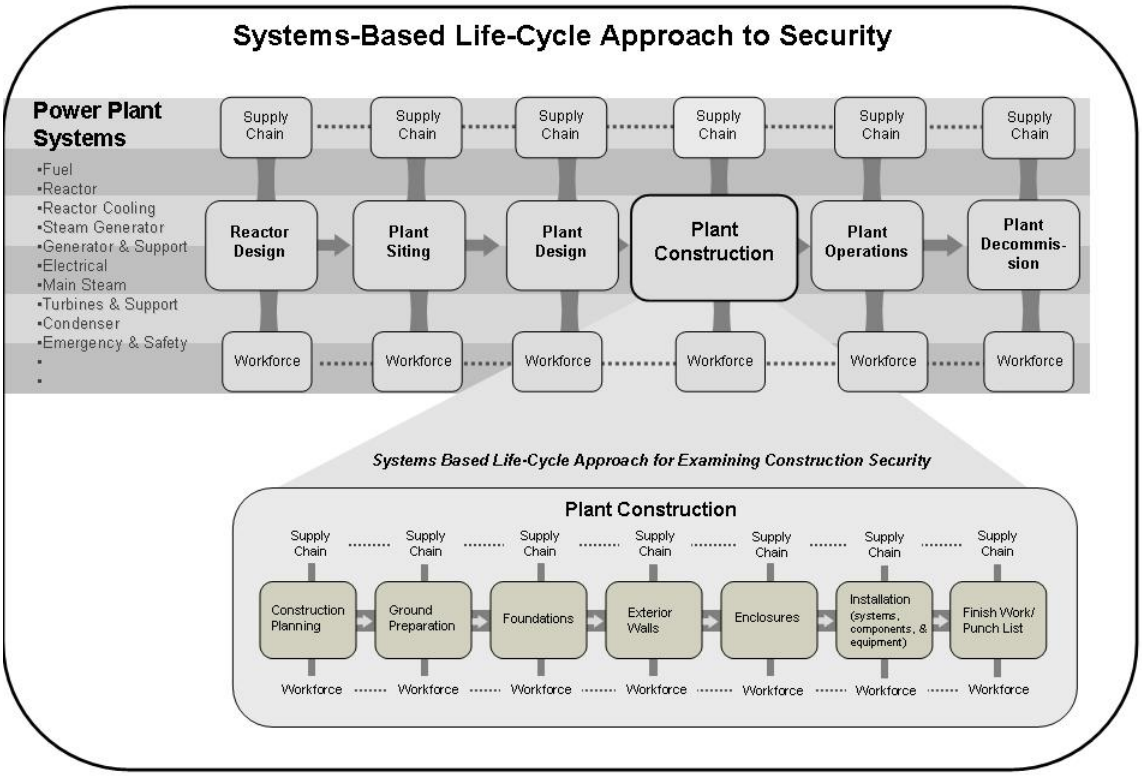


Figure 2.1 Multi-Level Systems-Based Life-Cycle Approach for Examining Security during Construction

Cost-Benefit Orientation

The experts consulted for this project consistently reflected an embedded cost-benefit orientation in their discussions about the need for and value of security measures during the construction of NPPs and in other CI sectors. When asked to validate the project team's proposed analytical approach, they uniformly confirmed that a cost-benefit orientation was essential for an analytical framework addressing regulatory alternatives and construction projects. They emphasized that any recommendations for enhanced security requirements must be based on demonstration of need, effectiveness, and a positive benefit-cost balance. During discussion about the proposed approach, several

[9] The systems represented in Figure 2.1 are for illustration and are not intended to be complete.

of the experts expressed the opinion that, in addition to potentially improving security, a systems-based life-cycle approach is also likely to provide more cost effective security than would a fragmented, phase-by-phase approach. In part, this is because it would encourage consideration of the security issues of each life-cycle phase early in the design and planning process, thereby helping planners anticipate and eliminate potential conflicts between security and other performance objectives at each phase of the facility's life cycle.

Several of those consulted about the framework pointed out that a benefit-cost analysis is required before any Federal regulation can be imposed. They cautioned that true cost-benefit analyses require information about (a) the direct and indirect costs of implementing the alternative and (b) the value of the effects that result from its implementation. Both of these are typically difficult and relatively expensive to obtain. Several of the experts who had experience designing and implementing security programs also emphasized that individuals with different perspectives on risk and different roles in risk management tend to value costs and benefits differently, thus making the analysis even more complex. However, they suggested that, in some instances, the cost-benefit analyses of security measures employed at operating facilities might provide a basis for estimating the costs and benefits of similar measures applied during the construction phase.

Based on this advice, review of the literature (see for example, Garcia 2006 and 2001;), and their own experience, the project team concluded that the systems-based life-cycle analytical approach should include a cost-benefit orientation, even if costs and benefits can be considered only at a conceptual and general level. Even a cursory analysis of costs and benefits has the potential to provide important insights about need, feasibility, and the relative cost-effectiveness ranking of alternatives. Given the investigative nature of this study, the study addresses benefit-cost balance primarily as a factor to be considered; few alternative measures were specified in sufficient detail to provide a basis for collecting information to quantify benefits and costs.

2.3 Vulnerability Assessment Framework

Following the terrorist attacks of 2001, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (U.S. President 2003:viii) identified three general effects that terrorists try to achieve by targeting critical infrastructure. These are: (1) direct infrastructure effects – cascading disruption or arrest of CI functions; (2) indirect infrastructure effects – cascading disruption and financial consequences for government, society, and economy from public and private sector reactions to an attack; and (3) exploitation of infrastructure – using elements of a particular infrastructure to disrupt or destroy another target. These effects add to the more usual security concerns of large-scale construction projects: theft, fraud, and sabotage. Following 2001, a number of books and articles have examined the vulnerability of U.S. critical infrastructure (see for example, Bennett 2007; Forest 2006; Lewis 2006; U.S. Department of Justice (DOJ) 2002). In this literature, there is general agreement that the size, nature, and vulnerability of a CI determine, in part, its desirability as a potential terrorist target. The assessment of vulnerabilities and design of protective measures are key objectives of the national strategy on critical infrastructure protection. The vulnerability assessment framework developed through this national effort is applicable to the current study, though at a conceptual rather than detailed level, given the scope of

the project (see for example Acherman et al. 2006; Advisory Panel to Assess Domestic Response Capabilities 2002; Bennett 2007; Cameron 1999; Fein et al. 1995; Garcia 2006 and 2001; Landoll 2006; Lewis 2006; NERC 2002 a-e; Renfroe and Smith 2008; U.S. Department of Energy (DOE) 2002; U.S. DOJ 2002).

Within the broad systems-based life-cycle approach, the project team therefore applied a general vulnerability assessment framework to structure the inquiry and analysis and address the issue of CI security during construction. The vulnerability assessment framework consists of the following six interactive and iterative elements, as shown in Figure 2.2:

1. Characteristics of the facility and the construction life-cycle phase;
2. Threats;
3. Standard protective measures;
4. Vulnerabilities and risks;
5. Potential enhanced protective measures; and
6. Construction-phase security strategy and rationale.

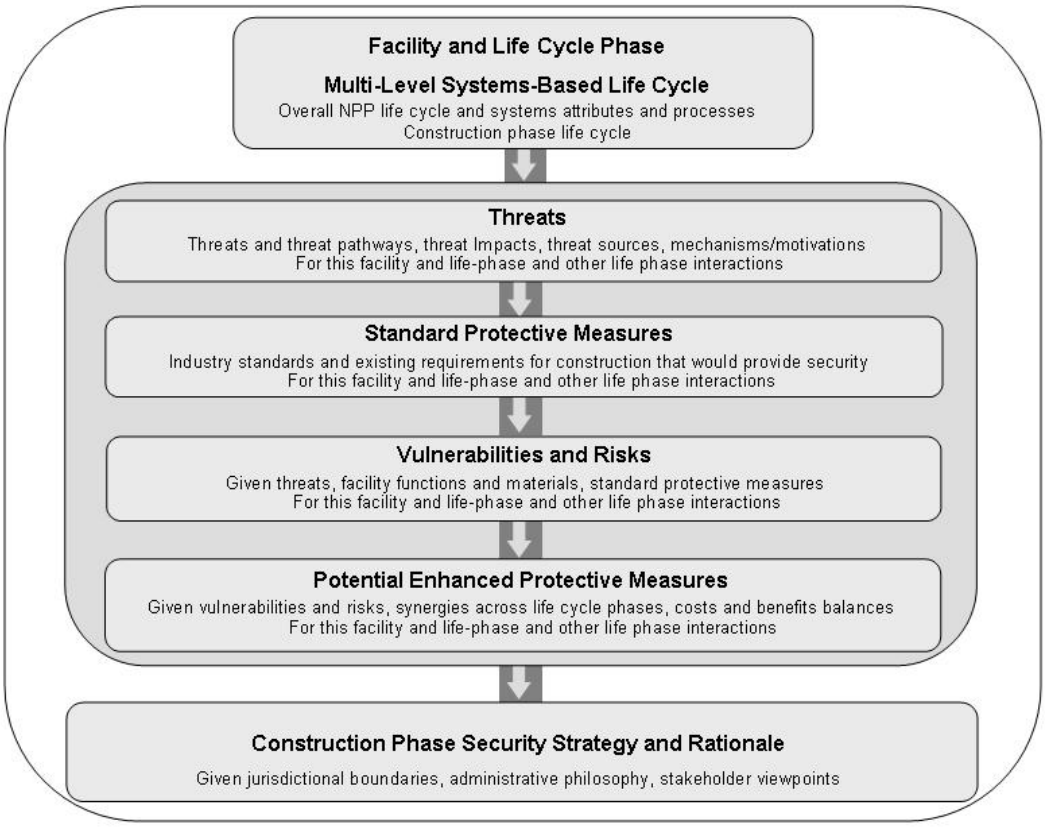


Figure 2.2 Vulnerability Assessment Framework

The experts consulted for the study emphasized the importance of understanding how attributes of the facility affect its desirability as a target, its vulnerabilities, and the evaluation of potential protective strategies. They identified (1) the ownership and

purpose of the facility (as a public-good or private-sector investment and asset); (2) the function of the facility (as a component or node of the nation's critical infrastructure); and (3) the potential for the facility to constitute a threat to public health and safety and common security as particularly important attributes to consider. This is consistent with the emphasis placed on these attributes in the U.S. Department of Homeland Security (DHS) strategy for assessing and protecting U.S. critical infrastructure (U.S. DHS 2002).

2.4 Personnel Security Focus

Within the broader question of security during the construction phase of U.S. NPPs and other CIs, the study's mandate was to focus on issues of personnel security.[10] These issues include the role of personnel in threats to security during construction, the pathways by which personnel could create such threats, the ways personnel could enhance or create vulnerabilities to those threats, and the protective measures effective in preventing, deterring, detecting, and mitigating them.

This study's focus is on security during construction: whether it is important, and how workers and other people might jeopardize it. In attempting to articulate why security is (or is not) important during the construction phase of CIs, the experts consulted emphasized three main reasons why security at NPPs and some other CIs is important. First, breaches of security can jeopardize facility safety, which in turn can jeopardize the safety of not only workers at the site but also, potentially, surrounding populations.[11] Second, for some facilities such as NPPs, security is essential to protect the facility, its contents, and associated technologies and information from being captured or acquired by an adversary. Third, security measures help to ensure continued functionality through protection of the facility and the assets it represents from damage or destruction.

The risk and vulnerability literature typically distinguishes between safety and security threats based on intent. Security programs are normally designated as addressing intentional threats and safety programs designated as addressing non-intentional (accidental/force-of-nature) threats (Bennett 2007; Forest 2006; Lewis 2006; U.S. DOJ 2002). However, for CI facilities such as NPPs, this distinction is not as clear. Individuals without independent malicious intent can be recruited/coerced into assisting malicious insiders or outsiders and may jeopardize security inadvertently. An individual failing to do his or her job correctly or being inattentive to signs of threat or vulnerability are simple examples of an inadvertent threat.[12]

The experts emphasized the importance of considering all the pathways by which personnel with access to or working at a site could threaten safety and security, either

[10] For this study, we define personnel security as the requirements, programs, and measures implemented to provide reasonable assurance that the personnel involved in any of the life-cycle phases of a facility or system will perform their assigned duties in a reliable and trustworthy manner, will not be impaired from any cause that adversely affects their ability to competently perform duties pertinent to safety or security, and are suitable, in terms of trustworthiness and reliability, to access the workplace and perform their assigned duties without constituting an unreasonable risk to the safety and security of the site, the facility, its systems, or components.

[11] Chapter 3 provides a more detailed discussion of this attribute of some CI facilities.

[12] The literature on information system security and protection and personnel security consistently reflects the need to consider both inadvertent and intentional actions by personnel (Anderson 1999; Anderson et al. 2002; INEEL 2004; Wilson et al. 2005). Hapgood (2008) also discusses the intersection between safety and security.

intentionally or inadvertently, as well as the importance of including measures to address both intentional and inadvertent threats in the analysis. The inclusion of measures to address intentional as well as inadvertent behaviors is consistent with recent guidelines on personnel security, particularly those designed to address information security or to qualify personnel for accessing classified or sensitive materials (Crow 2004; Kraemer and Carayon 2007; INEEL 2004; U.S. Department of Defense (DOD) 1999; Ward et al. 2006).

Personnel security is concerned with individuals' trustworthiness and reliability and it addresses both unintentional and intentional actions. Consideration must be given to personnel reliability and fitness for duty (to address inadvertent errors, lapses, or failures to reliably and competently perform assigned duties) as well as to intentional actions taken to harm or degrade some aspect of the CI. Consequently, the personnel security focus of this study includes consideration of both (a) the pathways by which malicious adversaries can threaten the security of a CI facility during construction and its security and safe operation once completed; and (b) the pathways by which other personnel can intentionally or unintentionally increase the vulnerability of the facility to such threats or magnify their potential consequences. These concerns overlap, as illustrated in Figure 2.3.[13]

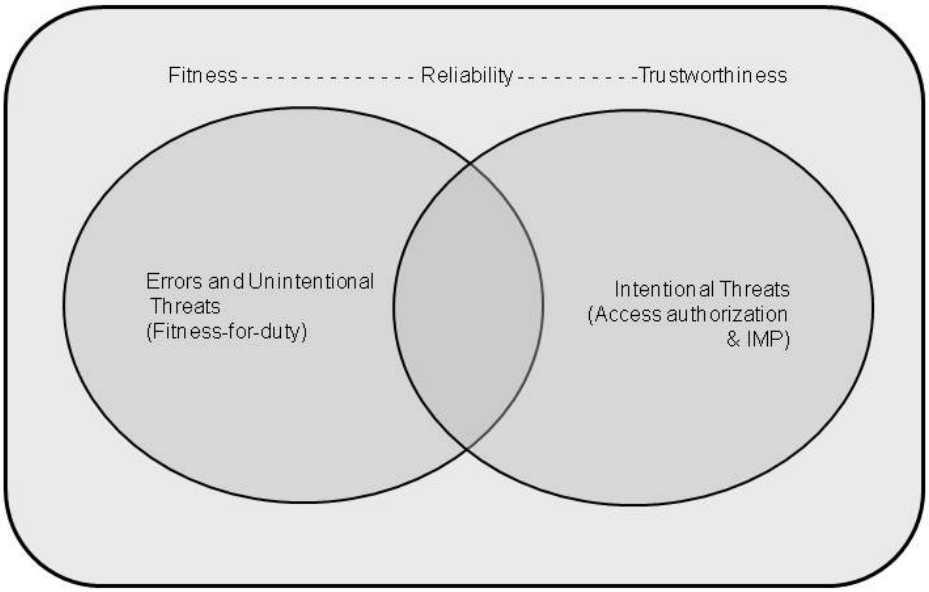


Figure 2.3 Personnel Security Framework

The systems-based life-cycle approach, combined with the vulnerability assessment framework, facilitates consideration of where, when, and by whom threats and vulnerabilities may occur, and therefore, where, when, and for whom protective personnel security measures may be warranted. Questions of timing and targeting are particularly pertinent and complex during the construction phase, given the dramatic

[13] However, the study did not analyze personnel during construction from a safety perspective to identify what protective measures might be appropriate to achieve safety goals separate from security considerations.

differences in the number, characteristics, and duties of the personnel on-site (and in the supply chain) at different sub-phases of construction and the changing character of structures, systems, and components over the sub-phases of the construction process.

This study focused primarily on the construction site and personnel working on-site. However, the experts consulted by the project team strongly recommended that on-site personnel security considerations should be placed within the broader framework of construction security threats and protection measures. They recommended addressing off-site personnel and their potential to threaten the security of the facility under construction as well. The discussion of potential next steps in Chapter 8 and the results of the workshop hosted by The Infrastructure Security Partnership summarized in Appendix C reflect these recommendations.

3. Characteristics of CI Facilities and the Construction Life Cycle Phase

3.1 Overview of the Chapter

This chapter summarizes the information that experts and the literature identified as important about the attributes of CI facilities and the construction phase of their life cycle with regard to construction security considerations. The significance of a CI facility as a national or technological icon or symbol, its function as an asset in the CI system, and its potential as a threat/hazard to public health and safety are among the attributes of CIs that influence its desirability as a potential terrorist target and affect the extent, nature, and distribution of impacts that could result from a terrorist attack. Other attributes that affect security strategy and regulation include a facility's ownership and its role as a public good and private investment.

The construction phase of a CI facility has its own cycle of sub-phases that often involves different workers, companies, and activities, and that affect different facility systems differently. This complexity complicates decisions about when, where, and what protection is warranted and effective. This chapter summarizes expert views about the attributes of the construction phase life cycle that present particular security challenges, such as the volume, diversity, and temporary nature of individuals, vehicles, and materials entering and exiting the construction site. It also discusses the attributes of facility location and site characteristics that experts identified as most influential in security strategy and practice, for example, proximity to an operating facility, location within a site that already requires personnel security measures, and access routes/pathways to the site. Chapter 3 also discusses expert views about the importance of addressing the facility's interface with off-site workers, suppliers, and systems, which tend to be especially diverse and frequent during the construction phase. Although extending beyond the construction site itself, the experts emphasized the importance of considering potential threat pathways via these interfaces.

3.2 CI Facilities as Assets and Threats/Hazards

The terrorist attacks of 2001 precipitated a major effort in the U.S. to inventory, characterize, and prioritize CI and key assets from a homeland security perspective and to develop more effective threat, vulnerability, and risk assessment methodologies to assist in this process.[14] One outcome of this effort was recognition that CIs and other key assets need to be evaluated both as:

- Assets, based on their function in the critical infrastructure system; and
- Potential threats/hazards, based on their potential to cause harm to public health and safety.

These two attributes affect these facilities' potential attractiveness as targets, as discussed in Chapter 4. They also indicate that both safety and security need to be considered when threat pathways and protective measures are assessed. NPPs, chemical plants, water treatment facilities, and dams are examples of CIs and other key assets that fall into the category of potential threats as well as CI assets.

[14] See Appendix B for a summary of some of these initiatives, primarily led by Presidential directives and the newly established Department of Homeland Security (DHS).

The potential for a CI to be a threat to public health and safety affects the analysis of threats and protective measures. Facilities that pose potential threats from terrorist attacks typically pose similar threats from accidents. Consequently, such facilities, and the agencies that regulate them, usually have a focus on safety and have implemented measures to reduce the potential for accidents. The potential for security breaches to jeopardize the safe operation of these types of CI creates an intersection between safety and security, and the strategies and measures used to achieve them. This intersection affects consideration of security during the construction of these facilities in two principal ways:

- It creates the potential for delayed impact threats, i.e., threats whose consequences are designed to occur after a delay in time, typically after construction is completed and the facility is in operation; and
- It requires consideration, as part of a threat analysis, of safety as well as security threat pathways.

Because NPPs are this type of facility, security considerations for NPPs include those caused both inadvertently, through errors or inattention, and intentionally, through deliberate malevolent actions.

3.3 CI Facilities as National/Technological Icons

Knowledgeable experts consider CI facilities that have the status of national or technological icons to be more attractive targets for terrorist attacks than less iconic or symbolic facilities. As icons, events concerning these facilities are typically subject to greater media and public attention than other facilities. Consequently, an attack, even potentially an unsuccessful attack, on an iconic facility can have strong symbolic meaning and psychological effects and may precipitate a cascade of economic and/or regulatory responses. (DeVan 2003.) A facility's iconic status interacts with its potential as a threat/hazard and its role in the critical infrastructure system to influence how the facility might be viewed as a potential target by terrorists and thus its priority for protection. Symbolic significance and consequences are not orthogonal. Attacks on highly symbolic targets are designed to evoke social and political consequences such as fear, anger, erosion of public confidence, and protective actions that can greatly magnify the impacts beyond the direct damage or destruction to the target facility/system. As Durling and Price (2006) point out, the cause of damage can influence the impacts that result. NPPs have been identified as having national and technological iconic attributes that affect their desirability as potential targets and the consequences of potential attacks on them (Beherens and Holt 2005; Chapin et al. 2002; Ferguson and Potter 2004; Fowler 1981).

3.4 CI Facilities as Public Goods or Private Investments/Property

CIs and key assets include both publicly- and privately-owned facilities and systems. Ownership affects the locus of decision making concerning a facility and the nature of the owner's and the public's interest in the facility. Table 3.1 summarizes some of the differences among public owners, private owners, and regulators in terms of roles and interests regarding U.S. CI facilities.

Table 3.1 Roles and Interests for CI

Roles & Interests / CI Attributes	CI as Capital Asset (Capital asset and revenue source)	CI as Provider of CI Functions	CI as Potential Threat
Private Owner	Primary purpose and interest		Secondary interest (liability concerns)
Public Owner	Secondary interest (public stewardship of resources)	Primary purpose	Secondary interest (public welfare responsibility and liability concerns)
Regulator/Public		Primary interest (but may not fall within jurisdictional authority)	Primary purpose and responsibility (protect public health and safety)

As pointed out in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (U.S. President 2003), the protection of U.S. critical infrastructure is a shared public-private responsibility. Following the terrorist attacks of 2001, government officials and public- and private- sector owners of CI have focused a great deal of effort on clarifying the relative roles of facility owners, regulators, and public safety/security providers in ensuring the security of U.S. CI.[15] Private-sector CI owners have questioned whether they have the responsibility, or the ability, to provide security adequate to protect against terrorist attacks of the scale demonstrated in 2001. They have argued that such protection is appropriately the responsibility of law enforcement and national security agencies. These issues were manifest in the discussions of "design basis threats," "enemies of the United States," and facility security capabilities that followed 2001 (U.S NRC 2003a, 2002, 1967).[16]

The public, and regulators representing the public interest, have multiple interests in the security of CI facilities. First, they have an interest in ensuring that the services provided by the facility are not delayed or disrupted. If the facility is a public facility, they have an interest in protecting the public investment made in the facility and in ensuring that the

[15] Appendix B summarizes some of these efforts.

[16] For NPPs, this has included dispute about what defensive security capabilities the licensee was responsible for providing and what law enforcement and national security local, state, and/or federal government was responsible for.

facility is not damaged or destroyed (thus requiring repair or replacement). In addition, they have an interest in protecting the facility from damage that might create a public hazard (for example a flood, toxic release, etc.).

Differences in roles, responsibilities, and interests in building and operating CI facilities influence the approach owners, contractors, and regulators take toward security. Both the experts consulted about industry standards and construction processes for both public and private CI facilities and the expert participants in The Infrastructure Security Partnership (TISP) workshop on construction security held in February 2008 (see appendix C) emphasized that cost and, consequently, the construction time-line were primary considerations for private-sector facility owners (including public corporations) and contractors. The potential need to enhance security during construction and build more robust buildings following the 2001 terrorist attacks have heightened these cost and time-line concerns. They noted that contractors are unlikely to implement security measures unless specifically required to do so by the facility owner, with the required measures delineated in the construction contract and enforced by the owner. The other entities with leverage over security measures during construction are those financing the construction (e.g., banks) and insuring the facility. However, according to the experts and literature consulted for the study, neither financial nor insurance institutions have made an organized effort to use this leverage to impose security requirements on owners or contractors during facility construction (Kosnick 2005; Kunreuther and Michel-Kerjan 2004; Lowhurst 2003).

3.5 Attributes of the Life-Cycle Phase: Facility Construction

The construction phase has a number of distinct attributes that affect threat pathways, vulnerabilities, and therefore, security planning and preparation. These include:

- The number and variability of workers, activities, materials, and equipment over the construction life cycle;
- The flow of personnel, vehicles, and materials across and within site boundaries;
- The characteristics of the construction workforce; and
- The characteristics of the construction industry.

The Number and Variability of Workers, Activities, Materials, and Equipment over the Construction Life cycle

Construction work sites are notable for the rapidity of change in the number and type of workers, the work activities, the materials being received and shipped off-site, and the stage of completion of structures. NPP construction is a multi-year, multi-billion dollar undertaking that involves different organizations at different times, a workforce of widely varying size and skill composition, and a changing array of vehicles and equipment. Construction of an NPP involves a buildup of workers from hundreds to thousands, followed by a workforce reduction of similar pace and scale. The specific composition of the workforce typically varies from day to day depending upon the phase of construction and tasks to be completed. Workers are employed on-site for differing periods of time, from days to years. Estimates of the peak construction workforce for new NPPs typically range between 2,000 and 4,000 workers, although the peak construction workforce at

some projects in the first round of NPP construction rose above 10,000 workers.[17] As an illustration, Figure 3.1 shows the projected workforce for the Tennessee Valley Authority's (TVA) proposed two-unit Bellefonte project (TVA 2008).

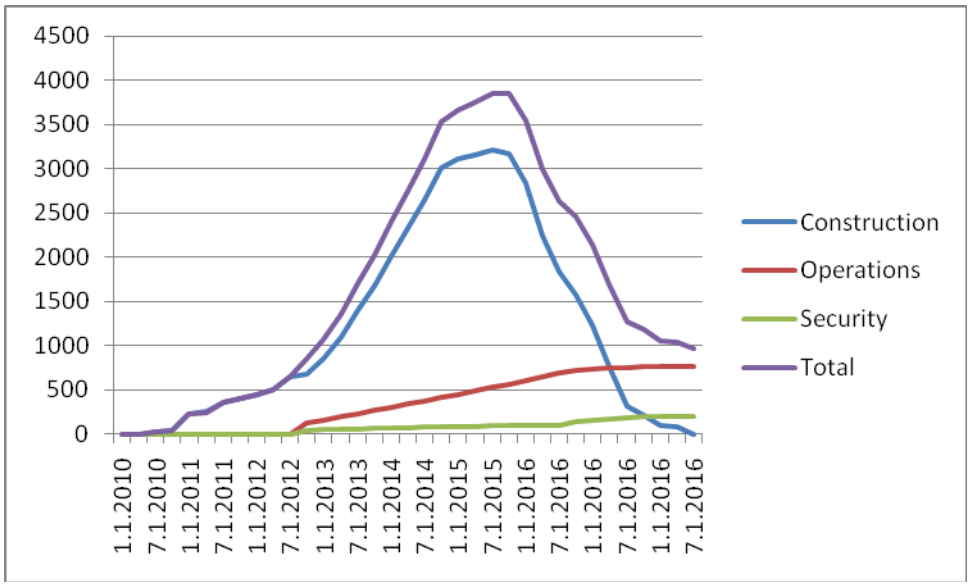


Figure 3.1 Projected Workforce Requirements during the Construction Phase of Bellefonte NPP Units 3 &4

The construction-phase workforce brings together a variety of workers, from general laborers, crafts-workers, specialized technicians, and engineers, to supervisors of these personnel. The construction workforce is typically assembled for the particular project and thus may include many workers who have not worked together before the project. In addition, operations-workers begin arriving on-site during the construction phase to start training and preparing for transition to operations status. As construction proceeds, an increasing number of workers will be working on, or working in areas with access to SSR-SSCs.

In addition to requiring many types of workers engaging in numerous different and changing activities, construction also involves the acquisition and use of myriad types of materials and equipment. The materials (including sand, gravel, cement, lumber, reinforcing and structural steel, cable trays, conduits and power cables, large and small bore piping, and small, medium, and very large manufactured/prefabricated components) and equipment also vary by sub-phase of construction. Some materials

[17] During the first cycle of NPP construction, work force numbers varied by site, but often rose to between 1,500 and 3000 on-site workers during construction periods that in many cases extended beyond six or seven years. For example, at the two-unit Peach Bottom construction site, the average quarterly workforce peaked at over 2,800 workers, and was above 1,500 for about five years (Bergmann and Pijawka 1981). Estimates of the peak construction workforce prepared for the U.S. Department of Energy indicate somewhat higher requirements – in the range of 2,400 workers for an average single GEN III plant (D'Olier 2005). The cumulative workforce can be up to 5,000 workers for a two-unit project that includes both skilled and unskilled workers, some of whom may be on-site for a number of years. It is worth noting, however, that most pre-construction estimates of workforce requirements for the first wave of nuclear power plants were lower than actually occurred (Chalmers et al. 1982).

and equipment are incorporated into on-site structures; others are used temporarily and then transported off the site. To add even more complexity, the materials and equipment used during construction are supplied and delivered to the site by a changing cadre of suppliers and transporters. This brings a variety of vehicles (vans, trucks of all types, trains/containers, barges) and non-employee personnel onto the site. Some of these vehicles and personnel may access the site frequently and regularly; others may make a single delivery and not access the site again.

The Flow of People, Vehicles, and Materials across and within Site Boundaries

NPP construction sites are characterized by a dense and continually changing flow of personnel, vehicles, and materials into, within, and out of the project site. Vehicles and personnel associated with materials and equipment suppliers and transporters constitute an important portion of this flow. Workers employed by a variety of different organizations arrive and leave in dense waves at shift turnovers. The number of "transient" personnel places an administrative burden on those responsible for verifying worker identification, confirming that deliveries have been ordered, checking for contraband and unauthorized materials being brought onto or taken off the site, and tracking the whereabouts of workers, vehicles, and materials while on-site. It is likely that a significant portion of the people, equipment, and materials will be unfamiliar to security staff while supervisory construction staff will be continually entering and leaving the site in relatively high numbers during much of the construction period, often in concentrated flows (Honnellio and Rydell 2007).

Workforce Characteristics

The construction workforce for NPPs is expected to include significant numbers of laborers, insulators, equipment operators; highly skilled crafts workers (boilermakers, pipefitters, electricians, and ironworkers); and administrative and support personnel. Many of the workers will be members of the crafts unions, and may be moving or commuting from distant locations. It is anticipated that if multiple NPPs are being constructed simultaneously, highly skilled workers will be in short supply and high demand, and that they may work serially at different NPP projects.

Substance Abuse Patterns

In addition to the large numbers and high turn-over of workers, construction workers have very different attributes compared to operating plant employees. A recent study of substance use by the U.S. Department of Health and Human Services (Larson et al. 2007) found construction workers to have the highest prevalence of alcohol use and the second highest prevalence of illicit drug use compared to other major occupational groups.[18] Although NPP construction workers may differ slightly from the average

[18] The findings for different occupational groups and industrial sectors are:

- The major *occupational* groups with the highest prevalence of past month heavy alcohol use were construction and extraction occupations (17.8 percent) and installation, maintenance, and repair occupations (14.7 percent). Community and social services occupations (2.8 percent) had the lowest prevalence of past month heavy alcohol use of the major occupations.
- The *industry* groups with the highest prevalence of past month heavy alcohol use were construction (15.9 percent); arts, entertainment, and recreation (13.6 percent); and mining (13.3 percent) industries. However, health care and social assistance (4.3 percent) and educational services (4.0 percent) had the lowest prevalence of past month heavy alcohol use compared with the other major industries.

construction worker, a review of media coverage during the first cycle of nuclear power plant construction revealed that on-site consumption of alcohol and illicit drugs by construction workers was a significant problem. Drug and alcohol use was frequently reported in the media as a example of the lack of good management, quality control, and security at the NPP construction sites.[19] More recently, drug and alcohol use among construction workers has been such a widely recognized and persistent problem throughout the construction sector that a number of labor unions have supported policies to require random drug testing of workers on construction projects and a growing number of states have enacted legislation requiring that construction workers on state projects be subject to random drug and alcohol testing.[20],[21] Use of illicit drugs not only creates safety concerns due to worker impairment, but potential pathways to criminals and criminal networks and vulnerability to pressure, coercion, exploitation, or duress (Contractors Association of West Virginia 2008; Fournier 2006; Gerber and Yacoubian, Jr. 2001; IBEW Journal 2005; Minchin et al. 2006; Willamette Week 1981).

Lack of English-Language Skills among Construction Workers

Many construction workers in the less-skilled crafts are not U.S. citizens and many are recent immigrants. A study sponsored by the National Association of Home Builders covering the period 2003-2006 found that approximately 29% of the workers in the construction industry were foreign-born. This is consistent with U.S. Department of Labor estimates that 28% of all construction workers were non-native in 2006 (*Nation's Building News* 2008). This leads to a situation in which many construction workers do

---

- Of the major *occupational* groups, food service workers (17.4 percent) and construction workers (15.1 percent) exhibited a higher prevalence of past month illicit drug use than other occupational groups. Those working in education, training, and library occupations (4.1 percent), community and social services occupations (4.0 percent), and protective service occupations (3.4 percent) had the lowest prevalence of past month illicit drug use among the major occupational groups.
- The major *industry* groups with the highest prevalence of past month illicit drug use were accommodations and food services (16.9 percent) and construction (13.7 percent). Public administration (4.1 percent), educational services (4.0 percent), and utilities (3.8 percent) had the lowest prevalence of past month illicit drug use.

[19] Our research identified media reports of drug and alcohol use on-site by construction workers, or drug busts and other substance-abuse related problems (often more than once) for many NPPs under construction, including the Midland, Seabrook, Shearon Harris, Trojan, and WPPSS plants.

[20] Chapman (2001) reports that the New York Office of Alcoholism and Substance Abuse Services (OASAS) found that construction workers had some of the highest rates of heavy alcohol and illicit drug use and that about 40 percent of industrial fatalities were linked to alcohol use. Drug testing is increasingly used by construction firms to deter drug and alcohol use. One company owner at the Construction Safety and Drug Abuse Executive Roundtable stated: "Drugs are omnipresent, especially in this business [construction]. So that's why we insist that our workers take a drug test initially. The best way to sum up hiring in this business is caveat emptor." Another factor driving drug testing for construction workers is New York Labor Law 240, which holds the contractor liable if anyone falls or is injured on a work site for any reason. However, it was noted that the various hierarchies of contractors and subcontractors coming and going at a site make implementation of a stringent drug screening program difficult to enforce. Many companies have employee assistance programs (EAPs) in recognition of the number of workers struggling with drug and alcohol problems. Roundtable participants also pointed out that because of the safety consequences of drug and alcohol use among construction workers, insurance companies increasingly require drug testing for companies and safety personnel, and that these companies are often in the front line in establishing company drug testing policies (Construction Safety and Drug Abuse – Executive Roundtable Highlights 2006). See also Stump (2007).

[21] Six states have enacted legislation requiring any individual or company receiving a grant from the state to have a drug-free workplace, including: California, Florida, Georgia, Illinois, and South Carolina. Several states specifically target construction workers, including Ohio, West Virginia, and Idaho (National Conference of State Legislatures 2006; Ohio Bureau of Workers' Compensation 2006; Thompson 2003).

not read, speak, or comprehend English well. Research has shown poor English skills to be an important contributor to safety and security mishaps on construction sites. A number of studies have called attention to the growing percentage of non-native English speakers in the construction industry and the role inadequately addressed language barriers have played in construction-industry fatalities. In a study examining this issue, O'Malley (2001) points out the increasing percentage of Hispanic workers in the construction industry, including those in unionized jobs. Although starting in the relatively unskilled jobs, an increasing number of Hispanics are moving into the operation of equipment. The International Union of Operating Engineers (IUOE), for example, has identified the language barrier as a sufficiently significant problem to workplace safety that they have established a National Hispanic Outreach Program (Business Insurance 2007).

Construction Industry Characteristics

The construction industry is composed of a mix of very large "prime contractors," which take on the overall management and integration of large-scale projects, and small- and medium-sized businesses that specialize in particular construction activities. For a variety of reasons, including the goal of providing business to local companies and workers, large-scale construction projects typically involve a number of different business entities, which may vary over the course of the construction process. Therefore, the workers at a construction site are likely to be employees of a number of different companies. Consequently, a construction project is likely to involve a complex contractual relationship among a number of different companies, and of workers who may be employees of the facility owner, the prime contractor, other contractors to the licensee, subcontractors to the prime, or subcontractors to other subcontractors. Each of the individual companies is likely to have its own employee selection and management processes, which have already been applied to their existing workers. This obviously creates a challenge to the establishment of consistent personnel processes and procedures (Arditi and Chotibhongs 2005; Thomas 1977).

Similar to the concerns about drug and alcohol use by construction workers are concerns about the involvement of organized crime in the construction industry. From the perspective of this study, these concerns focus on the potential of organized crime to jeopardize the quality of materials or work (through counterfeit or substandard materials) and the integrity of the quality assurance process (through bribery or corruption). Other concerns about the involvement of organized crime are that it increases the potential for theft of property, equipment, or information from the site and the introduction of contraband materials onto the site. (Berg and Hinze 2005; Kelly 1999; Gill 2007; Goldman 1988; Pro-Vigil 2007; National Legal and Policy Center 2003; Thomas 1977.)

The complexity and challenges of construction management have received greater attention in the literature recently, in part due to the emergence of more sophisticated management tools and greater attention to whole system design and sustainability (Bohra and Sharma 2006; Hendrickson and Au 2008; Muir 2005). A number of experts and media commentators expressed concern that the challenges of managing the construction of new NPPs would prove too great for managers who were dealing with new designs, were inexperienced with both the particulars of the modular construction process and nuclear construction requirements, and a workforce inexperienced in nuclear construction. As evidence that these concerns were warranted, they pointed to

the quality control problems, cost overruns, and schedule delays experienced during the first round of NPP construction and the similar problems occurring at the new plants being constructed in Finland and France (Cummings 1981a,b; Diablo Canyon Independent Safety Committee 2007; Feld and Carper 1997; Government Printing Office 1982; Kanter 2009; Katz 2007; Lean and Owen 2008; Lochbaum 2006; New Scientist 2007; Sawai 2001; Smith 2008; Willamette Week 1981).

3.6 Attributes of Facility Location and Construction Site

Site Attributes

The initial discussions with experts also helped the project team identify the attributes of construction projects that affect the need for and effectiveness of security measures. They pointed out that security issues are influenced not only by the characteristics of the facility and the special vulnerabilities of the construction process, but also by the characteristics of the construction site itself. The continuous stream of workers, vehicles, equipment, and materials coming onto and leaving a large-scale construction site increases the potential threat vectors compared to most operating CI facilities. Construction sites at which the facility under construction is adjacent to or interspersed with components of an existing facility pose different security issues than those where the new facility is separate or alone on the site. In their discussions, the experts made distinctions between these two principal types of sites:[22]

- Sites without an existing operating facility of the same type, termed "separate/greenfield" construction sites; and
- Sites with an operating facility of the same type, termed "shared" construction sites.

At shared sites, the new facility can be adjacent to the existing one – the most likely situation for NPPs – or interspersed with components of the existing facility as, for example, are many port construction projects. Some of the applications for new NPPs are for separate sites, but others are for sites that already have one or more operating nuclear units. For simplicity, the analysis focused primarily on separate/greenfield sites, where the security needs during construction are not confounded by the presence of an operating facility.[23] A determination that security measures are warranted at separate/greenfield sites makes the strongest case that an under-construction facility merits protection.

In addition to these two major distinctions, the experts also identified other aspects of the location of the site (for example, proximity to roads, along navigable waterways, below nearby hills) and site layout (amount, characteristics, and ownership of buffer areas; number and distance between entry points) that would influence the need for and design of security measures. However, given the focus of the study on personnel security, the

[22] Although many other features of the site, such as proximity to population centers, also affect the security considerations for a facility and its construction, proximity to an operating facility was determined to be the most salient for this analysis.

[23] Because the issues of security during construction and their potential for consequences during the subsequent operation of the facility are complex and had received little prior discussion or analysis, discussions with experts required simplifying and focusing the examination. As discussed in Chapter 5, more detailed examination of the implications of site characteristics for security, particularly between separate/greenfield sites and shared sites, would be beneficial.

principal focus was on measures needed to ensure that the flow of workers, materials, and vehicles onto, within, and off of the site could be monitored and controlled without interfering with or experiencing interference from other neighboring facilities and activities.

3.7 Attributes of Facility Interface with Off-Site Workers, Suppliers, and Systems

The experts consulted for this project emphasized that off-site workers, suppliers of NPP components, and plant systems themselves merited concern as potential sources of security threats. Plant construction draws upon an extended, off-site workforce involved in off-site component construction, manufacture, and assembly, and the purchase-transport supply chain. This report addresses these workers only briefly, but notes their potential importance to facility security. The supply chain during construction is a continuous stream of building materials and equipment coming onto the site, followed by a steady stream of components and systems for the facilities as they are being built. The experts pointed out that the supply chain during construction is more varied and less subject to security than during operations and can be vulnerable at many points. The security of the supply chains of safety- and security-related components may be particularly important to facility security, especially for closed/sealed components, which may be difficult to inspect fully by visual examination, and for safety and security-related software systems. In addition, they noted that the supply chains for the increasing proportion of materials, components, and systems being obtained from foreign countries might pose particular challenges because those supply chains tend to be long, complex, and pass through less secure transit points.

4. Threats

4.1 Overview of the Chapter

This chapter discusses threats to CI and the extent to which the experts consulted believe there are threats and vulnerabilities to CI under construction that warrant attention. It summarizes the way experts characterized threats and vulnerabilities, particularly those during the construction phase.

Section 2.3 above describes a six-element vulnerability assessment framework that the project team used to structure its overall inquiry. Two of those elements are analysis of threats and analysis of risks and vulnerabilities remaining after applying standard protective measures to address those threats. This chapter addresses both of those elements, although with a low level of specificity.

4.2 Contextual Considerations

Adequate characterization of threats to a facility requires information about the type of adversary, the adversary's potential actions, motivations, and capabilities, and the actions of insiders that might facilitate or enable the adversary (U.S. Department of Justice 2002:13). Understanding the threats provides the basis for designing protective measures and determining when and to whom they are applied.

The Impact of the 2001 Terrorist Attacks on the Assessment of Threats to U.S. Critical Infrastructure

After the 9/11 terrorist attacks, managers of CI throughout the United States re-examined their security needs. The NRC assessed threats, vulnerabilities, and mitigation strategies for operating reactors, revised its "design basis threat,"[24] heightened physical protection and personnel security requirements, initiated an insider mitigation program, and processed security clearances for selected employees in the nuclear industry so they could access classified threat and vulnerability information.[25] The NRC also developed security design requirements for new reactor licensing activities (U.S NRC 2005b) and expanded its mission to include security in addition to safety as a priority focus.[26] For the NRC, as for organizations responsible for the

[24] The design basis threat is defined as: "A profile of the type, composition, and capabilities of an adversary. The NRC and its licensees use the design-basis threat (DBT) as a basis for designing safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. The DBT is described in detail in Title 10, Section 73.1(a), of the Code of Federal Regulations [10 CFR 73.1(a)]. This term is applied to clearly identify for a licensee the expected capability of its facility to withstand a threat. See U.S. Regulatory Commission SECY-05-0120, July 6, 2005 for a summary of NRC post 9/11 activities.

[25] The U.S. NRC's September 2006 Backgrounder on "Nuclear Security – Five Years After 9/11" summarizes these activities.

[26] The U.S NRC *Strategic Plan: Fiscal Year 2000-Fiscal Year 2005* states: "Our highest priority is safety, and our performance goals focus our attention on the achievement of this priority." The message from the Chairman in the U.S NRC *Strategic Plan: Fiscal Years 2004-2009* includes the following acknowledgement: "The events of September 11, 2001, brought to this country a new recognition of the importance of physical security and emergency preparedness. We recognize that safety, security, and emergency preparedness are integrated activities, and we have revised the plan to reflect this new reality." The commentary on the changing regulatory environment notes: "NRC strategic initiatives will include significant emphasis on strengthening the interrelationship among safety, security, and emergency preparedness." In addition, the FY2004-2009 Strategic Plan added "Security" as one of its five goals, second only to "Safety." By the

security of nuclear facilities and radioactive sources worldwide, 9/11 caused a shift in perspective and an expansion of focus. As noted in International Atomic Energy Agency (IAEA) interim guidance on security for radioactive sources (IAEA 2003:1), "before 11 September 2001, the security of radioactive sources was largely addressed by measures protecting the sources from unintentional access by inappropriately qualified personnel or attempts at theft for financial gain. This assumption has now had to be modified to also include the need to prevent access to certain sources by people deliberately and malevolently seeking to cause radiation exposure or dispersal of radioactive materials."

The NRC also recognized the need to determine whether the heightened threat of sabotage and terrorist attacks extended to facilities under construction. Specific issues were raised as the NRC undertook revision and updating of a number of regulations, including 10 CFR Part 26, "Fitness for Duty Program," and its physical protection and access authorization requirements (10 CFR §§ 73.55 and 73.56). The principal question was whether sites under construction had vulnerabilities that could be exploited to yield consequences of regulatory concern to the NRC (i.e., that threatened the public health and safety, common defense and security, the environment, interruption of the normal operations of the plant, or radiological sabotage to a degree that warranted regulatory action, given the motivation and capability of the potential adversaries).

Increased awareness of the potential for acts of major sabotage or terrorism in the U.S., combined with the growing momentum for new NPP construction, fueled debate over security needs during NPP construction. Perhaps because no other CI sector is facing the same dramatic resurgence of proposed new construction, no similar debate about security during the construction of other critical infrastructure sectors has yet emerged.[27] However, almost all sectors have been affected by the major federal initiatives to reduce the vulnerability and increase the resilience of the U.S. CI, driven by presidential directives and Department of Homeland Security programs. These initiatives are developing and deploying new technologies (smart badges, detection equipment, etc.), establishing new requirements (access control, standard identity credentials, fingerprinting, searches, etc.), and changing expectations about security and access in ways that will affect all sectors. Appendix B summarizes some of these initiatives. Many of the changes being introduced by these initiatives will have occurred by the time new NPP construction is underway, and some have the potential to significantly change the cost in time and effort required to implement advanced security measures potentially pertinent to the nuclear industry.

Regulatory Authority: Questions about Whether Threats during Construction Rise to the Level of Regulatory Concern for the NRC

The NRC's regulatory authority is defined and circumscribed by the Atomic Energy Act of 1954, as amended; the Energy Reorganization Act of 1974; and other Federal legislation. This authority includes the licensing and regulation of commercial nuclear

---

FY2008-2013 Strategic Plan, the number of strategic goals was limited to two – "safety" and "security," framed in terms of ensuring "adequate protection in the secure use and management of radioactive materials."

[27] The experts consulted for this study commented on this phenomenon and expressed the view that such a debate is warranted. They also uniformly indicated that they would be interested in participating in such a debate.

power plants, and other uses of radioactive materials, "in order to protect public health and safety, promote the common defense and security, and protect the environment." (U.S. NRC NUREG-1614, Vol. 4)

The exact boundaries of this authority are subject to interpretation. Disagreements about the nature of the threats and consequences that would rise to the level of regulatory concern and fall within the regulatory authority of the NRC have influenced discussions about the appropriate response to threats associated with human factors, organizational and managerial characteristics, and personnel for many years. Both the NRC and the regulated entities have an interest in ensuring that the NRC does not impose unnecessary regulations, or regulations that exceed its mandate. However, both the NRC and the public have an interest in ensuring that the NRC does not fail to impose requirements where they are within its authority and serve the public interest. The debate has tended to center around threats whose consequences, though not resulting in a radiological release, theft of radiological material, or acquisition of safeguards or critical security information, nevertheless pose a significant risk to:

- Public confidence in the safety and security of nuclear power;
- Continuity of operation of nuclear power plants;
- The safety and security of workers at the site and its immediate vicinity.

The experts consulted for this project identified pathways by which delayed impact threats could cause damage to an operating plant that could result in a radiological release and adversely affect public health and safety, common defense and security, and the environment. These pathways clearly fall within the NRC's scope of authority.[28] They also identified pathways that would cause grave damage to the plant under construction, but without the potential for radiological release. This is where the debate centers on regulatory authority and scope. Does preventing the destruction of the plant under construction, with its concomitant damage to the health and safety of the workers and nearby residents, public confidence in the safety and security of NPPs, and damage to the environment, fall within the regulatory authority of the NRC? It is beyond the scope of this project to resolve this debate, but the consideration of the threats to NPPs under construction provides an instructive illustration of the ambiguity about the boundaries of the NRC's regulatory authority and its practical consequences. Further discussion of this issue is suggested as a worthwhile next step in Chapter 8.

4.3 Considerations for Threat Assessment

Types of Threats

Based on a review of the literature and consultations with experts, the project team examined the following security threat types to help ensure that the entire range of potential threats is considered:

- Immediate and delayed impact threats;
- Intentional and inadvertently-caused threats;
- Threats caused by insiders, outsiders, and insiders colluding with outsiders.

[28] This then becomes a question of whether the threat is judged to be sufficiently likely to warrant regulatory action, and falls into the debate described in step one.

The increased concern about premeditated malevolent intent following the 2001 terrorist attacks has led to a distinction between two types of threats that might occur during the construction phase:

- Immediate threats; and
- Delayed impact threats.

For immediate threats, both the causes and consequences occur during the construction phase; for delayed impact threats, the causes may occur during the construction phase, but the consequences occur after fuel has been brought onto the site or the plant has begun operating. Earlier phases in the life cycle, for example facility siting or plant design, may affect the potential for either or both of these types of threats. The terrorist attacks of 2001 and subsequent threats to U.S. and international targets, combined with the revised estimates of the potential capabilities of adversaries, have dramatically influenced assessment of security needs throughout the U.S and heightened concern that both immediate and delayed impact threats should be considered more seriously.

Debate over Whether There Are Threats of Concern during NPP Construction

Overview of the Debate

A first step in determining whether there are threats of concern during NPP construction is to understand the range of viewpoints about the existence of such threats and the principal arguments used to support those viewpoints. A second step is to understand the range of viewpoints about what constitutes a threat of regulatory concern for the NRC, the criteria used to make this determination, and viewpoints about whether either immediate or delayed impact threats during construction meet those criteria. Important to the debate are viewpoints about two types of threats that may occur during the construction phase: immediate and delayed impact threats.

Immediate and Delayed Impact Threats: Questions about their Existence and Potential for Impact

Among the arguments that have been made are that threats with the potential for consequences that warrant protective measures and NRC regulation do not exist until either fuel is on site or the plant has reached criticality.[29] In the latter case, the argument is that the plant would already be subject to the enhanced security measures mandated for operating plants and that therefore no additional measures or regulation is warranted. Both these arguments depend on the assumptions that: (1) only consequences involving nuclear materials warrant regulation and therefore no direct impact threats during construction before the arrival of fuel could achieve the level of regulatory concern;[30] and (2) delayed impact threats do not constitute a credible threat, either because they (a) do not have the potential to cause sufficiently severe consequences, (b) the probability of such threats is so low as to not merit regulation, or (c) existing

[29] The Nuclear Energy Institute (NEI) made this argument in its comments to the NRC on the proposed FFD rule's subpart K dealing with construction. See USNRC, publishing date uncertain, Summary and Analysis of Public Comments Received on Proposed Revisions to 10 CFR Part 26 - Fitness for Duty Programs.

[30] See above. The argument is that all NRC safety and security regulation is targeted toward the design basis threat (DBT), which is centered upon preventing radiological release or acquisition of radioactive materials.

construction security, safety, and quality assurance/quality control (QA/QC) practices are adequate to detect and neutralize any threats that might occur. In support of these assumptions, the argument is made that delayed impact threats would require such a long time horizon that they would not be of interest to terrorists or criminals and hence would not be undertaken.

In addition, there are more nuanced arguments that focus on earlier phases in the life cycle. From this perspective, reflected by some of the experts in nuclear facilities consulted for this project, focusing on security during construction may be too late and too indirect, and requirements should instead be placed on earlier phases in the life cycle (such as reactor design, plant design, and plant siting,[31]) which can impact both operational and construction security. A more effective strategy, those making this argument claim, would be to take security into greater account earlier in the life cycle in order to reduce security risks during the construction phase to a point they do not pose a significant concern. A corollary argument is that adequately addressing risks associated with the supply chain could significantly mitigate risks during construction. Review of the numerous initiatives undertaken to enhance security of America's critical infrastructure following the terrorist attacks of 2001 reveals that only limited attention has been given to security during construction, at any phase of the life cycle for most CI sectors, even by those proposing a life-cycle approach to security. Consequently, it is possible that security during construction could be enhanced by measures taken earlier in the life cycle.[32]

Conversely, there are also arguments that both immediate and delayed impact threats may warrant enhanced security during construction. Immediate threats, such as intentional acts of sabotage during construction, could destroy or seriously damage a facility. Evidence that NPP construction sites are a target for saboteurs or terrorists could alarm the public and increase fear and opposition to continued development of nuclear facilities. The nuclear revival could be stalled. In this way, immediate threats could result in major economic consequences and may be a significant concern, not only for the nuclear industry but also for U.S. national energy policy.

Table 4.1 summarizes the differing views regarding threats during NPP construction.

Expert Opinion on the Need to Address Threats during Construction

Consistent with this latter argument, some of the experts consulted argued that inattention to security during the construction phase is a significant omission. They stressed that the possibility of delayed impact threats should make construction security a priority issue and that the susceptibility of a construction site to threat pathways involving the supply chain and the workforce make it essential that construction security be thoroughly examined and precautions taken as needed.

Arguments about the need for security before fuel is delivered to the site or the plant reaches criticality reflect which, if any, of these threats are believed to be credible. The cost of protecting against these kinds of threats could be significant. Those who do not

[31] Plant siting can influence the desirability of the target in terms of the impact on the surrounding area and population. Plant siting can also make access to the site more difficult and the standoff distance greater.
[32] One purpose of the life-cycle approach is to provide a framework for this type of examination.

Table 4.1 Summary of Differing Views Regarding the Existence of Threats of Concern

	Threats of Concern Do Not Exist	Threats of Concern Do Exist
Immediate Threats	• Significant security threats do not exist until nuclear material has been brought onto the site, at which point, the plant is subject to the enhanced security measures mandated for operating plants.	• Intentional acts of sabotage during construction, though perhaps not a health and safety risk, could alarm the public and increase their fear of nuclear power to the point of disrupting or completely derailing the impending nuclear renaissance.
Delayed Impact Threats	• These threats require too long of a time horizon to be of interest to terrorists. • Existing construction security, safety, and QA/QC practices are adequate to detect and eliminate such threats. • While it is readily apparent that earlier phases in the life cycle (such as reactor design, plant design, and plant sitting) can impact operational security, the impact of construction security on operations is less obvious.	• Terrorists' time horizon is not too short to preclude their interest in perpetrating these kinds of threats. • Existing construction security, safety, and QA/QC practices are not adequate to deter and/or detect these threats. • It is not difficult to imagine ways that security during construction could impact security during operations. Moreover, threat pathways associated with the supply chain and the workforce tend to be greater during construction than during operations.
Costs/Benefits	• The costs of protecting against unlikely threats of this nature may make building new NPPs financially undesirable for utilities.	• Not spending the money to protect against these kinds of threats could result in far greater costs.

believe threats of this nature exist during the construction phase conclude that the costs of enhanced security would outweigh the possible benefits and express concern that the addition of such unnecessary requirements could cumulatively make building new NPPs financially infeasible.[33]

On the other hand, if one believes these threats are credible, it is clear that the costs of failing to protect against them would be great, easily outweighing the costs of enhanced protection. Even a subverted threat could have major costs. This is why experts consulted for this project believe it is important to systematically examine and assess the likelihood of these threats, determine whether and how these threats can be reduced or eliminated, estimate the costs associated with an effective protective strategy, and examine regulatory and management authorities and responsibilities. Only then is it possible to determine what constitutes acceptable risk, who is responsible for which aspects of that risk, and what needs be done, if anything, to achieve the level of acceptable risk during new NPP construction.

[33] This reflects a concern expressed during the first wave of NPP construction that opposition groups had a goal of raising costs, through delays and challenges, as a way to stop further NPP construction (Cook 1980).

Factors Affecting Threats

Potential Perpetrators

Perpetrators of threats can be insiders, outsiders, or insiders colluding with outsiders. Given the potential for delayed impacts, they can be workers in different phases of the life cycle, including the supply chain.

The scope of this project did not include a full threat assessment regarding the intent and capabilities of terrorist groups or other potential saboteur groups or individuals. Rather the project team interviewed representatives from the counter-intelligence community and nuclear security experts to ascertain their sense of the nature of the threat environment. These experts affirmed that there are groups who have expressed interest in and have the capability to perpetrate significant threats targeting NPP construction. A classified report summarizing this analysis was submitted to the NRC in 2006 documenting the basis for this position.

Relative Target Desirability

In addition to determining whether possible perpetrators exist, it is important to assess the relative desirability of NPP construction as a target – desirability pertains to why potential perpetrators would select NPP construction as a target.

Comparison of Desirability – Operating and Under-Construction NPPs as Threat Targets

An additional element of the arguments about whether threats to NPPs under construction warrant protective regulation is that those interested in attacking a NPP would focus their efforts on operating plants rather than NPPs under construction. Although this argument is countered by the historical evidence that clearly demonstrates that NPPs under construction have been the subject of many attacks at various levels of violence and destructiveness, examination of the relative desirability of operating and under-construction NPPs provides useful information about potential threat pathways and construction site characteristics.

Factors Affecting Target Desirability

In assessing the existence of threats to NPPs during construction and determining whether there is a basis for imposing deterrence and protection measures, it is important to understand the factors affecting their desirability as threat targets. Discussions with experts and review of the literature indicate that three main factors are particularly pertinent to a facility's desirability as a terrorist target:[34]

- Symbolic significance;
- The extent, nature, and distribution of the impacts that could result from an attack; and
- The ease of perpetrating a successful attack.

[34] DeVan (2003). Durling and Price (2006) point out the importance of incorporating symbolic significance and its consequences for the impacts of terrorist attacks in assessing and prioritizing security measures. They note that the cause of damage can influence the impacts that result.

Symbolic significance and consequences are not orthogonal. Attacks on highly symbolic targets evoke social and political consequences such as fear, anger, erosion of public confidence, and protective actions that can greatly magnify the impacts resulting directly from the damage or destruction of the target. Assessment of consequences must take into account both the direct and indirect impacts resulting from the attack. The ease of perpetrating a successful attack depends on many factors, including the number of possible threat pathways, their accessibility to potential perpetrators, the difficulty of detecting the threat, and the resources available to counter the threat. These related factors together contribute to the overall cumulative risk and inform the overall protection strategy: The number of pathways and the risk associated with each pathway affects the challenges and difficulties in providing adequate protection.

In their efforts to prioritize protection of U.S. critical infrastructure, the Department of Homeland Security has sponsored a number of task forces, studies, and forums. The results emphasize both the complexity of the task and the need to take into account inter-facility and cross-system dependencies that affect the consequences of impacts on any individual facility or sector (U.S. DHS 2007). Given the limited scope of this project regarding risk, threat, and vulnerability assessment, the investigation acknowledged these complexities, but focused on a comparison of the relative desirability of operating NPPs and NPPs under construction. This focus not only simplifies the investigation of credible threats but also supports the analysis of which, if any, of the personnel security measures required for operating NPPs might be appropriate and needed for NPPs under construction.

4.4 Historical Evidence of Threats to NPPs and Other CIs under Construction

There is ample evidence in the open literature that nuclear power plants and other nuclear facilities under construction have been the subject of successful attacks, both from state-initiated military and non-state actors. Attempted intrusions and terrorist or military attacks have been made on nuclear power stations in South Africa, Spain, France, Spain, and Syria. For example, in 1977 and 1978 workers were implicated in the bombings of the Spanish Lemoniz NPP. In 1979, a bomb exploded in the Goesgen plant in Switzerland shortly before the plant was scheduled to go into operation. In 1982, two out of five rockets launched against the Superphoenix breeder reactor in Creys-Malville, France, reached the site, and in South Africa four bombs were exploded at the Koeberg NPP under construction (Schneider 2001; Johnston 2003; Mohtadi 2006; Nuclear Monitor 2003). Some of these attacks have resulted in the complete destruction of the facility.

It is clear that there are individuals and groups with an interest in damaging, delaying, or shutting down nuclear power plants, and that a subset of them may want to cause widespread death and disruption. Recent examples include the protests and incursions at the NPPs under construction in France and at the Olkiluoto NPP in Finland, and numerous statements from domestic and anti-U.S. terrorists identifying nuclear facilities as potential targets. The threat conveyed in a letter sent to the New York Times four days after the terrorist attacks on the World Trade Center in 1993 warning that nuclear facilities were also targets and an interview on the al-Jazeera TV station stating that Al Qaeda initially planned to include a nuclear plant in its 2001 attack sites serve as examples (Beherens and Holt 2005; Greenpeace International 2007; Mitchell 1993).

Some of these documented events involve attacks from off-site, but others involve either disgruntled workers or workers actively participating with off-site colleagues. Some of these groups and individuals have demonstrated both a sufficiently long time horizon to attempt delayed-threat actions and the capability to successfully attack and damage NPPs under construction. In addition, there is ample evidence from construction projects in every sector, including nuclear energy, that errors and vandalism by workers may escape prompt detection and correction and that QA/QC practices and security oversight during construction can be subject to significant failures and shortfalls.[35]

Consequently, there is little debate that immediate threats could have significant consequences for the security (and even existence) of the plant, the health and safety of workers and persons in the immediate vicinity of the construction site, public confidence in nuclear power and its regulators, and impact on the long-term continuity of NPP operation. Given the historically demonstrated interest and capability to cause grievous impact on NPPs under construction, and to inflict significant adverse impacts in all the dimensions mentioned above, the question therefore becomes whether immediate threats that occur before fuel is on site constitute a sufficient risk that they reach a level of regulatory concern for the NRC. Based on the previous discussion about regulatory authority, it is not surprising that expert opinion differs, depending upon where the line of regulatory authority is drawn.[36]

The other significant question is whether NPPs under construction are subject to delayed impact threats that meet even the conservative interpretation of regulatory authority. As indicated previously, the scope of this project did not include detailed or site and time specific threat and vulnerability assessments of the type needed to delineate the risks. However, PNNL counterterrorism and security experts affirmed that there is sufficient evidence that intentional actions taken during the construction phase could either increase operational risk or directly cause a delayed event. This event could constitute a sufficient risk to public health and safety, the common defense and security, and continuity of plant operations, and thus cannot be ruled out as a threat.[37] They also affirmed, as is reflected in the open literature, that there is considerable evidence of individuals and groups with a variety of capabilities that have expressed interest in damaging, delaying, or shutting down nuclear power plants.[38] They also pointed out that a goal of terrorist attacks is surprise, so that a lack of historical precedence is not a good basis for assumption of future safety.

---

[35] Inadequate management oversight, pressuring of quality assurance/quality control (QA/QC) inspectors, and falsification of QA/QC documentation was an alleged issue at a number of U.S. NPPs during the first wave of construction (Perrow 1999; Ferguson 2004; Lochbaum 2006), and QA/QC issues on the Trans-Alaska Pipeline rose to the level of congressional investigations. In addition, experts on high-rise construction identified that ensuring the validity and completeness of QA/QC procedures was an on-going and difficult challenge.

[36] The Atomic Energy Act established the role of the NRC, separating regulation (the NRC's role) from promotion of nuclear power in 1954. In the post-9/11 security environment, it should be noted that DHS has undertaken to develop regulations to enhance security at a variety of critical infrastructure sectors, and to support regulations such as the REAL ID Act of 2005, and the Transportation Worker Identification Credential (TWIC), whose effects may extend to workers at NPPs during construction. A question discussed in Chapter 5 as warranting further consideration is how the NRC and DHS might work together to address regulation of construction security at NPP sites.

[37] PNNL submitted a classified report summarizing this analysis to the NRC in 2006.

[38] One example includes the threat conveyed in a letter sent to the *New York Times* four days after the terrorist attacks on the World Trade Center in 1993 warning that nuclear facilities were targets (Mitchell 1993).

Experts consulted for this study were of the opinion that detection of a delayed impact threat at a U.S. NPP under construction could have major repercussions for all NPP construction sites and perhaps at operating NPPs as well, particularly if information about the effort became public.[39] Evidence of such a threat could potentially affect the overall energy infrastructure and production capacity of the U.S, as well as precipitating corrective security measures that could well be very costly and disruptive.[40]

Operating NPPs

An operating NPP is perhaps a more desirable target than many other types of CI for several reasons. First, a successful attack on an operating plant could result in significant economic and potentially major public health consequences, as well as activating a high degree of fear. Second, the desirability of an NPP is heightened for many potential perpetrators by its symbolic significance: the potential to affect public confidence, activate public fears about nuclear power and radioactive materials, and precipitate adverse effects on the entire nuclear power industry. Civilian U.S NPPs, though built and operated for peaceful purposes, are, for some people, symbolically and technologically linked to nuclear weapons and radiological contamination. Possessing the capacity to build nuclear facilities has become symbolic of a country's might. Exclusion from the nuclear community has been a source of contention for some countries and organizations and successfully breaching security at NPPs is a stated goal of some international non-state terrorist groups.

Nuclear power also has practical and symbolic importance for some nonproliferation activists as well as for some health and safety and environmentalist groups, although the number of such groups that would have an interest in causing a major nuclear event is very small. In a more mundane way, operating NPPs may also be desirable targets for disgruntled workers, in part because violations have the potential to precipitate expensive investigations and mitigation requirements. As discussed above, information in the public domain indicates that both international terrorist groups and domestic antinuclear groups have targeted or considered targeting nuclear facilities in the U.S. Interviews with counter-intelligence experts further reinforced the view that operating NPPs are desirable targets.[41] Although at a different level, opposition to nuclear power plants has resulted in vandalism and sabotage, as well as breaches of security (Honnellio and Rydell 2007). Although perhaps not intended to cause a serious accident during the operation phase, such breaches of safety and security protections create the potential for an accumulation of errors and failures that could have unintended severe consequences.[42]

[39] For security reasons, much of the information about threats and threat efforts is not made public.

[40] Leibert (2007) points out that instilling fear and precipitating structural changes that are detrimental to the smooth conduct of the economy and government are among the primary objectives of terrorism.

[41] For example, as recently as spring 2008, two maintenance workers were arrested in Sweden on charges that they had participated in a bomb threat at a Swedish nuclear power facility (Magnusson and Pfalzer 2008).

[42] Bunn and Bunn (2002), as well as the Union of Concerned Scientists' website, document some of these incidents. Davis-Besse is a frequently cited example of accumulated errors leading to a threat to safety. Ballard's (1997) analysis of the RAND/St. Andrews database found that energy facilities have consistently been targets of terrorists, and that U.S. energy facilities were the subject of a disproportionately high share of those attacks (52.1 percent of the total energy facility attacks over a 13-year period).

Because there is reasonable evidence and consensus among those in the NRC and the nuclear industry that operating NPPs are desirable targets, substantial effort has been directed at protecting operating plants. Although operating NPPs have always had a significant level of security, security measures were further strengthened after 9/11. The result is that operating plants are not easy targets. The greatest remaining concerns expressed in the public domain are sabotage by insiders, the possibility of suicide attackers, a concerted attack by a terrorist team (possibly aided by insiders), or the use of innovative and/or high-powered weapons such as truck bombs or a fully-fueled airplane.[43]

4.5 Expert Opinion Regarding Threats to NPPs during Construction

Whether NPPs under construction are desirable targets that warrant protection is beginning to be addressed in the U.S. To further this effort, the project team reviewed available open literature and interviewed several nuclear vulnerability assessment experts, nuclear facility construction experts, and terrorism experts to determine what types of threats might be perpetrated, what consequences might result from threats to an NPP under construction, and the ease of perpetrating successful threats.

There was full consensus among the experts interviewed that there is a basis for believing that there are credible threats to many types of CI during construction. Compared to other types of CI, they believed that this would be a relatively high concern for NPPs under construction.

All the experts interviewed believed delayed impact threats are a concern. The experts identified several types of possible delayed impact threats, including:[44]

- Hidden explosives (in components such as HVAC, in pipes, or even in concrete) that could be remotely detonated after nuclear fuel was brought on site or the plant was operational;
- Intentional compromise of critical safety systems, structures, or components that would impair safety once the plant was operational;
- Intentional compromise of the security systems and infrastructure (such as creating intentional closed circuit TV (CCTV) blind spots, cloning electronic access, compromising alarm systems) that would impair the ability to provide adequate protection after the plant had nuclear fuel on site or became operational;

[43] The Energy Policy Act of 2005 identified twelve factors that could affect the need to revise the designbasis threat (DBT). These include: 1) the events of September 11, 2001; 2) an assessment of physical, cyber, biochemical, and other terrorist threats; 3) the potential for attack on facilities by multiple coordinated teams of a large number of individuals; 4) the potential for assistance in an attack from several persons employed at the facility; 5) the potential for suicide attacks; 6) the potential for water-based and air-based threats; 7) the potential use of explosive devices of considerable size and other modern weaponry; 8) the potential for attacks by persons with a sophisticated knowledge of facility operations; 9) the potential for fires, especially fires of long duration; 10) the potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals; 11) the adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility; and 12) the potential for theft or diversion of nuclear material from such facilities (NRC Frequently Asked Questions about NRC's Design Basis Threat Final Rule at http://www.nrc.gov/security/faq-dbtfr.html).

[44] Hidden surveillance devices were not identified as a major concern during NPP construction by these experts.

- Acquisition of critical information about safeguards and security that, in the hands of terrorists, could render the plant more vulnerable to a subsequent attack;[45]
- Creation of a concealed on-site cache of weapons or explosives that could be used to aid in an attack on the plant at a later time;
- Hidden surveillance devices;
- Delayed biocontamination (such as in HVAC);
- Compromised materials;
- Sabotage;
- Fraud/theft/crime;
- Blundering and ineptitude; and
- Inattention and passivity.

A few experts said they had not thought about delayed impact threats prior to the inquiry. However, most immediately grasped the importance of such threats. They agreed, for example, that a delayed impact event affecting a new operating plant could have great symbolic significance and resulting consequences. As with attacks on an operating plant, they identified the potential for the consequences of a single delayed impact event on a plant under construction to extend beyond the targeted plant by creating fear and uncertainty about what targets might be next.

The terrorist experts interviewed warned that it would be a mistake to assume that terrorists would not be interested in creating delayed impact threats at NPPs under construction. They pointed out that terrorists have shown themselves to be highly strategic and to have sufficient long term planning capability, as well as the organizational infrastructure to carry out complex, long-term endeavors. In addition, terrorists have shown persistence in re-targeting previously selected facilities or pathways over a period of multiple years and with a variety of methods (e.g., attacks on the World Trade Center).

These experts also thought that immediate threats during construction are a concern and that these threats originate from a variety of sources. They cited both historical and recent sabotage and eco-terrorism, including the protest/eco-terrorist event in 2007 at the Olkiluoto nuclear power plant being constructed in Finland, in which protesters gained access to the construction site and occupied one of the construction cranes (Laughter 2005; Greenpeace International 2007). They also referenced the detonation of a bomb in the steam generator of the Spanish Lemoniz NPP in 1977 as construction was nearing completion and the plant was undergoing preoperational testing as a signal immediate impact event that affected nuclear power construction in Spain. They said that analysis of the objectives of anti-U.S. terrorist groups indicates that a successful immediate impact threat significant enough to provoke public fear and resistance to the nuclear revival would be a highly desirable consequence, demonstrating their ability to overcome obstacles, influence the U.S. economy, and affect an emerging CI sector.[46]

[45] In addition, PNNL staff submitted a classified assessment of general types of security threats that could potentially be introduced during the construction phase of an NPP.

[46] DeVan (2003) identifies the potential to affect an entire economy or industrial sector and the potential to cause secondary physical or health impacts as features that make some new facilities more attractive to

The experts also indicated that, compared to operating plants, construction sites are easier targets. Less attention and resources are committed to physically securing access to a NPP construction site than to an operating site. During construction, the external/internal boundary is quite fluid because of the sheer number and variety of persons, vehicles, and equipment coming onto the site. They noted that historically, construction sites have been subject to a high incidence of theft and vandalism, much of which is attributed to persons authorized to be on the job site (estimates range from 30 to 85 percent). This has led experts on construction security to recommend both physical and personnel security measures that include extensive background checks and regular drug abuse checks for all personnel for a broad range of construction projects (Gill 2007; Pro-Vigil 2007; Berg and Hinze 2005).

The experts pointed out that physical security measures focusing on physical barriers (such as locks, gates, and fences) intended to keep the unauthorized and those with malicious intent out of construction sites are typically far less challenging to overcome than the "defense in depth" security strategies employed at operating plants. In addition, they noted that there was far greater openness once inside the site perimeter of a construction site than at an operating facility, allowing possible saboteurs to move rather freely throughout the site. They noted that physical security, even for NPPs being built on sites adjacent to an operating plant, might not be comparable to that of the operating plant. They also thought that much of the physical security that did exist was likely to be directed at protecting the operating plant from exposure to risks stemming from the adjacent construction site rather than protecting the construction site itself. According to the experts, physical security for separate/greenfield sites was likely to be even less robust unless new requirements are imposed.[47]

The experts identified the supply chain providing construction sites with materials and plant components as another major threat vector. As discussed in section 3.6 above, they noted that the construction supply chain was likely to be less subject to security than the operations phase supply chain. They pointed out that, given global supply trends, less-developed countries are likely to become more important as suppliers to CI construction projects and that this may increase the difficulty of overseeing and adequately securing the projects' supply chains because less-developed countries may combine known terrorist organizations with weak counter-terrorism capabilities.

Some experts suggested that construction sites would also be more vulnerable to insider threats and insider/outsider collusion than operating plants would be. Several factors were identified as contributing to this vulnerability:

- The workforce is much larger, with higher turnover;

---

terrorists than others. He points out that one consequence of the attacks of 2001 was to change the standards of care in design and construction of facilities.

[47] The experts familiar with these facilities generally reported that construction of facilities, including nuclear facilities, on shared sites tended to be subject to the same, or similar, personnel security measures as those applied to personnel at the operating facility. In many of these cases the new construction was taking place within the secured area of the existing facility's site or required construction workers to pass through or access portions of the operating facility to conduct their work. However, these security measures were implemented primarily to protect the operating NPP and only secondarily to protect the NPP under construction.

- Characteristics of construction workers, as opposed to employees at an operating NPP, make them a greater security risk;
- It is more difficult to screen all the individuals who need access to the construction site; and
- There may be resistance to employing rigorous screening during construction, in part because it may make it more difficult to meet hiring goals.

The experts cited the characteristics of NPP construction workforces noted in section 3.5 above – their greater turnover rates; their patterns of drug and alcohol use; the potential that some will have poor English skills – and the involvement of organized crime in the construction industry as creating both safety and security concerns. They also identified changes in the overall construction workforce, which suggest that the future NPP construction workforce may have greater opportunity to work serially at multiple plants, as increasing the opportunity for an insider to acquire knowledge of the construction process, security systems, and plant design.

Some experts also identified the security workforce at construction sites, including guards, as a potential concern in terms of reliability and diligence. They cited a number of instances in which security guards at operating NPPs have been found sleeping on the job,[48] and noted that a rapid and substantial increase in the demand for security workers, accompanied by the fact that security worker pay is fairly low, may make it difficult to recruit highly dependable and reliable persons for these positions. They noted that construction sites are likely to provide less permanent and desirable employment for security workers than operating plants, contributing to the challenge of finding and keeping trustworthy and reliable workers.[49]

Although these discussions focused on the ability of workers or outsiders with intent to threaten the security of the plant under construction and, through delayed impact threats, the operating plant, the experts also discussed the potential for an accumulation of unintentional errors and omissions to jeopardize security, both during construction and for the operating plant. In the discussions about delayed impact threats, they pointed out that, in addition to the potential for construction security threats to affect subsequent phases of the NPP life cycle, protection against some of the threat pathways involves other phases of the life cycle. For example, the security of the design and production phases for critical systems affects the threats that could exist during the construction phase, and, consequently, during the operating phase as well. Likewise, they cautioned that plant design itself impacts the types and level of threat risk during construction.

To derive additional information about the threat categories, the project team asked the experts to review a list of potential threats, add any threats they thought should be included, and, based on their knowledge and experience, rate the extent to which they

[48] Fatigue management among guards has been a persistent problem throughout the security industry. A recent illustration was provided by a video of sleeping guards at the Peach Bottom NPP in Pennsylvania that was covered in the *Washington Post* on January 4, 2008 (Mufson 2008).

[49] Paul Parfomak's (2004) monograph for the Congressional Research Service (CRS) provides a useful profile of this occupation and the impacts from the post-9/11 security context in the United States. The Project on Government Oversight (POGO) investigation into nuclear power plant security in early 2001 found that the security guards reported being under-manned, under-trained, under-equipped, underpaid, and unsure about guidance regarding the use of deadly force (POGO 2002).

thought the types of threats posed a serious concern to CIs under construction. Most of the experts on construction said that few of the types of threats listed had been given much attention in their CI sector and that, unfortunately, they and their colleagues had not yet systematically and fully examined threats that might occur during the construction phase. However, several noted the emergence of security consulting companies that provide integrated security planning and implementation to construction projects, and whose expertise is helping project owners apply a life-cycle perspective and security knowledge to facility planning.[50]

The experts then had several opportunities to discuss and assess the potential threat pathways in more detail and to identify those they considered to be of greatest concern. This discussion produced the following information about potential threat pathways:

- *Hidden explosive devices.* The specific pathways occur throughout the construction life cycle. For example, explosive devices that could be remotely detonated once the plant is operational could be hidden in the ground near critical plant components during site preparation, in the cement foundations, in electrical or other pipes as construction progresses, or in enclosed components, such as the HVAC, brought onto the site toward the end of construction. These pathways are vulnerable to internal and external perpetrators acting alone, but insider/outsider collusion would increase the probability of success of most of these pathways.
- *Compromised critical systems, especially software systems.* Critical safety- or security-related systems, including software systems, could be compromised at several points in the supply chain. Insider/outsider collusion increases the chances of successfully carrying out this kind of security threat, particularly if insider receivers and/or QA testers help prevent compromised systems from being detected.
- *Access to critical information.* It may be possible for individuals on the construction site to obtain a great deal of information about the facility design and security and safeguards procedures. A careful assessment of whether and how this information could add up to a safeguards or security concern is needed.
- *Immediate acts of vandalism or sabotage.* This threat pathway includes caching weapons or explosives on site for later use. According to media reports, it is thought that workers at the Spanish NPP, Lemoniz, smuggled explosives onto the site in small quantities over a period of time to assemble enough for a significant explosion. These types of threats, along with direct attacks discussed below, may be the most difficult to protect against, particularly if the adversary is prepared not to survive the attack. The perpetrators of vandalism and sabotage may have the intent of causing financial harm to the facility owner or disrupting the nuclear power industry (Purvis 1999)
- *Direct external attacks.* History indicates that this type of threat, up to and including missile attacks on NPPs under construction, cannot be dismissed. Factors that have historically been associated with direct attacks (such as truck bombs, missiles, etc.) from off-site are political-military conflicts and civil-political

[50]High-security government facilities and, to a somewhat lesser extent, casinos, appear to be an exception to this general statement. Experts reported that these facilities have conducted sophisticated threat and vulnerability assessments for many years, and design their construction process to take such threats into account.

opposition, either directly against NPPs or as part of a broader political conflict. There is evidence that insiders often aid such attacks. In a number of cases, these attacks have been so severe that the NPP under construction was destroyed or badly damaged.[51]

Table 4.2 presents a summary of these discussions about threats.[52]

Table 4.2. Expert Judgments Regarding Threats during Construction

Potential Threat Categories	Summary of Expert Comments
Hidden explosives	Considered among the most likely and consequential for immediate impact; potential difficulties with concealment while maintaining effectiveness lowered the rating for delayed impact use. Historical evidence of successful use (small amounts brought onsite over time)
Hidden surveillance devices	Hidden surveillance devices may not be as major a threat for NPPs as for facilities in which confidentiality and protection of sensitive information is more central (such as embassies, casinos, and other federal government installations)
Hiding/storing other types of materials that may be of use later	Considered a feasible, potential component of a larger threat strategy; hiding/storing materials, including weapons, has been used in the past
Delayed biocontamination (such as in HVAC)	Considered an unlikely choice as a threat strategy, (due in part to unfamiliarity with this threat); acknowledged as potentially highly disruptive if used
Compromised critical systems	Considered a potentially effective delayed impact threat, hard to detect, but requiring complex expertise, planning, and execution
Built-in weaknesses in security system(s)	Considered to be among the most likely threats, but probably not as a stand-alone strategy
Compromised materials	Considered by be likely enough to warrant prevention, but primarily because multiple motives could lead to this threat
Obtaining critical information about plant layout, security system, safety systems for sale or use	Considered by to be among the most likely threats, but probably not as a stand-alone strategy (i.e., need to combine with other threats to cause large consequence)

[51] 10 CFR 50.13 exempts licensees from providing "design features or other measures for … protection against the effects of attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person." This exemption has led to the parsing of what constitutes an "enemy of the United States." It has also played a central role in discussions about how responsibility for protecting against such attacks is, and should be, allocated among the federal, state, and local law enforcement agencies and the site owner. The distinction between an attack by "an enemy of the U.S." and a criminal attack was pointed out by Lymon (2003), who suggests that this may create a need for another agency, such as DHS, to take greater responsibility for the aspects of security for NPPs that do not fall under the jurisdiction of the NRC.

[52] See Appendix B for the interview guide used to structure these discussions.

Table 4.2 (continued)

Potential Threat Categories	Summary of Expert Comments
Sabotage (general)	Considered by experts to be among the most likely threats and to have high potential to cause immediate impacts, with disgruntled workers as or more likely than terrorists to perpetrate the sabotage
Fraud/theft/crime	Considered by experts to be among the most likely threats, but with somewhat constrained safety/security consequences because not undertaken to cause damage or safety consequences
Blundering and ineptitude	Considered to be likely and potentially costly; recognized as potentially enabling of other threats and potentially warranting greater prevention focus (rather than catch and fix)

5. Protective Measures

5.1 Overview of the Chapter

The published literature contains limited information about industry standards or practices to provide security during the construction phase of large-scale projects or CI facilities, particularly with regard to personnel security. Some sources do discuss physical security measures that could be employed to protect the construction site and reduce theft of materials and equipment (Abderrahim et al. 2004; Berg and Hinze 2005; DeVan 2003; Fournier 2006; Gill 2007; Khalafallah and El Rayes 2008; Kosnick 2005; Sowman 2005). Others discuss the causes of safety issues at construction sites, (primarily language issues, drug and alcohol use, and the nature of the construction activities) and protective measures to improve safety at construction projects (*Business Insurance* 2007; Chapman 2001; Construction Safety and Drug Abuse Executive Roundtable 2006; Contractors Association of West Virginia 2008; Haslam et al. 2005; Minchin et al. 2006; O'Malley 2001; Ohio Bureau of Workers' Compensation 2006; State of Ohio Legislature 2004; Thompson 2003; DoL). Only a few studies were found that specifically discuss either the need for or the practice of security measures during construction.

Therefore, the project team also gathered information through discussions with experts who had recent experience with construction projects across a range of critical infrastructure sectors. (These interviews are also described in Chapter 2, above.) The project team asked these experts to describe the typical construction practices in their sector and their views about whether those practices provided adequate protection against the types of security threats, new and old, discussed in this report. The experts were asked to discuss the sector in which they worked and then, to the extent that their knowledge permitted, to discuss NPP construction in particular. This chapter presents this information.

It should be noted that, consistent with its personnel security focus, the project team did not undertake to elicit detailed information about engineering, structural, or physical security measures during these discussions, although the open-ended nature of the questions led some experts to identify them as important security considerations. Although these measures are recognized as important, they are not addressed in detail in this report.

5.2 Standard Practice

The team's investigation of security measures at U.S. CI under construction since 2001 found examples of a wide range of security measures, but little evidence that a CI-wide standard of security practice had been or was being developed. The experts interviewed for the study noted examples of CI sites where one or more of the following types of measures or approaches were used during the construction phase:

- Plant design for security;
- Planning and contract requirements;
- Management and employee involvement programs;
- Physical security measures and systems, particularly guards, gates, and badges;

- Personnel security measures;
- Surveillance and inspections;
- Information and cyber security programs; and
- Supply chain security programs.

The personnel security measures reported being used at one or more CI-sector construction sites included:

- Pre-employment screening;
- On-site access authorization controls;
- Fitness-for-duty checks;
- Behavioral observation programs; and
- Close supervision.

All construction projects were reported to implement, at minimum, measures to prevent theft, fraud, and vandalism, primarily by controlling access to the site and secondarily by inspecting people, equipment, and materials entering and leaving the site.

Typical security-related measures reported across all CI sectors are focused on preventing access to the work site by unauthorized people and vehicles or by workers impaired by drugs or alcohol, keeping contraband items (drugs, alcohol, firearms, etc.) from being brought onto the site, preventing theft of materials from the site, and controlling where workers may go on site. According to the experts consulted for this project and the limited literature available, pre-employment measures to verify the identity of those accessing the site or to check on their character, criminal history, or associations have not typically been applied to construction workers in most CI sectors. These measures have been institutionalized in only a relatively few private sectors, primarily those subject to regulatory requirements (such as NPP licensees, casinos, facilities and personnel dealing with classified material), and then only sparingly, during construction. Notably, such measures were reported to be much more uniformly applied to workers at facilities being constructed for the Federal government, facilities being built on shared sites, and facilities and workers subject to licensing requirements.

The increased attention to terrorism and insider threats following 9/11 began to change the typical patterns. As described in Appendix B, federal initiatives to address illegal immigration, control fraud and exploitation of minors, and to address general "homeland security" considerations have led to considerable expansion in the number and types of individuals subject to requirements for fingerprinting, criminal history checks, and acquisition and use of "credentials" affirming their true identity. An increasing number of these "credentials" (badges, licenses, documents, and passports) include not only photographs but biometrics as well. Examples include the federal programs requiring all federal government employees to be fingerprinted and to obtain a new "personal identity verification" card/badge; for transportation workers to obtain a "transportation worker identification credential" (TWIC); and for all employers to ensure that employees provide the documentation necessary to verify their identity and legal status and to complete the I-9 Form. Despite these initiatives, the experts reported that typical construction security practices have not changed much over several decades, and that 9/11 has only affected

construction security for a few select sectors, such as airports, ports, and government-owned facilities.

The experts were unanimous in noting that it is the owner of the facility who determines what security measures are to be employed during construction, and that unless the owner imposes security measure requirements on its contractors, they are unlikely to be implemented. They emphasized repeatedly that cost considerations dominate decisions about security measures during construction in the private sector. They also unanimously observed that the issue of security during the construction of critical infrastructure and high-asset facilities has been discussed very little and is only rising to prominence. All agreed that, for their sectors, examination of the need for additional security measures during construction and identification of best practices is needed. Unless CI facility owners gain a stronger sense of the need for security during the construction phase, or external requirements are imposed on CI facilities, the experts agreed that implementation of measures to ensure construction security were likely to remain spotty and fairly minimal.

That said, the experts indicated that state and federal regulations governing the health and safety of workers and environmental protection, particularly those of the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) and the U.S. Environmental Protection Agency (EPA), are taken seriously. Though often not considered security related, these regulatory requirements have nevertheless resulted in widespread adoption of some security-related measures. The experts frequently noted that both the regulations and their enforcement are becoming more stringent, and that compliance is increasing as contractors learn through experience that violations are likely to have significant financial consequences.

The team's investigations indicated that, largely driven by these health- and safety-related requirements, the following measures are frequently employed on construction projects throughout all the sectors:

- Controls to limit site access to authorized personnel (fences and gates);
- Badging to identify authorized personnel;
- Maintaining records of worker presence and location on the site;
- Regular, required safety and health briefings;
- Pre-employment and for-cause drug and alcohol testing, and, in an increasing number of instances, random drug and alcohol testing during employment; and
- Reporting requirements for accidents and/or exposure to hazardous materials.

Background checks, often including fingerprinting and criminal history checks, are a prerequisite for employment in a wide range of professions, sometimes including construction, as discussed below.

Both the literature and a number of those interviewed pointed out that, just as security and safety can be jeopardized via many pathways, they can also be provided or reinforced by multiple methods. Several of the experts spoke at length about the importance of effective measures to ensure implementation of safety, security, and quality measures. They also noted the potential for worker ineptitude or corruption to

jeopardize quality assurance and quality control processes. Indeed several had been involved in efforts to detect, prevent, and counteract such problems. They stressed the need to assure rigorous implementation of QA/QC procedures, but also pointed out that a greater emphasis on measures to prevent problems might be more effective than relying on QA/QC processes to catch errors or problems after they occur.

The experts indicated that typical quality assurance and quality control practices required of construction contractors now include:

- QA/QC procedures and documentation requirements;
- External QA/QC assurance teams;
- Materials and equipment acceptance programs that include verification sampling, testing, and inspection; and
- Quality control procedures that require rigorous sampling requirements and use of certified, independent laboratories.

Among the variety of facility types represented by those interviewed, only government-controlled, off-shore oil drilling, chemical plant, and casino facilities applied comprehensive access authorization and fitness-for-duty measures during construction for separate sites.[53] In general, the experts reported that personnel security measures similar to those at the operating facility were applied to construction workers when the construction site was proximate to or interspersed with an operating facility. For example, workers building a shared-site liquefied natural gas (LNG) facility were subject to the same full-scope personnel security program as the workers at the operating LNG facility. This was also true for construction workers at shared-site port, airport, and DOE construction projects. Aside from facilities being constructed for the federal government, and those whose workers were required to obtain security clearances, none of the CI sectors addressed in this study required psychological testing of construction workers. This does not mean that some workers might not have been subject to such requirements as part of their overall employment, but only that the on-site security measures did not include a psychological testing component.

A number of those interviewed also pointed out that the complex nature of construction workforces should be taken into account when considering personnel security measures during construction. Most construction projects involve many different companies. While many of the workers on a particular construction project may be hired specifically for that job, a number of others may be long-time employees of those companies and may be subject to company, rather than project-specific, personnel security policies and measures. Thus, implementing security measures that cover all workers at the site uniformly will be complex, and may require employers to either redo elements of the security program or develop methods to validate and integrate employee records for use at the project. This complexity is likely to increase security program costs.

[53] One expert indicated that individual utility policy led one utility to apply the operating plant personnel security measures to workers constructing a nuclear power plant during the 1980s, even though this was not required by regulation and was not the common practice in the industry. In the chemical and off-shore oil examples, the experts identified "special considerations" (e.g., particularly high threat context; intellectual property protection) as drivers of the extensive security measures being implemented.

Drug and Alcohol Testing

The experts consulted for this project rated cumulative errors and insider-outsider collusion as threats of concern. Impaired workers, or workers addicted to illegal drugs, were considered both safety and security threats and as unreliable workers, likely to have poor attendance and low efficiency. However, initially, most of these experts did not think of workplace drug and alcohol testing as a security-focused protective measure. Rather, they considered them to be safety-related measures. Upon reflection, they subsequently rated workplace testing as an important protective measure for both safety and security.

Concerns about impaired workers and the consequences of illicit drug use have led an increasing proportion of employers to implement drug policies and workplace drug and alcohol testing programs. Caplan and Huestis (2007:732) estimated that almost half of the American workforce was subject to testing for illegal drugs, and Reynolds (2005:7) reported that 67 percent of all major U.S. corporations had drug-testing policies. A growing number of construction industry representatives, including crafts unions, have endorsed drug and alcohol testing of construction workers, acknowledging the high incidence of drug and alcohol use among constructions workers and the role it plays in on-site accidents and safety incidents (*IBEW Journal* 2005). For similar reasons, a growing number of states have passed regulations to either explicitly allow or require random drug testing for workers on construction sites.

Comprehensive workplace drug and alcohol testing programs typically include provisions for pre-employment, for cause, post-accident, random, and follow-up testing. Both the available literature and the experts consulted indicated that pre-employment, for-cause, and post-accident testing were increasingly common for construction workers in all sectors. Random testing of construction workers was reported to be less common, particularly at projects with a high proportion of temporary workers. Considering the persistent issues of drug and alcohol use and workplace impairment among construction workers and the vulnerabilities created by drug and alcohol addiction, the experts emphasized the importance of keeping impaired workers and addicts off the construction site. They acknowledged the logistical challenges of implementing random drug and alcohol testing for a workforce with high turnover and intermittent schedules and indicated that technologies that would allow on-site, immediate identification of drug and alcohol use would make this approach much more useful for construction sites.

Identity Verification and Badging

All the experts consulted for this project agreed that identity verification and badging were essential elements of every site security program. As discussed in Appendix B, since 9/11 the federal government has made a concerted effort to improve the technologies for and expand the use of identity verification and badging, or credentialing. Security managers noted that recent investments had resulted in badges/cards and reader technology that made managing site access easier, more reliable, and more efficient. The federal requirement for all employers to confirm the identity and immigrant status of every employee (Form I-9) establishes a minimum standard that all construction projects will have to meet. Some of the experts consulted for the study indicated that access control technologies using biometrics, including fingerprints, were likely to come into increasing use, particularly on sites with large numbers of workers

entering and exiting at the same time. Several experts reported that the access control/security systems at some construction sites were already using technology that could be programmed to restrict access to specific areas on the site and to provide a record of when and where the worker was on the site. This was reported to be particularly useful for sites such as casinos, banks, and nuclear power plants, where access control needs to become more restrictive and controlled as construction progresses.

Terrorist Screening

The federal government initiated the development of a terrorist screening process following 9/II to provide a way to check quickly and at any time whether an individual is on the terrorist watch list. Established within the Federal Bureau of Investigation (FBI) by Homeland Security Presidential Directive (HSPD) 6, the terrorist screening database consolidates the government's information about known or suspected terrorists into a single, searchable database (see description in Appendix B). It is designed particularly for federal, state, local, and tribal law enforcement agencies, the U.S. State Department, the Bureau of Citizenship and Immigration Services, and the Transportation Security Administration and, increasingly, employers at CI facilities. The TSC process does not include or reference information on criminal histories. Though more effective when the fingerprints of the individual are included, they are not required for the screening process. The Terrorist Screening Center operates 24/7 to support rapid screening of individuals, for example for transportation security, border security, or customs officials. The experts agreed that submitting employee information to the Terrorist Screening Center was a way to provide an additional level of assurance that known terrorists were not being hired for jobs at CI facilities. Most of the experts consulted for this study did not express an opinion about the effectiveness or utility of the terrorist screening process; however, several reported that they were familiar with instances when the screening process identified individuals on the watch list. The restrictions on fingerprinting and access to FBI criminal history record information that apply to entities regulated by the NRC[54] do not apply to submittal of names to the terrorist screening process.

Fingerprinting and FBI and Local Criminal History Background Checks

In pre-employment screening, personal information and fingerprints are used to match individuals with the criminal history records maintained by the FBI. Until recently, records of the fingerprints of individuals without a criminal history were not retained in the FBI database. This is the reason that each time a background check is conducted, a new set of fingerprints is collected. The Fingerprint Identification Records System (FIRS) of the FBI now maintains identification and criminal history record information on individuals fingerprinted:

- As a result of law enforcement action;
- For federal employment or military service;
- For alien registration and naturalization purposes ("a limited number of persons");
- To have their fingerprints on record for personal identification purposes.

[54] Only licensee employees can be authorized to have access to FBI Criminal History Record Information. Divulging this information to others risks violating 28 USC 534 and 42 USC 2169.

The Attorney General of the United States is authorized under 28 U.S.C. 534 to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records and to exchange such records and information with, and for the official use of, authorized officials of the federal government. The FBI, which has had major responsibility for fingerprint identification since 1924, maintains an automated database that integrates criminal history records submitted by state, local, tribal, and federal criminal justice agencies. Each state has a criminal records repository that is responsible for collecting and maintaining the criminal history records submitted by the law enforcement agencies in the state. State record repositories are the primary source of criminal history records maintained at the FBI (U.S. DOJ 2006:13).

The FBI's Criminal Justice Information Services (CJIS) Division, which was established in 1992, is the central repository for criminal justice information services in the FBI. It administers the FBI's Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Instant Criminal Background Check System (NICS). The IAFIS provides automated fingerprint search capabilities, latent fingerprints, and responses using "life-scanned" fingerprints (i.e., fingerprints are collected on a machine that captures the fingerprint image digitally), although it can also process paper fingerprint submissions. It also operates the Interstate Identification Index (III), a component of the IAFIS designed to provide automated, searchable criminal history record information based on records of federal offenders and records of offenders submitted by all states and territories. The III includes identification data such as name, birth date, race, and sex, and contains FBI and state identification numbers from each state that has information about an individual. By the end of 2005, 48 states were participating in III (U.S. DOJ 2006:13). There are restrictions on who can access this information. The Bureau of Justice Statistics, which operates this program for the FBI (U.S. DOJ Bureau of Justice Statistics 2007) states that:

> "NCIC data may be provided only for criminal justice and other specifically authorized purposes. For criminal history searches, this includes criminal justice employment, employment by Federally chartered or insured banking institutions or securities firms, and use by State and local governments for purposes of employment and licensing pursuant to a State statute approved by the U.S. Attorney General. Inquiries regarding presale firearm checks are included as criminal justice uses."

The post 9/11 period has seen an expansion in the range of workers subject to fingerprinting and criminal history checks. Both the federal government and state and local governments have imposed requirements for workers and license applicants to be fingerprinted and subject to criminal history checks. In addition to all federal government employees and anyone working in a secure area at a port or airport, workers in the following jobs are subject to these requirements in at least some states: 1) construction workers when working at sites where children are present; 2) all federal workers; 3) health care workers; 4) individuals applying for a gambling/gaming license; 5) day care workers; and 6) individuals employed at federally insured financial and banking institutions.

Most of the CI construction projects described to the project team did not subject workers to fingerprinting or FBI criminal history background checks. Exceptions were projects whose workers were subject to an external requirement either because of the

nature of the project (e.g., involving classified information or facilities) or the sector/occupation (e.g., transportation workers at ports and airports, casino workers) and a project in which the facility owners were responding to a heightened threat environment (e.g., the off-shore oil platform construction project, which was a non-U.S. project). In addition, some facility owners (for example, an LNG project) required construction workers to be subject to criminal history background checks, but without fingerprinting. In some cases, this was because the employer was not authorized to impose a fingerprinting requirement on the workers.

The experts reporting on facilities that used local criminal history background checks indicated that these checks were typically part of a comprehensive construction security program and were often provided by a contractor specializing in personnel security measures. The experts generally considered fingerprinting and criminal history checks to be useful tools for enhancing site security. They pointed out that maintaining security files on each construction worker would add to the administrative burden and increase recordkeeping costs for the owner/licensee, who would be required to demonstrate that the requirements were being met. This was identified as a special burden at projects which otherwise would maintain only payroll files for construction workers.

Employment History and Character Checks

The experts indicated that employment history and character checks, when conducted, were more often considered part of the organization's pre-employment human resources due diligence process than its security program, unless specifically required by security clearance or regulatory requirements. Nevertheless, the experts agreed that employment history and character checks, though time consuming, did provide employers useful information about the trustworthiness and reliability of potential employees. All the projects dealing with classified materials or facilities, plus the chemical plant, LNG facility, casino, and information-sensitive embassy construction projects, subjected construction workers to background checks that included some degree of employment histories and character checks.

Escorts, Behavior Observation, Monitoring, and Supervision

The experts reported that it was standard procedure at construction sites to require escorts for visitors, including delivery vehicles. The degree of concern for security influenced the rigor of the escort program and the records kept on visitors and vehicles entering the site. A number of experts emphasized the critical role supervision and supervisors play in maintaining site safety and security. They noted that management's commitment to and support for security greatly influenced the on-site behaviors of supervisors and workers. The experts agreed that alert workers and supervisors, if so motivated, provide the best resources to reinforce security measures and identify vulnerabilities and lapses. The experts described few instances of formal behavioral observation programs at the projects they knew about, but noted that security was being integrated into the regularly scheduled safety meetings at some projects, a development they considered an example of best practice. The behavioral observation programs identified in the study emphasized what to look for and how to report suspicions of inappropriate behavior. They noted that awareness of the importance of safety measures on construction sites was reflected in programs that emphasized industrial safety.

Monitoring technologies, such as smart badges, access controls, and cameras, had been used at a number of the projects described by the experts, who said they expected these technologies to be increasingly ubiquitous at construction sites in the future. They thought these types of technologies would also be used to enhance quality assurance and quality control programs. One expert familiar with construction quality assurance issues indicated that these technologies, combined with peer checking and close supervision, were critical to prevent fraud and carelessness at complex construction sites.

Adequacy of Protection

The project team asked the experts whether construction practices in general, not just construction security practices, provide adequate protection against the potential threats they thought warranted attention at CI construction sites. Adequate protection would mean that all the potential threat pathways have protections commensurate with their level of potential risk.

There was consensus among the experts that neither typical construction practices nor industry standards and regulatory requirements governing security, occupational health, safety, and environmental protection, and QA/QC practices provide adequate protection against the security threats of concern these facilities may face.[55] Several of the experts associated with the nuclear industry pointed out that in earlier nuclear plant construction projects, work and material quality deficiencies, combined with deficiencies in QA and QC programs caused major problems (Altman et al. 1984; GPO 1982; U.S. NRC 1982a-c; Willamette Week 1981; Winslow 1984). NUREG-1055 (U.S. NRC 1984) discusses these issues.[56] Similar problems with poor work or materials and inadequate QA/QC programs have also occurred with other large-scale construction projects. For example, the Trans-Alaska Pipeline project experienced serious problems that resulted in significant delays, additional costs, and political investigations (U.S. House of Representatives Energy and Commerce Committee 1993).

Quality problems have proven difficult to resolve. Although quality practices have evolved to some extent since the first wave of U.S. NPP construction, recent investigations of safety and QA/QC practices during nuclear construction in other countries indicate that serious issues still exist. Some of the same quality control problems experienced during the construction of the first round of U.S. plants have been identified at the Olkiluoto plant in Finland, at the Rokkasho Reprocessing Plant in Japan, and at the Areva Shaw MOX fabrication facility construction project in South Carolina (Nuclear Engineering International 2006; Goodall 2008; Russell 2008).[57] These

[55] Managers of government-sponsored projects that implemented full-scope security measures during the construction phase, often because the facility was embedded within a secure site that also included operating facilities, had higher confidence that adequate protection was provided. However, they did not consider their projects to represent "typical" construction practices.

[56] These problems led to the NRC staff proposing a long-term review and study of quality problems in the nuclear industry, and a case study at six nuclear power plants under construction. The quality problems involved both design and construction, and were found to be related to inexperience. (U.S. NRC 1984, NUREG-1055; U.S. NRC 1982 SECY-82-352).

[57] Excerpt from a WGHOF (working group on human and organizational factors) meeting held October 2006 regarding construction issues for the Olkiluoto 3 EPR in Finland found that safety, generic engineering culture, and quality assurance were questionable in many instances and control over the subcontactors by both the vendor and the licensee failed in the Olkiluoto case.

problems include issues with welds, rebar, and cement and are being attributed to inexperience and inadequate management (Lean and Owen 2008; Russell 2008; Sassoon 2008).

Experienced construction managers among the experts indicated that, even if construction contracts specify heath, safety, and quality controls, the number of subcontractors and the intensity and complexity of site activities tend to make adequate control and coordination difficult. Experience also indicates that inexperience with the particular management and task requirements has been an important source of construction phase quality problems (IAEA 1999; Goodall 2008; Sawai 2001). Both the literature and experts consulted for the project identified the rapid growth in the number of nuclear power plants being built during the first round of NPP construction as a factor contributing to the quality problems and warn that these problems could reoccur if this pattern of rapid growth is repeated.

Given this history, and the importance of QA/QC compliance, some of those interviewed stressed the importance of assuring that those responsible for security, safety, and QA/QC exhibit the highest level of trustworthiness and reliability. However, they noted that personnel security measures for these types of workers during construction typically do not provide such assurance.

These experts also emphasized the frequent failure of typical construction practices to screen all components as carefully as needed to detect hidden explosives. They pointed out that typical security measures for inspecting and testing systems during construction do not adequately address the supply chain pathways. This is the case even though an increasing proportion of components and materials are being purchased from foreign suppliers. Reliance on foreign suppliers makes the supply chain longer, more complicated, and, usually, less familiar and more difficult to verify. The experts also noted that, because protection against individuals attempting to obtain critical information via the supply chain is typically not considered, protective measures against this potential threat are seldom implemented.

In summary, the experts interviewed for this project agreed that typical construction practices are insufficient to assure security of construction sites. They also agreed that a thorough assessment of the threat pathways was needed to evaluate what measures would provide adequate security. They were not aware that such an assessment had been conducted. The experts pointed out that ensuring greater security during construction also requires attention to plant design and siting, supply chain structures and requirements, and workforce screening and selection. The methodology for vulnerability assessment developed by Sandia National Laboratories for chemical facilities, which includes features of the site that affect its accessibility and recognizability, was cited as an example of a tool that could be used to structure such an assessment (U.S. Department of Justice 2002).

5.3 Expert Opinion about Potential Protective Measures

Protective Measures to Assure Security

The experts were asked to identify what measures they believed would adequately protect CI under construction in the post-2001 threat environment. The project team

also reviewed initiatives underway to enhance the security and resilience of U.S. critical infrastructure across sectors to identify protection initiatives of potential relevance to NPPs.

Regarding measures needed to adequately protect CIs under construction, the experts emphasized that protection needs vary by CI sector. For example, they noted that, at some facilities subject to high surveillance threats, security specialists would consider monitoring systems to detect hidden surveillance devices necessary to achieve the desired level of security. One expert, who had overseen security during the rebuilding of the U.S. embassy in Russia (after it was torn down as a result of discovering hidden surveillance devices), said that CI facilities such as embassies might be best thought of as security projects with a construction focus. He observed that this was certainly not true of NPPs, whose complex engineering and construction requirements created challenging demands on the construction managers. He suggested that, compared to embassies, projects like NPPs might be thought of as simultaneous construction and security projects.

As discussed in Chapter 4, the experts were asked to discuss and assess potential threats to CIs under construction and the threat pathways associated with them. The experts were then asked to rate a list of possible measures in terms of their importance in addressing those potential threats. The list included physical security, personnel security, supply chain security, cyber security, and security interfaces with safety and QA/QC measures. The experts were asked to add any important measures not included on the list. The revised list and a summary of expert judgments about the potential security measures are shown in Table 5.1.

Potential Protective Measures for Threat Pathways of Greatest Concern

The experts were then asked to discuss potential protective measures specific to the threat pathways considered to be of greatest concern for CIs under construction. Their observations were as follows:

- *Hidden explosive devices.* Protecting against pathways involving hidden explosive devices could involve thorough explosive detection measures for everything and everyone coming onto the site and/or thorough explosive detection covering all critical areas and facilities on the site at key points during their construction.
- *Compromised critical systems, especially software systems.* Protection against this threat pathway has to begin at the initial phase of the supply chain for each system with the potential to impact the safety and/or security of the operating NPP. Software systems may be particularly vulnerable because developers could embed hidden messages or commands, known as Easter eggs, in the code that are designed to avoid detection by typical software testing procedures. The Easter eggs could be designed to activate when a set of favorable conditions occurs, thus potentially contributing to propagation of a significant nuclear event. Several possible protective strategies include: (1) directing personnel security at particular supply chain workers, such as software developers, code reviewers, and software system testers and/or (2) implementing state-of-the-art security-oriented techniques and technologies.

Table 5.1 Summary of Expert Judgment Regarding Need for Enhanced Measures to Address Threats

Security Measures	Comments
Pre-Construction Plant Design ➢ Life-cycle perspective ➢ Increase standoff ➢ Maximize physical protective barriers ➢ Increase structural integrity and resiliency (load issues, etc) ➢ Decrease collateral damage (types of materials, windows, etc. ➢ Enhance fire resistance ➢ Improve emergency egress and access ➢ Facilitate security response ➢ Enhance resiliency if a critical system fails ➢ Maximize the ability to isolate compromised/damaged components to minimize the downtime (and costs) of recovery ➢ Separate design drawing responsibilities across multiple subcontractors	TISP workshop participants emphasized the value and importance of considering security during construction during the design phase. Experts agreed that a life-cycle perspective on threats and protective measures was useful. Experts recommended that attention to the pre-construction design phase could save money and enhance security. Because few of these measures involved personnel security, they were not addressed in detail and were not rated by many experts, but were a topic of interested discussion and emphasis.
Construction Planning & Requirements ➢ Additional security specifications in construction contracts with clear enforcement/incentive measures ➢ Security liability agreements ➢ Good risk management planning ➢ Life-cycle perspective	As with the previous category, both TISP workshop participants and other experts recommended construction planning and the establishment of requirements as ways to enhance both construction, and subsequent operation security cost effectively. They rated each of the individual items important and useful, particularly good risk management, which was rated very important, followed closely by additional security specifications in contracts with clear enforcement/incentive measures. Experts consulted for the study supported the life-cycle perspective and emphasized the importance of addressing security measures in contracts.
Management/Employee Involvement ➢ Have owner staff on construction management team ➢ Good labor/union relations ➢ Strong security culture & awareness/training programs ➢ Broad scope behavioral observation program that includes security	The experts generally rated the items in this category as moderately important to security. They considered behavioral observation programs that included security to be quite important, the most important in this group. Owner staff participation and a strong security culture and awareness training programs were rated fairly important to security, but subsequent discussions emphasized the importance of management support. The experts rated good labor/union relations as only slightly important to construction security.

Security Measures	Comments
Physical Security ➢ Badging/proximity cards ➢ Perimeter access/exit controls ➢ Interior access controls ➢ Intrusion detection (alarms/security seals/tampering indicating devices)	The items in this physical security category received variable importance ratings by the experts. Perimeter access/exit controls were rated as quite important, but subsequent discussions identified badging and perimeter controls as essential, standard staples of construction security. Badging/proximity cards were rated fairly important. The experts considered intrusion detection measures and interior access controls less important.
Personnel Security ➢ Biometric access controls ➢ Identity verification ➢ Background checks ➢ US citizen requirements ➢ Local crime checks ➢ Fingerprinting & national crime check ➢ Terrorist Screening (TSC) ➢ Pre-employment psychological testing ➢ Pre-employment drug testing ➢ For-cause drug testing ➢ Random drug testing ➢ Behavioral observation program that includes security ➢ Escort program ➢ Higher supervisor/worker ratios	Experts rated identity verification and background checks as very important. Pre-employment psychological testing and TSC screening were not rated by many of the experts in the initial rating process, some of whom reported a lack of familiarity with TSC screening. In subsequent discussions some experts mentioned psychological testing as a potentially useful measure for those employees in positions of trust. Some experts at the TISP workshop recounted positive experiences with TSC checking. Some of the experts rated local criminal history checks and fingerprinting and national crime checks as not very important. Expert opinion was divided about whether national or local criminal history checks were more effective. Many of the experts considered it important to check the background of potential employees. The remaining items were considered moderately important to security.
Surveillance/Searches/Inspections ➢ Surveillance cameras ➢ Undercover security agents (also see “Devious Dan” program in Other) ➢ Roving security patrols ➢ Periodic searches for explosives ➢ Perimeter entry/exit searches ➢ Security walk downs/spot checks ➢ Chain-of-custody requirements ➢ Security-informed QA/QC ➢ Security-oriented material/component inspection & testing of all key components ➢ X-raying, scanning, sniffing key components ➢ Red team security inspections	Experts considered surveillance cameras and spot checks very important to security, followed closely by inspection and testing of key components. Roving security patrols, periodic searches for explosives, and ex-raying /scanning key components were rated as moderately important, although subsequent discussions of potential threats led some experts to consider these measures more important. Perimeter entry/exit searches were rated only as somewhat important, and chain-of-custody requirements were rated not very important. Subsequent discussions indicated that site security programs at a number of sites rely on entry/exit searches, which was a common practice at first round NPP construction sites. Undercover security agents, security-informed QA/QC, and red team security inspections were rated by only a few experts, who generally rated them as important in some circumstances.

Security Measures	Comments
Information and Cyber Security ➢ Divide and fragment work ➢ Audits ➢ 2-person administrator rule	The information and cybersecurity items were added in the course of discussions and therefore did not receive systematic ratings. Discussions indicated that experts consider these items increasingly important to security.
Other ➢ "Devious Dan" programs** ➢ Location monitoring that allows analysis of "approaches" to work areas	Experts familiar with QA/QC validation at large-scale construction sites were very enthusiastic about validation/challenge programs such as "Devious Dan" programs.
Supply Chain Protection Measures (materials, components, software systems): ➢ Greater security-oriented specifications in vendor contracts ➢ Vendor background checks and assessments ➢ Personnel security requirements for key vendors & off-site contractors ➢ Spot checks of vendors ➢ Having owner oversight personnel located at vendor sites ➢ Built-in software protections & code alteration detection capabilities ➢ Certified and tracked chain of custody ➢ Tamper proof containers/packaging	The experts consulted for this project included several who were firm advocates of supply-chain security and who emphasized the importance of implementing a complete supply-chain security program during construction. Few experts rated these items during the initial rating process. In subsequent discussions, a number of experts indicated that their initial concept of construction security had not extended to the supply chain. However, following discussions of the potential threats to the supply chain, many of the experts indicated that supply chain security during construction appeared sufficiently important to warrant careful attention.

*** A "Devious Dan" program involves having randomly selected persons assigned to do things to intentionally test the performance of various aspects of the protection program.*

Experts recommended that the most effective protection strategy might be to distribute development of the product among a number of suppliers. Using software systems as an example, this would mean implementing procedures to (a) distribute code development among different providers, making it difficult for them to design and embed effective Easter eggs; (b) have highly competent and trustworthy individuals review and certify all critical software; (c) use a public key of the certification to detect any changes made to the software after this point by running algorithms that would be very difficult to elude; and (d) build into all significant systems the ability to detect whether the code has been altered. While it is difficult to create effective Easter eggs that will both produce the intended outcome and avoid detection, it is also difficult to find these Easter eggs prior to certification. Moreover, building code into systems to detect changes in other software systems may have to pre-date the construction phase – it may actually need to be initiated during plant design and continued into construction.

If these protection strategies are not built into the software, the experts warned that software security during construction can be a much bigger concern. The experts pointed out that this strategy places increased demands on management and system integration, and has the potential to introduce other errors in the system.

- *Access to critical information.* Protection strategies would require implementing measures to ensure that work was structured and distributed in a way that prevented workers from obtaining too much information. Increasing attention to this potential threat is needed before the construction process proceeds to the point that critical information is revealed.
- *Immediate acts of vandalism or sabotage.* The extent of personnel oversight and physical security can be limited on a construction site because there are so many workers and the site is so open. It may be possible to protect an adjacent operating plant from exposure to sabotage stemming from the construction site, but protecting the construction site is expected to be extremely difficult. Protective strategies might include hidden observation cameras and enhanced behavioral observation programs that focus on security as well as safety issues and include training and participation on the part of supervisors, QA/QC, and workers.
- *Direct external attacks.* History indicates that this type of threat, up to and including missile attacks on NPPs under construction, cannot be dismissed. Factors that have historically been associated with direct attacks (such as truck bombs, missiles, etc.) from off-site are political-military conflicts and civil-political opposition, either directly against NPPs or as part of a broader political conflict. There is evidence that insiders often aid such attacks. One of the purposes of personnel security measures would be to detect and deter such insiders.

Security Initiatives of Potential Relevance to CI Construction Security

A number of current initiatives to enhance the security and resilience of U.S. critical infrastructure have the potential to affect the costs and benefits of providing enhanced protection during NPP construction.

As described in more detail in Appendix B, presidential initiatives and programs undertaken by the Department of Homeland Security and other federal agencies are changing the security landscape in the United States. Sector-specific directives to assess and improve security at critical infrastructure facilities are affecting a growing proportion of the CI sectors at the facility level and may develop into additional regulatory requirements. In addition, a number of initiatives will have direct consequences for individual workers.

Perhaps the most widespread consequences of these governmental initiatives will result from the series of initiatives regarding proof of personal identity. These initiatives require employers and state licensing agencies to impose new, more stringent standards for verifying the identity of individuals, for example, at borders and for employment applications. They also require individuals to acquire and present standardized "smartcard" identification credentials in order to work in particular sectors (for example, maritime and air transportation and federal agencies). These requirements for verifying

identity and citizen/immigrant status are being imposed on all employers (Form I-9), federal employees (Personal Identity Verification (PIV) cards), and transportation workers, especially those involved in maritime commerce (Transportation Worker Identification Credentials –TWICs).

Associated with these initiatives to require verification of individuals' true identity are multiple federal initiatives to develop the data and methods to improve the effectiveness and speed of background checks. These initiatives include the Terrorist Screening Center, the FBI's fingerprint and criminal records databases and screening tools, and broader requirements for who is subject to screening. In the course of implementing these programs, both the sponsoring government agencies and their contractors have done considerable work to develop and refine both the technologies (tamper-resistant badges; badge readers, etc.) and to develop criteria for determining that an individual is eligible for the credential (e.g., what background information is disqualifying, what are the appeal procedures, and so on).

The focus on homeland security has created a number of initiatives to improve technologies for surveillance and screening of individuals. The development and deployment of these technologies at public facilities and work places are likely to affect both the tools that are available for use at NPPs, and the expectations of workers about being subject to surveillance and screening, both for access and during the work day.

There is little question that by the time NPP construction is underway, expectations concerning security and the procedures for verifying true identity and criminal history/terrorist links will be quite different than they are in 2009.

5.4 Summary

The expert opinion and secondary data assembled for this analysis indicate that enhanced protection measures are warranted for at least a subset of CIs under construction and that this subset includes NPPs. The experts and relevant literature indicate that the security measures deployed for CIs during construction in many sectors are inadequate to protect against post-2001 threats. Enhanced requirements for security during construction have been established for several CI sectors, including seaports and airports, military bases, foreign embassies, and many federal government facilities. Enhanced security measures are warranted for NPPs under construction. The full range of potential security measures are being applied to the construction phase in some sectors and by some facility owners, demonstrating that these measures can be deployed in a construction setting.

This investigation found that enhanced security measures are generally implemented only in response to regulation, as with casinos and ports, or as a consequence of owner specifications. However, the experts warned that cost and schedule pressures, along with how risks incurred during the construction process are allocated among contractors and owners, often lead owners to accept higher risks than may be in the public interest. Regulatory and cost/benefit analyses of alternative requirements were beyond the scope of the study. However, expert opinion is that the consequences of inadequate security during construction could be extremely high, and that enhanced security measures would have ancillary safety and efficiency benefits that may partially offset the costs of

implementation. In addition, measures taken during the design and siting phases could reduce the need for or cost of security measures during construction.

In addition to information about the specific security measures discussed above, the experts provided the following general observations about the construction industry and factors affecting security needs and measures:

- The construction industry is highly cost and schedule driven. The facility owner determines whether and what security requirements will be implemented. Without either regulatory requirements or requirements imposed by the entities financing and insuring the facility, decisions regarding what security measures to implement will be determined by the owner's balancing of those measures' costs with their expected benefits. In part these decisions are driven by direct costs, but the potential for other costs such as law suits, labor conflicts, and delays resulting from the imposition of pre-employment or workplace screening and selection procedures are important considerations.
- Personnel security measures are significantly influenced by OSHA requirements and resulting liability exposures. Concern for compliance with environmental, and health and safety regulations was often cited as the driving factor in heightened use of and attention to drug and alcohol testing, badging, site access control, and behavior observation programs. Responsibility to implement and comply with these requirements was often vested in the entity responsible for managing on-site construction.
- Construction has among the highest industrial accident rates of any occupations. Errors and accidents from impairment, carelessness, or lack of adequate supervision, training, and equipment were cited as the major sources of problems at most construction sites, followed by incidents of fraud and vandalism for sport or revenge. Increased attention is being given to preventing work place violence by disgruntled or mentally unstable workers following multiple incidents in the U.S. that have resulted in deaths and severe injuries.
- Construction projects that require construction workers to have access to all or part of an operating facility tend to employ extensive personnel access authorization and fitness-for-duty measures, frequently the same as for operational workers. Responsibility for implementing elements of these programs is often contracted to specialty companies. Large-scale CI construction projects being conducted within or proximate to operating facilities with security concerns tend to have a full-time security manager.
- The study found full-scale access authorization and fitness-for-duty programs being implemented during construction at (a) federally-owned or -controlled facilities (e.g., embassies, government laboratories and production facilities, offices in which sensitive activities are conducted or information stored); (b) sites where construction required or provided the potential for workers to gain access to an operating facility that employs personnel security measures (e.g., LNG facilities, ports and airports); (c) the later phases of construction in facilities under regulations that require personnel controls (e.g., casinos); (d) facilities being constructed within a particularly high threat context (e.g, off-shore oil platforms); (e) facilities protecting process-related intellectual property (e.g., a high-tech chemical facility); and (f) NPP construction sites where an existing unit is already operating.

- Managerial attention is a scarce resource on large-scale construction sites, particularly those as complex as nuclear plants. When both the management and the workforce are inexperienced with these types of projects, problems may multiply. Many of the problems with the first wave of NPPs were attributed to management inexperience and to an inadequate number of experienced personnel to expand management as project demands increased and became more complex. The new NPPs now being built in France and Finland are experiencing these same problems.

6. Construction Security Strategy and Enhanced Personnel Security Measures

6.1 Overview of the Chapter

This chapter builds on the discussions of the need for security at NPPs under construction and effective prevention measures in Chapters 2 and 3, and focuses specifically on the technical basis for possible NRC requirements to promote personnel security during the construction phase of NPPs. This analysis is based on the systems-based life-cycle approach described in Chapter 2. It considers the conclusions reached about the validity of the claims that there are threats to NPPs under construction whose prevention, deterrence, and mitigation fall within the jurisdictional authority of the NRC. It is also considers the information presented in Chapters 4 and 5 about standard practices during CI construction and the role regulation plays in the application of personnel security measures at private sector facilities. It concludes that the NRC is warranted in imposing personnel security measures to prevent, deter, and mitigate threats of concern during the construction phase of NPPs.

The chapter examines the pathways by which personnel could create threats during construction of NPPs. It also discusses how requirements for personnel fitness for duty, trustworthiness, and reliability would address those pathways by reducing the potential for unintentional errors and omissions due to worker impairment and for intentional acts of vandalism, sabotage, or aid to outsiders by workers who are untrustworthy or unreliable.

Although focusing on personnel security, this analysis reflects the clear message of the experts consulted for this project that effective security requires an integrated security strategy that addresses the entire range of threat pathways, vulnerabilities, and protection measures. The objective of this analysis is not to specify a particular set of personnel security measures, but to provide the technical basis for implementing measures to assure that those personnel in a position to create a credible threat during the construction process are prevented from doing so. This discussion focuses primarily on the portion of the construction process that involves workers on the construction site and those overseeing and managing them. The extended, off-site workforce involved in off-site component construction, manufacture, and assembly, and the purchase-transport supply chain is addressed only briefly.

As part of this analysis, the chapter outlines the dimensions of personnel security requirements for operating NPPs and discusses the basis for applying those requirements during the construction phase. It is noted, however, as discussed in Chapter 3, that differences in the characteristics and threats pertinent to operating and under-construction NPPs may require unique measures during construction that are not identified by this analysis.

6.2 Threats of Concern that Fall within NRC's Regulatory Authority Exist for NPPs under Construction

The experts and relevant literature identified several threats of concern during the construction phase of NPPs. Greatest weight was given to threats that could result in a delayed impact on the plant once it is in operation. Delayed impact threats have the

potential for consequences that jeopardize the public health and safety, the common defense and security, and the environment. However, historical evidence demonstrates that threats to the security of the plant while it is under construction should not be dismissed. Immediate threats can pose a significant risk to (a) public confidence in the safety and security of nuclear power; (b) continuity of operation of nuclear power plants; and (c) the safety and security of workers at the site and its immediate vicinity.

The experts consulted for this project concluded that the following threats are credible, given the current threat environment in the U.S. and the desirability of NPPs as potential targets, and that the consequences of a successful attack would be of a nature and degree that protection against them falls within the regulatory scope of the NRC:

- Direct external attacks;
- Immediate acts of theft, vandalism, or sabotage;
- Hidden explosive devices;
- Compromised critical safety- and security-related SSCs, especially software systems from sabotage or accumulated errors;
- Compromised or deficient major components or materials from sabotage or accumulated errors;
- Access to and theft of critical information; and
- Caching weapons or explosives for later use.

6.3 The Open Nature of Construction Sites and Characteristics of Workers Warrant Personnel Security Measures

The basic characteristics of a large-scale construction site and persistently demonstrated attributes of construction workforces increase the potential for both inadvertent and intentional threats. The numbers of workers, delivery personnel, vehicles, and materials crossing site borders every day, combined with the varying duration and schedule of workers during construction, pose personnel management challenges. The persistent tendency of construction workers to use drugs and alcohol and to bring them onto the construction site is well documented and recognized as warranting testing requirements.

6.4 Protective Measures Are Available to Achieve Personnel Security

Personnel security is achieved through hiring competent, reliable, and trustworthy workers, training and supervising them effectively, and implementing measures to prevent, deter, detect, and mitigate careless, impaired, untrustworthy, malicious, or malevolent behaviors, thereby reducing the potential for the pathways through which workers inadvertently cause or intentionally implement threats. Measures to establish the true identity of a worker and to control a worker's access to the site or to particular locations on the site are prerequisites for implementation of other personnel security measures. Table 6.1 summarizes these factors, their causes or indicators, and typical measures used to prevent, deter, detect, or mitigate them. Evaluation of the relative effectiveness or cost-benefit of these measures is beyond the scope of this project. The purpose of this table is to illustrate that a range of personnel security measures has been found by this study to be effective and appropriate for addressing the pathways

through which workers can threaten the safety and security of the facility and the construction site.

Table 6.1 Worker Attributes, Causes or Indicators, and Typical Protection Measures

Worker Attribute	Causes/Indicators	Typical Measures Used to Prevent, Deter, Detect, Mitigate
True identity	➢ Physical features/biometrics ➢ Documents ➢ Knowledge	➢ Pre-employment identity verification and screening ➢ Fingerprinting ➢ Other biometric measures (iris, hand, face) ➢ Official identification documents (birth certificates, drivers' licenses, passports, military papers, social security card) ➢ Passwords
Authorization for site/work place access	➢ Badge ➢ Escort requirement	➢ Badge issuance and control procedures ➢ Entry/exit access control limited to badged or escorted workers ➢ Personnel and vehicle checks/searches/ surveillance ➢ Escort requirements ➢ Peer-checking/ 2-person rules ➢ Smart badges to document site access/egress/ movement and location on site ➢ Safety/security training
Impairment due to drug or alcohol consumption or abuse	➢ Drug use ➢ Alcohol use ➢ Drug or alcohol possession on site ➢ Drug sales	➢ Pre-employment and pre-assignment drug and alcohol testing ➢ For cause drug and alcohol testing ➢ Random drug testing ➢ Behavioral observation by co-workers and supervisors ➢ Self-reporting of medications ➢ Employee assistance programs
Fatigue	➢ Lack of adequate rest	➢ Shift scheduling ➢ Fatigue self-reporting

Worker Attribute	Causes/Indicators	Typical Measures Used to Prevent, Deter, Detect, Mitigate
Mental instability	➢ Stress ➢ Mental illness ➢ Poor employment and credit histories ➢ Poor social relationships	➢ Psychological testing and interviews ➢ Life stress surveys and self-assessments ➢ Self-reporting ➢ Employment history review ➢ Credit history review ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Employee assistance programs
Vulnerability to pressure, coercion, exploitation, or duress	➢ Weak character ➢ Engagement in illicit activities, including drug use and drug sales ➢ Financial duress ➢ Criminal or terrorist networks ➢ Bringing contraband onto the site ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Pre-Employment and pre-assignment drug and alcohol testing ➢ Random drug testing ➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Employee assistance programs
Criminal or weak character	➢ Criminal record ➢ Poor job history ➢ Criminal or terrorist network ➢ Poor credit history; fraud ➢ Poor social relationships ➢ Bringing contraband onto the site ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Pre-Employment and pre-assignment drug and alcohol testing ➢ Random drug testing ➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Employee assistance programs

Worker Attribute	Causes/Indicators	Typical Measures Used to Prevent, Deter, Detect, Mitigate
Conflicting allegiances	➢ Stated allegiances ➢ Memberships in organizations ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews
Malevolent intent	➢ Statements of intent or desire ➢ Antagonistic or aggressive behavior ➢ Bringing contraband onto the site ➢ Taking materials offsite without authorization ➢ Accessing sites and information without authorization	➢ Entry/exit searches ➢ Psychological testing and interviews ➢ Employment history review ➢ Credit history review ➢ Criminal history check ➢ Terrorist screening ➢ Character reference checks ➢ Behavioral observation by co-workers and supervisors ➢ Supervisory interviews ➢ Red-teams ➢ Security-oriented QA/QC ➢ Insider threat mitigation programs
Inattention to or unawareness of security requirements	➢ Lack of knowledge ➢ Absence of security orientation	➢ Awareness and training programs ➢ Responsibility assignment

Typically, access authorization (AA), fitness-for-duty (FFD), and insider mitigation programs (IMP) are designed to implement these measures. Access authorization programs normally focus on ensuring that only authorized persons are allowed onto the site or into controlled areas, and that those authorized for access are trustworthy and reliable. Their principal focus is on preventing insider threats. Recently, considerable attention has been given to access authorization for internal information systems, in addition to physical access to buildings and sites.

Fitness-for-duty programs typically focus on providing reasonable assurance that:

- Individuals are trustworthy and reliable as demonstrated by the avoidance of substance abuse and are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause, which in any way adversely affects their ability to safely and competently perform their duties;

- Individuals who are not fit to perform the duties that require them to be subject to the FFD program are detected early and prevented from performing those duties;
- Workplaces subject to FFD requirements are free from the presence and effects of illegal drugs and alcohol; and
- The effects of fatigue and degraded alertness on individuals' abilities to safely and competently perform their duties are managed commensurate with maintaining public health and safety.

Insider mitigation programs share the goal of ensuring the trustworthiness and reliability of the workforce with the AA programs. They typically focus on supplementing the measures implemented by AA programs but with a greater focus on counterterrorism intelligence, surveillance, and information sharing across agencies and sites.

These measures can be tailored to be commensurate with the threat and need.

6.5 Graded Approaches Would Tailor Protective Measures to Avoid Undue Burdens and Costs

One of the particular features of the construction process that makes security regulation difficult is the changing nature of the workforce, activities, and site over time as construction proceeds from site clearing to pre-operational testing. In order not to impose personnel security requirements on workers who present minimal risk, the security experts at the TISP conference recommended that regulators take a construction phase- and position-graded approach to addressing personnel security. The experts recommended examining the nature and timing of security measures that might be needed during the construction phase, followed by a subsequent analysis to determine how responsibility for requiring and implementing those measures should be assigned. These analyses would provide the basis for designing the appropriate, tailored requirements. Based on the information gathered for this study, the project team also concluded that the security measures, and regulatory requirements, would fall within different regulatory programs, given the need to address both intentional threats, which are primarily trustworthiness- and reliability-based, and unintentional threats, which are primarily fitness- and reliability-based.

The experts at the TISP workshop concluded that focusing on workers engaged in constructing, or with access to, SSR-SSCs would provide an appropriate level of protection, while reducing administrative and personnel costs. They also thought that at least some verification of identity prior to badging and limiting unescorted access to the construction site to badged workers would be prudent, given the history of attacks on NPPs under construction. In addition, as has become common practice, the experts recommended that individuals with control over site access, work assignments, and the various fitness-for-duty, access authorization, quality assurance inspections, and other site security programs be subject to "operational" level personnel security requirements, given the level of their responsibilities and roles in ensuring the integrity and effectiveness of any of the measures applied to the general workforce. Figure 6.1 illustrates this graded approach to determining levels and types of personnel security measures appropriate to different worker categories over the course of the construction process.

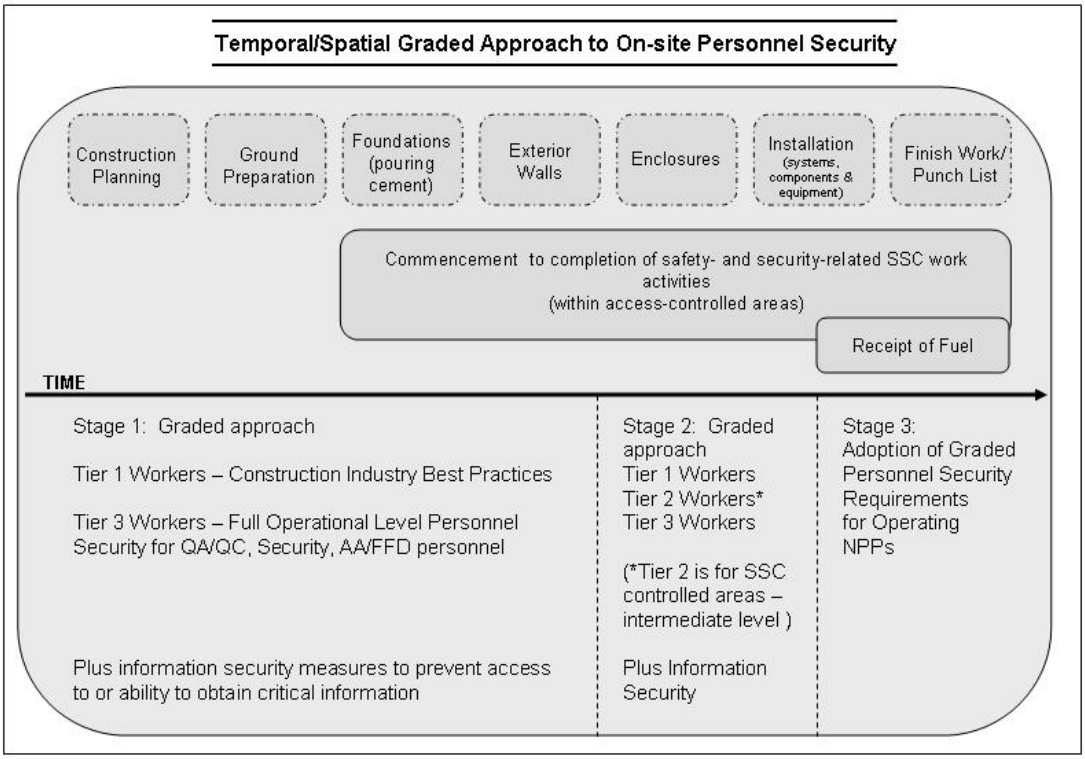


Figure 6.1 Temporal/Spatial Graded Approach to On-site Personnel Security

Table 6.2 illustrates a potential graded approach for applying personnel security requirements during the construction phase of an NPP. It identifies the categories of workers/duties identified as meriting consideration for tailored application of those requirements, a brief rationale for applying requirements to that group, and the phase of construction or duty assignment for which the requirements would be applied. Table 6.2 is intended as a model for consideration. As mentioned previously, more detailed analysis of the overall life cycle of NPPs, particularly of the life cycle of the construction phase, along with more rigorous analysis of the costs and benefits associated with each of the proposed requirements, is needed. However, the threats and pathways this study identified, coupled with the effectiveness of personnel security requirements to address those threats and pathways, indicate that there is a technical basis for applying personnel security requirements during construction. This more detailed analysis would help to determine how narrowly or broadly the personnel security programs should be focused, and which particular requirements should be applied to which workers at what phase of the construction process.

6.5 Cross-Walk with AA-FFD-IMP Programs Applied to Operating NNPs

The experts agreed that one approach to the analysis discussed in the previous section would be to consider which of the security measures utilized or required for an operating facility would be needed and effective during the construction phase, and when and to whom they should be applied. They noted that this kind of cross-walk between construction and operating security needs would have to take into account differences between the operating and under-construction conditions and threats when considering

Table 6.2 Graded, Temporal Approach Applied to Work Groups during NPP Construction

Work Group	Rationale for Coverage	Phase of Construction or Task Assignment
Operating Personnel	➢ Will have access to site information and planning that could jeopardize the security of the facility.	➢ Full trustworthiness and reliability (T & R) and drug and alcohol (D & A) measures from project initiation
Supervisors and Managers	➢ Controlling programs and personnel assignments ➢ Able to subvert any security measures or programs	➢ Full T & R and D & A measures from construction initiation
FFD/AA/IMP Program Personnel	➢ Controlling information that influences job access and assignments ➢ Able to subvert FFD/AA/IMP programs	➢ Full T & R and D & A measures from construction initiation
Security Personnel	➢ Controlling site access and implementation of searches. Potentially have access to weapons.	➢ Full T & R and D & A measures from construction initiation
QA/QC Inspectors	➢ Controlling a process to identify evidence of carelessness, errors, or sabotage	➢ Full T & R and D & A measures either from construction initiation or from initiation of SSR-SSC activities
Personnel Working on SSR-SSCs	➢ Access to and engagement with SSR-SSC area, materials, and activities. Therefore increased consequences from pathways through which workers could cause or facilitate threats	➢ Full T & R and D & A measures from initiation of SSR-SSC activities
Personnel NOT Working on SSR-SSCs	➢ Access to site, ability to obtain information from observation; ability to collaborate with others to cache materials or assist others; ability to implement malicious actions.	➢ Basic T & R and D & A measures from initiation of construction

whether additional or different measures are needed for NPPs under construction. Conducting this type of cross-walk of requirements appropriate for facility operations and construction is among the next steps recommended in Chapter 7.

In the view of a number of the experts, it would be beneficial to examine the security threats and protection needs of the construction phase on their own merits in the context of the facility's systems and life cycle, drawing on logical analysis, the available literature, evaluations of existing programs and candidate measures, and recommendations about best practices and cost-effectiveness from a wide range of facilities. Only then, they said, could it be determined (1) whether and to what extent security measures required during NNP operation are appropriate for the construction phase and, equally important, (2) whether and to what extent there are security threats during the construction phase that require different strategies than those needed for operating plants and that would be insufficiently addressed by imposition of the operating requirements. They pointed out that there may be threats that are unique to the construction phase that require measures that are not needed for operating plants.

6.6 Personnel Security Measures Are Used in Other CI Sectors for Facilities under Construction

As discussed in Chapters 2, 3 and 4, the application of personnel security measures to construction-phase workers varies considerably by type of facility, sector, and ownership. Some facilities, such as embassies, facilities dealing with classified information, and facilities being constructed in close proximity to operating facilities that are subject to stringent security measures, employ the entire range of measures discussed in Table 5.1, and apply them from project initiation through project completion. Others employ a smaller subset of these measures. According to the information obtained for this project, almost all construction projects employ measures to control access to the construction site to authorized workers and vehicles, including some verification of personal identity and issuance of a site-specific badge. Many conduct access and exit searches. An increasing number conduct pre-employment, for-cause, and random drug and alcohol testing of all workers with access to the site. Some conduct background checks that include fingerprinting, FBI or local criminal background checks, employment history reviews, and credit reviews. Fewer conduct psychological screening of construction workers or character checks. Information was not obtained about fatigue management during the construction phase, with the exception of security workers.

The most common reported personnel security measures for sites under construction include:

- Controlling access to the site and limiting access to authorized personnel (fences and gates);
- Badging;
- Entry and exit searches or at least observation (to prevent contraband and theft);
- Records of worker presence and location on the site;
- Regular, required safety and health briefings;
- Pre-employment drug testing, and, in an increasing number of instances, random drug testing during employment; and

- Reporting requirements for accidents and/or exposure to hazardous materials.

6.7 Summary

The investigations carried out by this project indicate that there is a technical basis for personnel security requirements during the construction phase of NPPs, and that imposition of such requirements does fall within the jurisdictional authority of the U.S. NRC. There remains an open question of whether the potential for direct impact threats to the NPP as it is under construction itself is sufficient to warrant the NRC regulation of the construction process. This deserves further consideration, as discussed in Chapter 7. The particular design of the personnel security measures warranted by these threats is beyond the scope of this paper, but the systems-based life-cycle approach with cost-benefit considerations, combined with a vulnerability assessment, is viewed by the experts consulted in this effort as a useful approach for this more detailed analysis.

7. Suggested Next Steps

7.1 Overview of the Chapter

This chapter suggests several analyses and other efforts based on the recommendations made by the experts consulted for this project and information in the relevant literature. These next steps complement other NRC initiatives in preparation for renewed nuclear power plant construction activity.

7.2 Develop a Map of Life-Cycle Events and Regulatory Requirements to Facilitate Cross-Organizational Consideration of Security Needs and Options

The information obtained prior to and during the TISP workshop indicates that those advocating a systems-based and life-cycle approach to NPP security tend to focus primarily on how taking security into account during the reactor design, plant siting, and plant design phases could help mitigate security vulnerabilities during plant operation. This focus is being reinforced by the Department of Homeland Security's emphasis on the development of systematic methods for prioritizing security and resilience enhancing efforts. It is also supported by TISP's efforts to develop security and resilience standards, and by the increased participation of professional security integrators and planners, who are trained in systems-based, life-cycle analysis who are helping facility owners take security into account during the design phases of the life cycle.

Given the complex regulatory environment governing NPPs, developing a map that overlays the steps in each of the life-cycle phases with key milestones for the major systems and the applicable regulatory requirements would provide a useful basis for bringing together the pertinent personnel and identifying cross-element linkages and security considerations. The next step would be to develop a timeline that maps requirements and actions to steps in the NPP planning and construction process. It would be helpful to include in this timeline an indication of the typical duration of activities and intervals between key milestones. This would be most effective if done for each of the following major phases of the design-build-operate-decommission lifecycle:

- Reactor Design;
- Plant Siting;
- Plant Design;
- Plant Construction;
- Plant Operations;
- Plant Decommissioning.

7.3 Examine Regulatory Constraints and Authorities for Construction Security

It would be informative to engage experts in a discussion about roles, responsibilities, constraints and authorities concerning assurance of security during the construction of CI, particularly nuclear power plants. A question identified in discussions with experts for this project is whether the NRC's regulatory authority extends to threats whose

consequences, though not resulting in a radiological release, theft of radiological material, or acquisition of safeguards or critical security information, nevertheless pose a significant threat to:

- Public confidence in the safety and security of nuclear power;
- Continuity of operation of nuclear power plants;
- The safety and security of workers at the site and its immediate vicinity.

Assuming that there are threat pathways that could cause grave damage to the facility under construction, but without the potential for radiological or toxic release, a discussion with the appropriate knowledgeable experts to address the following question would clarify this important issue:

- Does preventing the destruction of the facility under construction, with its concomitant damage to the health and safety of the workers and nearby residents, public confidence in the safety and security of CI facilities, including NPPs, and damage to the environment, fall within the regulatory authority of federal or state agencies?

7.4 Examine Whether the Construction Phase Has Special Security Needs Not Addressed by Measures Developed for Operating Facilities

As discussed in Chapters 3 and 4, it is possible that the particular attributes of the construction process, site, and workforce create security needs that are not adequately met by the measures developed for operating facilities. Although this project provides a start on this process, more detailed analysis is needed that brings together experts in the systems being constructed, threat and vulnerability assessment, counterterrorism, and integrated security program design and implementation. This would also provide an opportunity to consider whether measures taken at other phases of the facility's life cycle might reduce or modify the security needs during construction.

7.5 Examine the Personnel Security Issues and Needs of Off-Site and Supply Chain Workers

The research conducted for this project identified a need to examine the security requirements, including personnel security, for the extended workforce involved in off-site component construction, manufacture, and assembly, and the purchase-transport supply chain and to identify the issues involved in implementing the security measures identified as appropriate for these workers and processes. This examination should include consideration of off-site design and production of software and information systems security needs.

7.6 Examine Whether Voluntary Measures Could Substitute for Regulatory Requirements

The TISP workshop revealed that some facility owners, particularly federal agencies, impose stringent personnel security measures on those constructing their facilities, even in the absence of regulatory requirements for such measures. This appears to indicate that in some cases voluntary programs may be adequate to achieve security needs. However, the experts interviewed for this project repeatedly emphasized that cost and schedule pressures, along with concerns about worker and/or union resistance,

generally resulted in cost-cutting and elimination of security measures. In addition, they indicated that concerns that legal challenges to screening and monitoring programs would cause unpredictable delays and costs further deterred implementation of stringent personnel security measures. It would be useful to examine this issue further.

7.8 Participate in Cross-CI Sector Discussions about Construction Security

The experts and literature consulted for this project revealed widespread agreement that there is substantial evidence supporting the need for a rigorous analysis of the threats, vulnerabilities, and consequences of security breaches during the construction phase of NPPs – or of any of the other U.S. CI. They recommended that such an assessment be updated as the threat environment changes. They also emphasized that it is particularly difficult to assess the threats resulting from intentionally malicious behavior. Consequently, several suggested that it would be useful to continue the discussion started at the TISP workshop, capitalizing on the work already done to develop a framework for considering construction security needs and potential protective measures. They thought that TISP might be an appropriate organization to convene such a forum and that bringing together experts with more direct responsibility for security planning and oversight and direct experience with the effectiveness and costs and benefits of various protective measures would be informative and useful, and would fill a void not currently being addressed. They suggested that consideration of security measures might be disaggregated to focus on particular aspects of construction security and protective measures that were of interest to the participants, while maintaining the systems-based life-cycle framework. The key questions identified in Appendix C provide a start on some of the outstanding issues these discussions could be designed to address.

7.9 Conduct Cross-Walk with AA-FFD-IMP Programs Applied to Operating NNPs to Determine Those Needed during Construction

As discussed in section 6.5 above, the experts consulted for this project suggested that one approach to determining the levels and types of personnel security measures that are appropriate during NPP construction would be to take measures commonly required during plant operations as a starting point. Then, by comparing differing conditions and threats presented by the construction and operating phases, analysts could determine what changes to operations-phase personnel security measures would be need to arrive at an appropriate personnel security program for NPP construction. Table 7.1 presents a suggested framework for such a cross-walk analysis.

Table 7.1 Cross-Walk of Requirements

AA and FFD Measures	Operating NPPs		NPPS Under Construction	
	UA Workers	FFD/AA program personnel	FFD/AA/QA program personnel	Construction Workers
True Identity and Smart Badges				
Personal History Disclosure				
Employment History				
Credit History				
Character and Reputation				
Criminal History and Records Check, Terrorist Screening, Arrest Self-Reports				
Psychological Assessment				
Behavior Observation Program and Supervisory Reviews				
Escorts				
Pre-Access Drug and Alcohol Testing				
For-Cause Drug and Alcohol Testing				
Random Drug and Alcohol Testing				
Fitness Monitoring				
Employment Assistance Programs				
Fatigue Management				
Privacy Protections, Consent, and Information Security				

8. Bibliography and References

Abderrahim, M., E. Garcia, R. Diez, and C. Balaguer. 2004. A Mechatronics Security System for the Construction Site. *Automation in Construction* 14:460-466.

Abel, Amy. February 4, 2005. Government Activities to Protect the Electric Grid. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress. Accessed 12.2007 at http://italy.usembassy.gov/pdf/other/RS21958.pdf.

Ackerman, Gary A., Jeffrey M. Bale, and Kevin S. Moran. 2006. Assessing the Threat to Critical Infrastructure. Chapter 2 in *Homeland Security: Protecting America's Targets. Vol. 3. Critical Infrastructure.* Edited by James J.F. Forest. Westport, CT: Praeger Security International.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. December 2002. *Fourth Annual Report to the President and the Congress. Implementing the National Strategy*. Prepared by RAND Corporation. Accessed 10.2007 at http://www.rand.org/nsrd/terrpanel/terror4.pdf.

Agarakova, Elena, Steven J. Buttacavoli, Sekret T. Sneed, and Jonathan J. Yang. 2000. Environmental Crimes. *American Criminal Law Review* 37(2):333-418.

Agnew, Christopher R. Aaron M. Hoffman, Justin J. Lehmiller, and Natasha T. Duncan. 2007. From the Interpersonal to the International: Understanding Commitment to the "War on Terror." *Personality and Social Psychology Bulletin* 33:1559-1571.

Aguilar, Rodolfo J. 1973. *Systems Analysis and Design in Engineering, Architecture, Construction, and Planning*. Englewood Cliffs, NJ: Prentice-Hall.

Allport, Gordon W., 1937. The Functional Autonomy of Motives. *The American Journal of Psychology* 50(1/4):141-156.

Altman, W., T. Ankrum, W. Brach. 1984. *Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants: A Report to Congress.* NUREG-1055. Washington, DC: U.S. Nuclear Regulatory Commission. Accessed 10.2007 at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1055/sr1055_full.pdf.

American Chemistry Council, the Chlorine Institute, Inc., and the Synthetic Organic Chemical Manufacturers Association. October 2001. *Site Security Guidelines for the U.S. Chemical Industry*.

American Society of Civil Engineers (ASCE). 2005. Infrastructure Report Card 2005. Accessed 10.2007 at http://www.asce.org/reportcard/2005/page.cfm?id=32.

Anderson, R.H. 1999. Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. *Report No. CF-163-DARPA*. Santa Monica, CA: Defense Research Institute.

Anderson, R.H., Thomas Bozek, Tom Longstaff, Wayne Meitzler, Michael Skroch, and Ken Van Wyk. 2002. *Research on Mitigating the Insider Threat to Information Systems -- #2. Proceedings of a Workshop.* Rand Corporation. Washington, DC: National Defense Research Institute.

Arditi, David, and Ranon Chotibhongs. 2005. Issues in Subcontracting Practice. *Journal of Construction Engineering and Management 121(8):866-876.*

Associated Press. November 4, 2008. Nuclear Group Warns About Construction. *AJC.Com*. Accessed 11.2008 at http://www.ajc.com/services/content/printedition/2008/11/04/srs.html.

Associated Press. June 11, 2008. Census to Fingerprint Half-Million Workers. MSNBC. Accessed 10.2008 at http://www.msnbc.msn.com/id/25103480/.

Auerswald, David P. 2006. Deterring Nonstate WMD Attacks. *Political Science Quarterly* 121(4):543-568.

Aven, Terje. 2009. Identification of Safety and Security Critical Systems and Activities. *Reliability Engineering and System Safety* 94:404-411.

Badolato, E.V. 1991. Environmental Terrorism: A Case Study. *Terrorism* 14(4):237-239.

Ballard, James David. 1997. A Preliminary Study of Sabotage and Terrorism as Transportation Risk Factors Associated with the Proposed Yucca Mountain High-Level Nuclear Waste Facility. Grand Valley State University. Published by the State of Nevada Agency for Nuclear Projects. NWPO-TN-018-96. Accessed 10.2007 at http://www.state.nv.us/nucwaste/trans/jballard.htm.

Barnes, Valerie, Brian Haagensen, and John O'Hara. 2001. *The Human Performance Evaluation Process: A Resource for Reviewing the Identification and Resolution of Human Performance Problems*. NUREG/CR-6751. Prepared by Performance, Safety and Health Associates, Inc. for the U.S. Nuclear Regulatory Agency Office of Nuclear Regulatory Research.

Barnes, V., I. Fleming, T. Grant, J. Hauth, J. Hendrickson, B. Kono, C. Moore, J. Olson, L. Saari, J. Toquam, D. Wieringa, P. Yost, P. Hendrickson, D. Moon, and W. Scott. 1988. *Fitness for Duty in the Nuclear Power Industry: A Review of Technical Issues.* Seattle, WA: Battelle Seattle Research Centers. NUREG/CR-5227.

Barton, Barry, Catherine Redgwell, Anita Rønne, and Donald N. Zillman, editors. 2004. *Energy Security: Managing Risk in a Dynamic Legal and Regulatory Environment*. New York, NY: Oxford University Press.

Bebchuk, L. A., and L. Kaplow. 1992. Optimal Sanctions when Individuals are Imperfectly Informed about the Probability of Apprehension. *Journal of Legal Studies* 21:365–370.

Beherens, Carl, and Mark Holt. February 2005. Nuclear Power Plants: Vulnerability to Terrorist Attack. Washington, DC: Congressional Research Service.

Benford,Robert D., and David A. Snow. 2000. Framing Processes and Social Movements: An Overview and Assessment. *Annual Review of Sociology* 26:611-639.

Berg, Robert, and Jimmie Hinze. 2005. Theft and Vandalism on Construction Sites. *Journal of Construction Engineering and Management* 131(7):826-833.

Bergmann, Pamela and David Pijawka. 1981. The Socioeconomic Impacts of Nuclear Generating Stations: An Analysis of the Rancho Seco and Peach Bottom Facilities. *GeoJournal Supplementary Issue* 3(1981):5-15.

Bernstein, Harvey M. 2002. Critical Infrastructure Protection Priorities: The Built Environment. Hosted by the Office of Science and Technology Policy (OSTP). Accessed 10.2008 at http://tisp.org/index.cfm?cdid=10842&pid=10261.

Bioscrypt System Uses Fingerprint Reader to Track Workers' Time, Attendance. August 10, 2007. *Daily Commercial News.* Accessed 2.3008 at www.dailycommercialnews.com/article/id23987.

Blumstein, A., Cohen, J. and Nagin, D., eds. 1978. *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*. Washington, DC: National Academy Press.

Bohra, S.A., and P.D. Sharma. 2006. Construction Management of Indian Pressurized Heavy Water Reactors. *Nuclear Engineering and Design* 236:836-851.

Borack, Jules I. 1998. An Estimate of the Impact of Drug Testing on the Deterrence of Drug Use. *Military Psychology* 10(1):17-25.

Brahme, R., A. Mahdavi, K.P. Lam, and S. Gupta. 2001. Complex Building Performance Analysis in Early Stages of Design. Seventh International IBSPA Conference, Rio de Janeiro, Brazil. August 13-15. Accessed 2.2008 at www.inive.org/members_area/medias/pdf/Inive%5CIBPSA%5CUFSC479.pdf.

Braun, Chaim. 2006. Security Issues Related to Future Pakistani Nuclear Power Program. Center for International Security and Cooperation (CISAC), Stanford University. Stanford, CA. Accessed 2.2008 at http://cisac.stanford.edu/publications/security_issues_related_to_pakistans_future_nuclear_power_program/.

Bukharin, Oleg. 1997. Upgrading Security at Nuclear Power Plants in the Newly Independent States. *The Nonproliferation Review* Winter:28-39.

Building Contractor Magazine. 2004. Union Carpenter and Contractors Lead the Way with ID Verification Program. Vol. III. Accessed 2.2008 at http://www.njcct.org/pdf/BCAMagFall2004-%20ID%20Verfication.pdf.

Bunn, George, and Chaim Braun. 2003. Terrorism Potential for Research Reactors Compared with Power Reactors: Nuclear Weapons, "Dirty Bombs," and Truck Bombs. *American Behavioral Scientist* 46(6):714-726.

Bunn, Matthew, and George Bunn. 2002. Strengthening Nuclear Security Against Post-September 11 Threats of Theft and Sabotage. *Journal of Nuclear Materials Management* Spring:1-13.

Business Insurance. October 23, 2007. Spanish Language Barriers Increase Hazards on Construction Sites. Accessed 3.2007 at http://www.workingimmigrants.com/2006/11/spanish_language_barriers_incr.html.

Business Roundtable Security Task Force. August 5, 2005. A Collaborative Strategy for Using National Criminal History Record Checks to Reduce the insider Terrorist Threat. Accessed 10.2007 at http://www.usdoj.gov/olp/pdf/businessroundtablecomments.pdf.

California Commission on Peace Officer Standards and Training. 1991. (Revised 2008). *POST Background Investigation Manual: Guidelines for the Investigator*. Accessed 10.2008 at http://www.post.ca.gov/selection/bim/bi.pdf.

Callaway, Rhonda L., and Julie Harrelson-Stephens. 2006. Toward a Theory of Terrorism: Human Security as a Determinant of Terrorism. *Studies in Conflict and Terrorism* 29:773-793.

Cameron, Gavin. 1999. *Nuclear Terrorism: A Threat Assessment for the 21st Century.* New York: Macmillan.

Caplan, Bryan. 2006. Terrorism: The Relevance of the Rational Choice Model. *Public Choice* 128:91-107.

Caplan, Yale H., and Marilyn A. Huestis. 2007. Drugs in the Workplace. In *Drug Abuse Handbook*, 2nd Edition. Steven B. Karch, editor. Boca Raton, FL: CRC Press. Pp.731-736.

Cappelli, Dawn, Andrew Moore, and Timothy Shimeall. Common Sense Guide to Prevention and Detection of Insider Threats. *U.S. CERT*. Accessed 3.2008 at http://www.us-cert.gov/reading_room/prevent_detect_insiderthreat0504.pdf.

Carpenter, Christopher S. 2007. Workplace Drug Testing and Worker Drug Use. *Health Services Research* 42(2): 795-810.

Caruso, V.L. 2003. *Outsourcing Information Technology and the Insider Threat*. Report No. AFIT/GIR/ENG/03-01. Wright-Patterson AFB, OH: Air Force Institute of Technology.

Chalk, Peter, Bruce Hofffman, Robert Reville, and Anna-Britt Kasupski. 2006. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*. Santa Monica, CA: RAND Corporation. Accessed 10.2007 at http://www.rand.org/pubs/monograph/2005/RAND_MG393.pdf.

Chalmers, J, D. Pijawka, K. Branch, P. Bergmann, J. Flynn, and C. Flynn. 1982. *Socioeconomic Impacts of Nuclear Generating Stations*. Prepared by Mountain West Research, Inc. for the NRC Office of Nuclear Regulatory Research. NUREG/CR-2750.

Chapman, Parke. January 10, 2001. Added Cost of Development: Substance Abuse-Construction Workers-Statistical Data Included. *Real Estate Weekly*. Accessed 1.2008 at http://findarticles.com/p/articles/mi_m3601/is_23_47/ai_69676202.

Chapin, Douglas M., Karl Cohen, W. Kenneth Davis, Edwin Kintner, Leonard Koch, John Landis, Milton Levenson, I. Harry Mandil, Zack Pate, Theodore Rockwell, Alan Schriesheim, John Simpson, Alexander Squire, Chauncey Starr, Henry Stone, John Taylor, Neil Todreas, Bertram Wolfe, and Edwin Zebroski. 2002. Nuclear Power Plants and Their Fuel as Terrorist Targets. *Science* 297:1997-1999.

Chester, C. V. 1976. Estimates of Threats to the Public from Terrorist Acts Against Nuclear Facilities. *Nuclear Safety* 17(6).

Chestnut, Sheena. 2007. Illicit Activity and Proliferation. North Korean Smuggling Networks. *International Security* 32(1):80-111.

Cockburn, Alexander. 2003. An Open Door for Nuclear Terrorism. North Carolina Waste Awareness and Reduction Network. Accessed 10.2007 at http://www.ncwarn.org/docs/articles/art-07-21-03COCKBURN-OpenDoorForTerror.htm.

Construction Safety and Drug Abuse Executive Roundtable. May 22, 2006. Construction Safety and Drug Abuse - Executive Roundtable Highlights. Washington, DC. Hosted by Avitar. Accessed 1.2008 at http://www.avitarinc.com/DC-construction-drug-abuse-highlights.cfm.

Contractors Association of West Virginia. 2008. West Virginia Alcohol and Drug-Free Workplace Seminar. Accessed 5.2008 at http://www.cawv.org/Alcohol%20and%20Drug%20Free%20Seminar%20Registration.pdf.

Cook, Constance Ewing. 1980. *Nuclear Power and Legal Advocacy*. Lexington, MA: Lexington Books.

Copeland, Claudia. 2007. Terrorism and Security Issues Facing the Water Infrastructure Sector. Updated May 18. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress.

Crocker, Thomas D., and Jason F. Shogren. 1999. Endogenous Environmental Risk. In *Handbook of Environmental and Resource Economics*, edited by Jeroen C.J.M. van den Bergh. Northampton, MA: Edward Elgar Publishing.

Crow, Ryan. 2004. *Personnel Reliability Programs*. McClean, VA: Project Performance Corporation.

C-TPAT Commonly Asked Questions. U.S. Customs and Border Protection Agency. Accessed 10.2007 at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml.

Cummings, Judith. October 3, 1981. More Disclosures on Diablo A-Plant. *New York Times.* Accessed 1.2007 at http://topics.nytimes.com/top/reference/timestopics/people/c/judith_cummings/index.html?offset=50&s=oldest.

Cummings, Judith. October 1, 1981. Blueprint Switch at Coast A-Plant Widens U.S. Inquiry on its Safety. *New York Times*. Accessed 1.2007 at http://topics.nytimes.com/top/reference/timestopics/people/c/judith_cummings/index.html?offset=50&s=oldest.

D'Antoni, Massimo, and Roberto Galbiati. 2007. A Signaling Theory of Nonmonetary Sanctions. I*nternational Review of Law and Economics* 27(2):204-218.

D'Olier, Robert. October 21, 2005. *DOE NP2010 Nuclear Power Plant Construction Infrastructure Assessment*. MPR-2776. Prepared for the U.S. Department of Energy by MPR Associates.

de Boef, Suzanna, and Paul M. Kellstedt. 2004. The Political (and Economic) Origins of Consumer Confidence. *American Journal of Political Science* 48(4):633-649.

Defense Science Board. January 2007. Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection. Washington, DC. Accession Number ADA461437.

Defense Science Board. September 21, 2007. *Mission Impact of Foreign Influence on DOD Software*. Accessed 10.2007 at http://www.acq.osd.mil/dsb/reorts/2007-09-Mission Impact of Foreign Influence on DOD Software.pdf.

Defense Science Board. September 2003. *Report of the Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities*. Washington, DC: Office of the Secretary of Defense.

Denning, D.E. 1999. *Information Warfare and Security*. Reading, MA: ACM Press.

DeVan, William. June 23, 2003. The Impact of Homeland Security on the Construction Industry. *Construction Weblinks*. Accessed 12.2008 at http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/June_23_2003/homeland_security.htm.

Deztech Information Services. 2006. Back to the Future of Employment Background Checks. *HR Management* 4.

Diablo Canyon Independent Safety Committee. 2007. 17th Annual Report, July 1, 2006 thru June 30, 2007. Accessed 5.2008 at http://www.dcisc.org/annual-report-17-2006-2007/volume1/4-07-emergency-preparedness.html.

Driscoll, L.N. 1994. A Validity Assessment of Written Statements from Suspects in Criminal Investigations using the SCAN Technique. *Police Studies* XVII:77-87.

Durling, Jr., R.L., and D.E. Price. 2006. *Use of the Homeland-Defense Operational Planning System (HOPS) for Emergency Management*. Lawrence Livermore National Laboratory. Presented at the International Conference on Probabilistic Safety Assessment and Management. New Orleans. May 14-19, 2006.

Electronic Privacy Information Center (EPIC). September 6, 2005. Comments of the Electronic Privacy Information Center on the Department of Justice Federal Bureau of Investigation AAG/A Order No. 005-2005. Accessed 2.2008 at http://epic.org/privacy/airtravel/tsrs_comments090605.html.

Entergy Nuclear Northeast. 2006. *Craft/Union Personnel Instructions for Gaining Unescorted Access to Indian Point Energy Center*. Revision 0. January. Accessed 10.2007 at http://www.entergy-nuclear.com/content/resource_library/forms/UNION_HALL_INFO_PACK_1-16-06.pdf.

Entergy Nuclear Northeast. 2006. *Indian Point Energy Center Non-Licensee Employee In-Processing Policy*. Revision 7. January. Accessed 10.2007 at http://www.entergy-nuclear.com/content/resource_library/forms/CONTRACTOR_PACKAGE_1-06.pdf.

Essex, David. March 19, 2007. Wigits for Digits. *Government Computer Network*. Accessed 10.2007 at http://www.gcn.com/print/26_06/43312-1.html.

Evans, Robert. 2005. Nuclear Power: Back in the Game. *Power Engineering* 109(10):20-25.

Federal Energy Regulatory Commission. Updated April 22, 2008. About FERC. What FERC Does. Accessed 5.2008 at http://www.ferc.gov/about/ferc-does.asp.

Federal Energy Regulatory Commission. March 3, 2003. Critical Energy Infrastructure Information, Order No. 630. *Federal Register* 68: 46456.

Fein, Robert A., Bryan Vossekuil, and Gwen A. Holden. 1995. *Threat Assessment: An Approach to Prevent Targeted Violence*. National institute of Justice Research In

Action. July. Accessed 10.2007 at http://www.ustreas.gov/usss/ntac/ntac_threat.pdf.

Feld, Jacob, and Kenneth L. Carper. 1997. *Construction Failure.* Second Edition. New York City: John Wiley and Sons.

Ferguson, Charles D., and Michelle M. Smith. 2008. How Not to Build Nuclear Reactors. *Bulletin of the Atomic Scientists* 64(4): 20-26.

Ferguson, Charles D., and William C. Potter. 2004. *The Four Faces of Nuclear Terrorism.* Monterey, CA: Monterey Institute of International Studies.

Fingerprint Recognition Access for Construction Site. June 26, 2007. UK Biometrics International. Prosecurity Zone. Accessed 2.2008 at http://www.prosecurityzone.com/Customisation/News/Biometrics/Fingerprint_recognition/Fingerprint_recognition_access_for_construction_site.asp.

Finon, Dominique, Gis Larsen, and Fabien Roques. 2008. Contractual and Financing Arrangements for New Nuclear Investments in Liberalized Markets: Which Efficient Combination? CIRED. France. Accessed 9.2008 at http://www.cessa.eu.com/sd_papers/wp/wp2/0207_Finon_Roques.pdf.

Firesmith, Donald G. 2005. A Taxonomy of Security-Related Requirements. Software Engineering Institute. Carnegie Mellon University. International Workshop on High Assurance Systems (RHAS'05 - Paris), August 29-30, 2005. Accessed 9.2008 at http://www.sei.cmu.edu/programs/acquisition-support/publications/taxonomy.pdf.

Firesmith, Donald G. 2003. Common Concepts Underlying Safety, Security, and Survivability. Technical Note CMU/SEI-2003-TN-033. Pittsburgh, PA: Software Engineering Institute.

Flanagan, Roger, and G. Norman. 1993. *Risk Management and Construction*. New York: John Wiley and Sons.

Fournier, Paul. April 10, 2006. Construction's Bad Habit. *New England Construction*. April 2006.

Fowler, W.W. 1981. *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems.* RAND Report N-1503-RC. March 1981.

Freeman J., and B. Watson. 2006. An Application of Stafford and Warr's Reconceptualisation of Deterrence to a Group of Recidivist Drink Drivers *Accident Analysis and Prevention* 38 (3): 462-471.

French, Michael T., M. Christopher Roebuck, and Pierre Kebreau Alexandre. 2004. To Test or Not To Test: Do Workplace Drug Testing Programs Discourage Employee Drug Use. *Social Science Research* 33:45-63.

Garcia, M. L. 2006. *Vulnerability Assessment of Physical Protection Systems.* Boston: Butterworth-Heinemann.

Garcia, Mary Lynn. 2001. *The Design and Evaluation of Physical Protection Systems.* Boston: Butterworth-Heinemann.

Gaukler, Paul, D. Sean Barnett, and Douglas J. Rosinski. 2002. Nuclear Energy and Terrorism. *Natural Resources and Environment* (Winter):165-207. Accessed

1.2008 at
http://www.abanet.org/environ/pubs/nre/specissue/gauklerbarnettrosinski.pdf.

Georges, Christopher. September 1992. Power Play – Citizen Oversight of Nuclear Power Plants. *Washington Monthly*. Accessed 10.2007 at http://findarticles.com/p/articles/mi_m1316/is_n9_v24/ai_12529976.

Gerber, Jonathan K., and George S. Yacoubian, Jr. 2001. Evaluation of Drug Testing in the Workplace: Study of the Construction Industry. *Journal of Construction Engineering and Management* 127(6):438-444.

Gill, David. 2007. Construction's Movable Feast. *Building Magazine.* 13.04.2007. Accessed 7.2008 at http://www.linx-int.com/PDF/BuildingMagazine040407.pdf.

Goldman, John J. May 20, 1988. Mafia Dominates Building Trade in N.Y., Study Finds. *Los Angeles Times*. Part 1, Page 1, Column 5. Accessed 10.2007 at http://www.thelaborers.net/lexisnexis/articles/mafia_dominates_ny_building_trade.htm.

Goodall, Chris. January 14, 2008. Nuclear Power: The New Generation. *Carbon Commentary*. Accessed 3.2008 at http://www.carboncommentary.com/2008/01/14/70.

Gordon, J.S. 1995. Point Paper: Response to Commission on Protecting and Reducing Government Secrecy Request for Information. Lockheed Martin Skunk Works. 13 September. Accessed 10.2007 at http://www.fas.org/sgp/othergov/skunkworks.html.

Government Printing Office. January 1, 1982. Quality Assurance in Nuclear Powerplant Construction. Oversight hearing before the Subcommittee on Energy and the Environment of the Committee on Interior and Insular Affairs, House of Representatives, Ninety-Seventh Congress, First Session, November 19, 1981. Serial No 97-26. NRC Chairman Palladino testified. Accessed abstract 10.2007 at http://www.osti.gov/energycitations/product.biblio.jsp?osti_id=5486519.

Greenpeace International. 30 May 2007. Protest at Olkiluoto Nuclear Plant Construction Site. Accessed 3.2008 at http://www.greenpeace.org/international/news/olkiluoto-nuclear-plant-day.

Hall, Randolph, Howard Bowman, Michael Orosz, and Terry O'Sullivan. 2005. Assessment Guidelines for Counter Terrorism. Los Angeles, CA: University of Southern California Center for Risk and Economic Analysis of Terrorism Events. Prepared for FEMA. Available at http://www.usc.edu/dept/create/assets/001/50787.pdf.

Hammond, Grant T. 2006. Deterrence for the 21st Century. Revised version of presentation given to the CSAF's Deterrence Seminar.

Hapgood, Fred. September 15, 2008. Safety and Security: The Intersection. CSO Physical Security. Accessed 10.2008 at http://www.csoonline.com/article/448972/Safety_and_Security_The_Intersection.

Harrell, Adele, and John Roman. 2001. Reducing Drug Use and Crime among Offenders: The Impact of Graduated Sanctions. *Journal of Drug Issues* 31(1):207-232.

Harris, Paul. 2003. 9/11 Two Years On: Big Brother Takes Grip on America: The US Response to 11 September Has Been an Unprecedented Clampdown on the Rights of Its Own Citizens. *The Observer*. September 7. P. 20.

Haslam, R.A., S.A. Hide, A.G.F. Gibb, D.E. Gyi, T. Pavitt, S. Atkinson, and A.R. Duff. 2005. Contributing Factors in Construction Accidents. *Applied Ergonomics* 36:401-415.

Hendrickson, Chris, and Tung Au. 2008. *Project Management for Construction*. Version 2.2. Accessed 10.2008 at http://pmbook.ce.cmu.edu/.

Hess, Rachel O., Charles A. Holt, and Angela M. Smith. 2007. Coordination of Strategic Responses to Security Threats: Laboratory Evidence. *Experimental Economics* 10:235-250.

Hess, S. December 2006. Technical Elements of a Risk-Informed, Technology-Neutral Design and Licensing Framework for New Nuclear Plants. Palo Alto, CA: Electric Power Research Institute.

Hirsh, Daniel. Nd. The Truck Bomb and Insider Threats to Nuclear Facilities. Nuclear Control Institute, Washington, DC. Accessed 10.2007 at http://www.nci.org/g-h/hirschtb.htm.

Hoffman, Bruce. 2002. Re-Thinking Terrorism and Counterterrorism Since 9/11. *Studies in Conflict and Terrorism* 25(5):303-316.

Holmgren, Ake J. 2005. Electricity Case: Risk Analysis of Infrastructure Systems – Different Approaches for Risk Analysis of Electric Power Systems. Los Angeles, CA: University of Southern California Center for Risk and Economic Analysis of Terrorism Events. Prepared for FEMA. Accessed 12.2007 at http://www.usc.edu/dept/create/assets/001/50786.pdf.

Holzer, Harry J., Steven Raphael, and Michael A. Stoll. 2002. Will Employers Hire Ex-Offenders? Employer Preferences, Background Checks, and Their Determinants. Institute for Research on Poverty. Accessed 10.2008 at http://www.ssc.wisc.edu/irp/.

Homeland Security Council. 2007. *National Strategy for Homeland Security*. Washington, DC. October. Accessed 10/2007 at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

Homer-Dixon, Thomas. 2002. The Rise of Complex Terrorism. *Foreign Policy* Jan-Feb:52-63.

Honnellio, Anthony, and Stan Rydell. 2007. Sabotage Vulnerability of Nuclear Power Plants. *International Journal of Nuclear Governance, Economy, and Ecology* 1(3):312-321.

Hopey, Don. September 14, 2006. Worker at Beaver Valley Nuclear Plant Conceals Review Failures. *Pittsburgh Post-Gazette.* Accessed 10.2007 at http://www.post-gazette.com/pg/06257/721763-28.stm.

Howe, David. 2004. Planning Scenarios: Executive Summaries: Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities. Washington, D.C.: Homeland Security Council. Accessed 10.2007 at http://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04_exec-sum.pdf.

Hutchinson, Robert. 2003. The Struggle for Control of Radioactive Sources. *Jane's Intelligence Review* 15(3):32-35. April 1.

IBEW Journal. 2005. IBEW Implements Drug Testing for Officers, Reps, Management Staff. January/February. Accessed 2.2008 at http://www.ibew.org/articles/05journal/0501/p19.htm.

IceNews – Daily News. May 16, 2009. Finland's Olkiluoto Nuclear Plant Site Could Be Shut Down. Accessed 6.2008 at http://www.icenews.is/index.php/2009/05/16/finland%e2%80%99s-olkiluoto-nuclear-plant-site-could-be-shut-down/.

Idaho National Energy and Environmental Laboratory (INEEL). 2004. *Personnel Security Guidelines*. Prepared by the Control Systems Security and Test Center for the U.S. Department of Homeland Security. Idaho Falls, ID: INEEL. Accessed 10.2007 at http://www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf.

Idaho National Energy and Environmental Laboratory (INEEL). February 29, 2000. Summary of INEEL Findings on Human Performance During Operating Events. Report No. CCN 00-005421.

Information Systems Laboratories. September 2007. *Nuclear Power Plant Security Assessment Format and Content Guide*. Rockville, MD: Information Systems Laboratories.

International Atomic Energy Agency (IAEA). 2007. *Nuclear Technology Review*. Vienna.

International Atomic Energy Agency (IAEA). 2003. *Security of Radioactive Sources: Interim Guidance for Comment. Vienna*. Accessed 3.2008 at http://www-pub.iaea.org/MTCD/publications/PDF/te_1355_web.pdf.

International Atomic Energy Agency (IAEA). 2000. *Safety of Nuclear Power Plants: Design: Safety Requirements*. Vienna.

International Atomic Energy Agency (IAEA). September 1999. *Management of Delayed Nuclear Power Plant Projects.* IAEA-TECDOC-1110. Vienna. Accessed 8.2008 at http://www-pub.iaea.org/MTCD/publications/PDF/te_1110_prn.pdf.

Jain, J.K. 2004. Civil Construction in Nuclear Power Plants. *NuPower* 18(4). Accessed 8.2008 at http://www.npcil.nic.in/nupower_vol18_4/articles/02CivilConstruction.pdf.

Jergeas, G., and J. Van der Put. 2001. Benefits of Constructability on Construction Projects. *Journal of Construction Engineering and Management*. ASCE. 127(4):281-290. Assessed 10.2008 at http://www.civ.utoronto.ca/sect/coneng/tamer/Courses/CIV1278/REF/benefits.pdf.

Johnston, Wm. Robert. 2003. Nuclear Terrorism Incidents. Accessed 10.2007 at http://www.johnstonsarchive.net/nuclear/wrjp1855.html.

Jones, Craig, Neil Donnelly, Wendy Swift, and Don Weatherburn. 2006. Preventing Cannabis Users from Driving under the Influence of Cannabis. *Accident Analysis and Prevention* 38(5): 854-861.

Kapardis, Andreas. 2003. *Psychology and Law: A Critical Introduction*. Second Edition. Cambridge, UK: Cambridge University Press.

Kanter, James. May 29, 2009. In Finland, Nuclear Renaissance Runs Into Trouble. *The New York Times. Accessed 6.2009 at http://www.nytimes.com/2009/05/29/business/energy-environment/29nuke.html?_r=1&pagewanted=print.*

Katz, Alan. September 5, 2007. Nuclear Bid to Rival Coal Chilled by Flaws, Delay in Finland. *Bloomberg.Com. Accessed 2.2008 at http://www.bloomberg.com/apps/news?pid=20601087&sid=aFh1ySJ.IYQc.*

Keenan, Charlie. 2002. Nuclear Nightmare? *Science World*. March 11.

Keeney, M., E., E. Kowalski, D. Cappelli, T. Shimeall, and S. Rogers. 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Accessed 10.2007 at http://www.cert.org/archive/pdf/insidercross051105.pdf.

Kelly, Robert J. 1999. The Upperworld and the Underworld: Case Studies of Racketeering and Business Infiltrations in the United States. New York: Springer.

Kennedy, Kirk. June 2007. Personal Communication (telephone interview). Chief, National Center for the Study of Counterintelligence and Operational Psychology, Directorate of Behavioral Sciences. Counterintelligence Field Activity, U.S. Department of Defense.

Kennewick Police Department. Nd. Controlling Theft and Vandalism at Construction Sites. Crime Prevention Division. Kennewick, Washington. Accessed 2.2008 at www.ci.kennewick.wa.us.

The Keystone Center. June 2007. *Nuclear Power Joint Fact-Finding: Executive Summary*. Keystone, CO: The Keystone Center. Accessed 2.2008 at http://www.keystone.org/spp/energy/electricity/nuclear-power-dialogue.

Khalafallah, Ahmed, and Khaled El-Rayes. 2008. Minimizing Construction-Related Security during Airport Expansion Projects. *Journal of Construction Engineering and Management* 134(1):40-48.

Kosnick, Scott. 2005. Terrorism and its Impact on the Construction Industry. Maryland University College Park. Accessed 1.2008 at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA454873&Location=U2&doc=GetTRDoc.pdf.

Kovacich, Gerald, and Edward P. Halibozek. 2003. *The Manager's Handbook for Corporate Security: Elements of a Good Personnel Security Program*. Cambridge: Butterworth-Heinemann.

Kraemer, Sara, and Pascale Carayon. 2007. Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists. *Applied Ergonomics* 38:143-154.

Kramer, Lisa A., Richards J. Heuer, Jr., and Kent S. Crawford. May 2005. *Technological, Social, and Economic Trends That are Increasing U.S. Vulnerability to Insider Espionage*. PERSEREC. Technical Report 01-10. Conducted by the Defense Personnel Security Research Center. Monterey, CA. Accessed 12.2008 at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=A433793&Location=U2&doc=GetTRDoc.pdf.

Krouse, William J., and Bart Elias. September 6, 2006. *Terrorist Watchlist Checks and Air Passenger Prescreening.* Washington, DC: U.S. Government Accountability Office.

Kull, L., L. Harris, Jr., and J. Glancy. 1977. VISA – A Method for Evaluating the Performance of a Facility Safeguards System. *Institute of Nuclear Materials Management Proceedings* 6(3):292-301.

Kunreuther, Howard, and Erwann Michel-Kerjan. 2004. Policy Watch: Challenges for Terrorism Risk insurance in the United States. *Journal of Economic Perspectives* 18(4):201-214. Accessed 10.2007 at http://opim.wharton.upenn.edu/risk/downloads/05-03-HK.pdf.

Landoll, Douglas J. 2006. *The Security Risk Assessment Handbook*. New York: Auerback Publications. *Dallas Morning News*. Accessed 2.2009 at http://www.dallasnews.com/sharedcontent/dws/bus/stories/DN-finnuclear_21bus.ART0.State.Edition1.4a5e710.html.

Landers, Jim. December 21, 2008. Texas Can Take Lessons from Finland's Nuclear Power Plant Delays.

Large and Associates. June 8, 2006. European Pressurized Reactor at Olkiluoto 3, Finland: Brief and Interim Review of the Porosity and Durability Properties of the In Situ Cast Concrete at the Olkiluoto EPR Construction Site. Accessed 10.2008 at http://www.largeassociates.com/3149%20Olkiluoto/R3149-A1%20Final%20Issue.pdf.

Larson, Sharon L., Joe Eyerman, Misty S. Foster, Joseph C. Gfroerer. 2007. *Worker Substance Use and Workplace Policies and Programs*. DHHS Publication No. SMA 07-4273, Analytic Series A-29. Rockville, MD: Department of Health and Human Services Substance Abuse and Mental Health Services Administration.

Laughter, Mark. 2005. *U.S. Nuclear Power Plants as Terrorist Targets: Threat Perception and the Media*. Master's Thesis. Department of Nuclear Science and Engineering. Cambridge, MA: Massachusetts Institute of Technology. Accessed 10.2007 at http://www.oas.samhsa.gov/work2k7/toc.cfm.

Lean, Geoffrey, and Jonathan Owen. April 13, 2008. Defects Found in Nuclear Reactor the French Want to Build in Britain. *The Independent* (UK). Accessed 9.2008 at http://www.independent.co.uk/news/uk/home-news/defects-found-in-nuclear-reactor-the-french-want-to-build-in-britain-808461.html.

Leibert, Richard A. 2007. The War on Energy: Why the United States and the international Community Need Cohesive Energy Infrastructure Security Policy. *Houston Journal of International Law* 29(2):453-483.

Levin, Brian, and Sara-Ellen Amster. 2003. An Analysis of the Legal Issues Relating to the Prevention of Nuclear and Radiological Terrorism. *American Behavioral Scientist* 46(6);845-856.

Lewis, Ted G. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: Wiley and Sons, Inc.

Libicki, Martin C., Peter Chalk, and Melanie Sisson. 2007. *Exploring Terrorist Targeting Preferences.* Prepared by the Rand Corporation for the U.S. Department of

Homeland Security. Accessed 10.2007 at http://www.rand.org/pubs/monographs/2007/RAND_MG483.pdf.

Lochbaum, David. October 16, 2006. Nuclear Revival or Nuclear Re-Run? Union of Concerned Scientists. Accessed 1.2008 at http://www.ucsusa.org/assets/documents/clean_energy/20061016-ucs-nrc-new-reactors.pdf.

Lowhurst, D.G., February 7, 2003. The New Federal Insurance Program for Terrorist Acts: How it Works and the Open Issues. Accessed 1.2008 at http://www.constructionweblinks.com/Resources/IndustryReportsNewsletter/Feb_12 2003.

Lyman, Edwin. 2003. Nuclear Plant Protection and the Homeland Security Mandate. Presented at the 2003 meeting of the Institute of Nuclear Materials Management. Union of Concerned Scientists Global Security Program. Accessed 5.2008 at http://www.ucsusa.org/global_security/nuclear_terrorism/nuclear-plant-protection-and.html.

Lyman, Edwin S., and David Lochbaum. 2006 Protecting Vital Targets: Nuclear Power Plants. Chapter 8 in *Homeland Security: Protecting America's Targets. Vol. 3. Critical Infrastructure.* Edited by James J.F. Forest. Westport, CT: Praeger Security International.

Lyons, Peter B. March 9, 2005. Perspectives Upon Joining the Nuclear Regulatory Commission. Presented at the Regulatory Information Conference, Rockville, MD. U.S. Nuclear Regulatory Commission Office of Public Affairs. Document No. S-05-005. Accessed 11.2007 at http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2005/s-05-005.pdf.

Macallier, Daniel. Drug Use and Justice: An Examination of California Drug Policy Enforcement. Press Release. Center on Juvenile and Criminal Justice. Accessed 12.2007 at http://www.cjcj.org/pubs/cadrug/cadrug.html.

Magnusson, Niklas, and Janina Pfalzer. May 21, 2008. Sweden Police Hold Two on Nuclear Sabotage Suspicion (Update 6). Bloomberg.com. Accessed 5.2008 at http://www.bloomberg.com/apps/news?pid=20601100&sid=a0xJ_LqsYoWE&refer=germany.

Mannisto, Ilkka. 2005. *Risk-Informed Classification of Systems, Structures and Components in Nuclear Power Plants*. Master's Thesis. Department of Engineering, Helsinki University of Technology. Accessed 10.2007 at http://www.sal.hut.fi/Publications/pdf-files/TMAN05.pdf.

Manski, C., J. Pepper, and C. Petrie, eds. 2001. Informing America's Policy on Illegal Drugs: What We Don't Know Keeps Hurting Us. Prepared for the National Research Council. Washington, DC: National Academy Press.

Maritime Transportation Security Act of 2002. 46 USC 2101. November 25, 2002. PL 107-295. Accessed 10.2007 at http://www.tsa.gov/assets/pdf/MTSA.pdf.

Martinez-Moyano, Ignacio J., Eliot H. Rich, Stephen H. Contad, and David F. Andersen. 2006. Modeling the Emergence of Insider Threat Vulnerabilities. *Proceedings of the 2006 Winter Simulation Conference*. Accessed 3.2008 at http://www.dis.anl.gov/publications/articles/Martinez-Moyano_et_al_2006_WSC.pdf.

McDonald, Patrick H. 2001. *Fundamentals of Infrastructure Engineering: Civil Engineering Systems*. New York: M. Dekker.

McGaffigan, Edward. March 13, 2007. Remarks at NRC's Regulatory Information Conference. No. S-07-020. Accessed 10.2007 at http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2007/s-07-020.html.

Meletiadis, Ananias. 2004. *The Deterrence Effect of the Implementation of the Department of Defense's Drug Prevention Policy among Military Personnel*. Thesis for the Naval Postgraduate School. Monterey, CA.

Meserve, Richard A. June 18, 2001. The Evolution of Safety Goals and their Connection to Safety Culture. Presentation to the Atomic Energy Society of Japan/American Nuclear Society Topical Meeting on Safety Goals and Safety Culture. Milwaukee, WI. Accessed 1.2008 at http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2001/s01-013.pdf.

Meserve, Richard A. April 11, 2002. Statement Submitted by the United States Nuclear Regulatory Commission to the Subcommittee Oversight and Investigations Committee on Energy and Commerce, United States House of Representatives Concerning Nuclear Power Plant Security. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/congress-docs/congress-testimony/2002/04-11-02SecTestimony.pdf.

Meserve, Richard. A. February 12, 2002. Risk-Informed Regulation and Reactor Oversight. Presentation to Naval Reactors Staff. Washington, DC. Accessed 5.2008 at http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2002/s02-002.html.

Michael, James B., Steven E. Roberts, Jeffrey M. Voas, and Thomas C. Wingfield. 2005. The Role of Policy in Balancing Outsourcing and Homeland Security. *IT Pro* July-August:19-23.

Minchin, Jr., R. Edward, Charles R. Glagola, Kelu Guo, and Jennifer L. Languell, 2006. Case for Drug Testing of Construction Workers. *Journal of Management in Engineering* 22(1): 43-50.

MIPT Terrorism Knowledge Base. Accessed 10.2007 at http://www.tkb.org/. Includes a bibliography search engine. Accessed 10.2007 at http://www.terrorisminfo.mipt.org/TerrorismBibliography.asp.

Mitchell, Alison. March 28, 1993. Letter Explains Motive in Bombing, Officials Now Say. *New York Times.*

Mohtadi, Hamid, and Antu Murshid. 2006. A Global Chronology of Incidents of Chemical, Biological, Radioactive, and Nuclear Attacks: 1950-2005. Milwaukee, WI: University of Wisconsin. Sponsored by the U.S. Department of Homeland Security.

Moore, C., V. Barnes, J. Hauth, R. Wilson, J. Fawcett-Long, J. Toquam, K. Baker, D. Wieringa, J. Olson, and J. Christensen. 1989. *Fitness for Duty in the Nuclear Power Industry: A Review of Technical Issues. Supplement 1*. Seattle, WA: Battelle Human Affairs Research Centers. NUREG/CR-5227 Supplement 1.

Moteff, John, and Paul Parfomak. October 1, 2004. Critical Infrastructure and Key Assets: Definitions and Identification. Congressional Research Service. Report for

Congress. Washington, DC: The Library of Congress. Order code RL32631 Accessed 12.2008 at http://www.fas.org/sgp/crs/RL32631.pdf.

Mufson, Steven. January 4, 2008. Video of Sleeping Guards Shakes Nuclear Industry. *Washington Post.Com.* Accessed 3.2008 at http://www.washingtonpost.com/wp-dyn/content/article/2008/01/03/AR2008010304442_pf.html.

Muir, Bob. 2005. Challenges Facing Today's Construction Manager. Supplemental Reading for University of Delaware Course on Construction Methods and Management. Accessed 7.2008 at http://www.ce.udel.edu/courses/CIEG%20486/Challenges%20Facing%20Today's%20CM.pdf.

Mullen, S.A., J.J. Davidson, and H.B. Jones, Jr. 1980. *Potential Threats to Licensed Nuclear Activities from Insiders*. NUREG-0703. Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards.

National Association of Home Builders. 2008. *Residential Construction Industry Fatalities 2003-2006.* National Association of Home Builders. Accessed 3.2008 at http://www.nahb.org/fileUpload_details.aspx?contentTypeID=3&contentID=88793&subContentID=131641.

National Association of Professional Background Screeners. August 4, 2005. Re: Criminal History Background Checks: Request for Comments. [To the Department of Justice]. Accessed 2.2008 at http://www.usdoj.gov/olp/pdf/0394_001.pdf.

National Conference of State Legislatures. January 2006. State Statute Chart on Drug Testing in the Workplace. Accessed 3.2008 at http://www.ncsl.org/programs/employ/drugtest.htm.

National Conference of State Legislatures. nd. Real ID Act of 2005 Driver's License Title Summary. Accessed 10.2007 at http://www.ncsl.org/print/standcomm/sctran/realidsummary05.pdf.

National Institute of Standards and Technology (NIST). January 2007. Biometric Data Specification for Personal Identity Verification. U.S. Department of Commerce. Accessed 10.2007 at http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf.

National Legal and Policy Center. 2003. Union Corruption Update Volume 3(5). Organized Labor Accountability Project. Accessed 10.2007 at http://www.nlpc.org/olap/UCU4/06_05_02.htm.

National Research Council of the National Academies. 2006. *Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities.* Washington DC: The National Academies Press.

Nation's Building News. April 7, 2008. Language Barriers Could Contribute to Job Site Fatalities. Accessed 7.2008 at http://www.nbnnews.com/NBN/issues/2008-04-07/Safety/index.html.

New York Times. February 14, 1988. Reactor Report Stirs Up Seabrook. Accessed 1.2007 at http://query.nytimes.com/gst/fullpage.html?res=940DE7DC133FF937A25751C0A96E948260.

NIDA Research Monograph, Number 63. *Prevention Research: Deterring Drug Abuse Among Children and Adolescent.* Accessed 12.2007 at http://www.nida.nih.gov/pdf/monographs/download63.html.

Nishimura, R., R. Bari, P. Peterson, R. Roglans-Ribas, and D. Kalenchuk. 2004. Development of a Methodology to Assess Proliferation Resistance and Physical Protection for Generation IV Systems. Americas Nuclear Energy Symposium, Miami Beach, FL. November 3-6, 2004. Accessed 10.08 at http://www.osti.gov/bridge/servlets/purl/841454-sC3HV2/native/841454.pdf.

North American Electric Reliability Council (NERC). 2002a. Security Guidelines for the Electricity Sector: Employment Background Screening. Accessed 10.2007 at http://www.esisac.com/library-guidelines.htm.

North American Electric Reliability Council (NERC). 2002b. Security Guidelines for the Electricity Sector: Physical Security. Accessed 10.2007 at http://www.esisac.com/library-guidelines.htm.

North American Electric Reliability Council (NERC). 2002c. Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information. Accessed 10.2007 at http://www.esisac.com/library-guidelines.htm.

North American Electric Reliability Council (NERC). 2002d. Security Guidelines for the Electricity Sector: Threat Response. Accessed 10.2007 at http://www.nerc.com/cip.html.

North American Electric Reliability Council (NERC). 2002e. Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment. Accessed 10.2007 at http://www.esisac.com/library-guidelines.htm.

Nuclear Energy Institute (NEI). 2008. Nuclear Power 2010: A Key Building Block for New Nuclear Power Plants. November.

Nuclear Energy Institute (NEI). 2006. Licensing New Nuclear Power Plants. October. Accessed 10.2007 at www.nei.org/index.asp?catnum=3&catid=1262.

Nuclear Energy Institute (NEI). September 25, 2006. News release – Nearly Seven of 10 Americans Favor Nuclear Energy, Support Building New Reactors at Existing Sites. Accessed 10.2007 at http://www.nei.org/newsandevents/americansfavornuclear/.

Nuclear Energy Institute (NEI). May 2003. Fact Sheet: Nuclear Plant Security. Accessed 4.2008 at http://www.nei.org/doc.asp?catnum=3&catid=290&docid=&format=print.

Nuclear Engineering International. May 9, 2006. Concrete Composition Delays Finland's Olkiluoto 3. Accessed 4.2008 at http://www.neimagazine.com/story.asp?storyCode=2036021.

Nuclear Engineering International. July 19, 2006. Regulator Reports as OL3 Delays Reach One Year. Accessed 4.2008 at http://www.neimagazine.com/story.asp?sectionCode=132&storyCode=2037524.

Nuclear Monitor. March 7, 2003. 25 Years Ago. World Information Service on Energy.

Oak Ridge Institute for Science and Education (ORISE). 2001. Personnel Security Assurance Program: Profile from 1992 through 2000. Prepared for the U.S. Department of Energy. Oak Ridge, TN: ORISE.

Office of Management and Budget. August 5, 2005. Implementation of Homeland Security Presidential Directive (HPSD)-1 Policy for a Common Identification Standard for Federal Employees and Contractors.

O'Malley, Penelope Grenoble 2001. Safety, Liability, Productivity: Breaking the Language Barrier on Construction Sites. Accessed 4.2007 at http://www.mstraka.com/portfolio/zerah/news2.pdf.

O'Neil, Michael and James X. Dempsey. 2000. Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry. *Depaul Business Law Journal* 12:97-117. Accessed 1.2008 at http://www.cdt.org/publications/lawreview/2000depaul.shmtl.

Ohio Bureau of Workers' Compensation. 2006. Ohio Law Makes Drug-Free Workplace Programs a Requirement for all State Construction Contractors. Accessed 12.23.07 at http://www.bwc.state.oh.us/employer/services/StateContract/StateContractdescriptions.asp.

Olmstead, Todd A., Jody L. Sindelar, Caroline J. Easton, and Cathleen M. Carroll. 2007. The Cost-Effectiveness of Four Treatments for Marijuana Dependence. *Addiction* 109(9):1443-1453.

Organization of Economic Development and Cooperation. July 2003. Security in Maritime Transport: Risk Factors and Economic Impact. Directorate for Science, Technology and Industry. Accessed 7.2007 at http://www.oecd.org/dataoecd/63/13/4375896.pdf.

Parfomak, Paul W. 2004. Guarding America: Security Guards and U.S. Critical Infrastructure Protection. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress. Order code RL32670. Accessed 10.2006 at http://fas.org/sgp/crs/RL32670.pdf.

Parfomak, Paul W. Updated October 4, 2007. Liquified Natural Gas (LNG) Infrastructure Security: Issues for Congress. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress. Order code RL32073.

Parkinson, Gerald. 2002. Terror-Proofing CPI Plants: Store Chemicals Properly, Limit Access to Control Rooms and Screen Employees. *Chemical Engineering* 109(1):27-32.

Parliamentary Office of Science and Technology. 2004. *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*. Report 222. Accessed 4.2008 at http://www.parliament.uk/documents/upload/POSTpr222.pdf.

Patterson, S.A., and G.E. Apostolakis. 2007. Identification of Critical Locations Across Multiple Infrastructures for Terrorist Actions. Reliability Engineering and System *Safety* 92:1183-1203.

Penney, Steven. 2007. Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach. *The Journal of Criminal Law and Criminology* 97(2):477-529.

Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk.* Princeton, NJ: Princeton University Press.

Petersen, Karen Lund. 2008. Terrorism: When Risk Meets Security. *Alternatives* 33:173-190.

Plant, Jeremy F. 2005. Competing Models for Enhancing Railroad Security. *The Public Manager* 34(3):13-20.

Pope, Daniel. 1990. Environmental Constraints and Organizational Failures: The Washington Public Power Supply System. *Business and Economic History* 19:74-82. Accessed 10.2006 at http://www.h-net.org/~business/bhcweb/publications/BEHprint/v019/p0074-p0082.pdf.

Pridemore, William Alex and Joshua D. Frielich. 2007. The Impact of State Laws Protecting Abortion Clinics and Reproductive Rights on Crimes Against Abortion Providers: Deterrence, Backlash, or Neither? *Law and Human Behavior* 31:611-627.

Privacy International. April 2004. Mistaken Identity: Exploring the Relationship between National Identity Cards and the Prevention of Terrorism. Washington DC. Accessed on 1.2008 at http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf.

Project On Government Oversight (POGO). August 6, 2007. Another Security Breach at Los Alamos. Accessed 4.2008 at http://www.pogo.org/pogo-files/alerts/nuclear-security-safety/nss-lanl-20070806.html.

Project On Government Oversight (POGO). September 12, 2002. Nuclear Power Plant Security: Voices from Inside the Fences. Accessed 4.2008 at http://www.pogo.org/p/environment/eo-020901-nukepower.html.

Pro-Vigil. 2007. Reducing Employee-Driven Job Site Theft. Accessed 8.2008 at http://www.pro-vigil.com/news/2007/10/reducing-employee-driven-job-site-theft/.

Prowler, Don. 2008. Whole Building Design. Whole Building Design Guide. National Institute of Building Sciences. Accessed 2.2009@ http://www.wbdg.org/wbdg_approach.php.

Purvis, James W. 1999. Sabotage at Nuclear Power Plants. Sandia National Laboratories. Albuquerque, NM. Accessed 1.2008 at http://www.osti.gov/bridge/servlets/purl/9593-cl8jIh/webviewable/9593.pdf.

Rasmussenn, Gideon T. nd. Insider Risk Management Guide. Accessed 5.2008 at http://www.gideonrasmussen.com/article-13.html.

Recent Terrorist Plots Highlight Insider Threat. 7 August 2007. Joint Homeland Security Assessment. Office of Intelligence and Analysis Homeland Security and Federal Bureau of Investigation.(Unclassified/OUO) Accessed 5.2008 at http://www.naiop.org/membersArea/government/reisac070807.pdf.

Regulation on Ensuring the Safety of Nuclear Power Plants. 2004 (amended June 2008) . OJ Issue 66. July. Accessed 10.2007 at http://www.bnsa.bas.bg/legislate/regulations/en/reg_safnpp_en.pdf.

Renfroe, Nancy A., and Joseph L. Smith. 2008. Threat/Vulnerability Assessment and Risk Analysis. Whole Building Design Guide. National Institute of Building Sciences. Accessed 2.2009 at http://www.wbdg.org/resources/riskanalysis.php.

Reuters. May 27, 2008. French Nuke Body Partly Halts Work on New Reactor. Accessed 10.2008 at http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSL2762459720080527.

Reyes, Luis A. September 14, 2004. Statement Submitted by the United States Nuclear Regulatory Commission to the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, United States House of Representatives Concerning Homeland Security: Monitoring Nuclear Power Plant Security.

Reynolds, Lawrence A. 2005. Historical Aspects of Drugs-of-Abuse Testing in the United States. In *Drugs of Abuse: Body Fluid Testing*. Raphael C. Wong and Harley Y Tse, editors. Totowa, NJ: Humana Press. Pp.1-10.

Rienstra, A. September 16, 2008. Splitting the Atom Costs Double in Finland. *IceNews – Daily News*. Accessed 2.2009 at http://www.icenews.is/index.php/2008/09/16/splitting-the-atom-costs-double-in-finland/.

Roberts, Steven. 2004. Tips and Trends for Homeland Security and Critical Infrastructure Protection. J*ournal of Homeland Security and Emergency Management* 1(4). Accessed 11.2007 at http://www.bepress.com/cgi/viewcontent.cgi?article=1080&context=jhsem.

Rosoff, H., and D. von Winterfeldt. 2007. A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach. *Risk Analysis* 27(3):533-546.

Rossin, A. David. 2003. Marketing Fear: *American Behavioral Scientist* 46(6):812-821.

Rothbart, Myron, and Bernadette Park. 1986. On the Confirmability and Disconfirmability of Trait Concepts. *Journal of Personality and Social Psychology* 50(1):131-142.

Russell, Pam Radtke. September 3, 2008. Fuel Facility Faces Fights for Funds, Workers and Suppliers. *Engineering News Record.* Accessed 11.3.08 at http://enr.construction.com/news/powerIndus/archives/080917.asp.

Sandler, Todd, and Kevin Siqueira. 2006. Global Terrorism: Deterrence versus Pre-emption. *Canadian Journal of Economics* 39(4):1270-1387.

Santos, J.R., and Y.Y. Haimes. 2002. Modeling the Psychological-Economic-Based Inoperability of Interconnected Infrastructures Due to Terrorism. Presented at the Society for Risk Management Annual Meeting.

Sassoon, David. September 19, 2008. Faulty Welds, Soaring Costs at Nuclear Plant in Finland. SolveClimate.Com. Accessed 2.2009 at http://solveclimate.com/blog/20080919/faulty-welds-soaring-costs-nuclear-plant-finland.

Savage, J.A. June 6, 2003. A Nuclear Whistleblower at Home. *AlterNet.*

Sawai, Masako. 2001. Rokkasho: A Troubled Nuclear Fuel Cycle Complex. *Science for Democratic Action* 9(4). Accessed 9.2008 at http://www.ieer.org/sdafiles/vol_9/9-4/rokkasho.html.

Schneider, Mycle. December 2001. The Threat of Nuclear Terrorism: From Analysis to Precautionary Measures. Presented at the *Democracies Faced with Mass Terrorism Meeting*, Paris. Accessed 5.2008 at http://www.wise-paris.org/english/reports/conferences/011210Terrorisme.pdf.

Schultz, Eugene. 2006. Convergent Security Risks in Physical Security Systems and IT Infrastructures. The Alliance for Enterprise Security Risk Management.

The Secretary of the Navy. June 2006. Department of the Navy Personnel Security Program. Washington, DC: Chief of Naval Operations (N09N) Special Assistant for Naval Investigative Matters and Security.

Seper, Jerry. September 16, 2005. 3 Illegals Arrested at Nuclear Station. *The Washington Times*.

Shaw, Eric, and Lynn F. Fischer. 2005 Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations. Accessed 1.2008 at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=A441293&Location=U2&doc=GetTRDoc.pdf.

Shea, Dana A. 2004. Critical Infrastructure: Control Systems and the Terrorist Threat. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress. Available at http://www.fas.org/irp/crs/RL31534.pdf.

Shearer, Robert A. 1999. Statement Analysis: Scan or Scam? – Scientific Content Analysis. *The Skeptical Inquirer*. May-June. Accessed 4.2008 at http://findarticles.com/p/articles/mi_m2843/is_3_23/ai_54600095/print?tag=artBody;col1.

Sheldon, F., T. Potok, A. Loebl, A. Krings, and P. Oman. 2004. Energy Infrastructure Survivability, Inherent Limitations, Obstacles, and Mitigation Strategies. *International Journal of Power and Energy Systems.*

Sitren, Alicia H., and Brandon K. Applegate. 2007. Testing the Deterrent Effects of Personal and Vicarious Experience with Punishment and Punishment Avoidance. *Deviant Behavior* 28:29-55.

Smith, Tim. November 2, 2008. NRC Cautions Nuke Industry after Discovery of Bad Concrete and Steel at SRS. *The Greenville News*. Accessed 11.4.08 at http://www.greenvilleonline.com/article/20081102/NEWS01/81102011/1059/ENT03.

Snowden, Lynne L. 2003. How Likely are Terrorists to Use a Nuclear Strategy? *American Behavioral Scientist* 46(6):699-713.

Sowman, Colin. 2005. Protecting Plant: The Second Construction Industry Theft Scheme Forum. *Plant Manager's Journal*. 10.01.2005. Accessed 8.2008 at http://www.accessmylibrary.com/coms2/summary_0286-12020571_ITM.

Stapleton, B.W. September 2005. Designation Guide for Safeguards Information. OUO-Security-Related Information. U.S. Nuclear Regulatory Commission, Division of Nuclear Security, Office of Nuclear Security and Incident Response.

Stasinopoulos, P., M. Smith, K. Hargroves, and C. Desha. 2009. *Whole System Design: An Integrated Approach to Sustainable Engineering*. London: Earthscan and The Natural Edge Project, Australia.

State of Idaho Legislature. 2004. Senate Bill No. 1373 State Construction Contracts. Accessed 5.2008 at http://www3.state.id.us/oasis/2003/S1373.html#daily.

Stevens, Gina Marie. February 28, 2003. Homeland Security Act of 2002: Critical Infrastructure Information Act. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress.

Strelan, Peter, Robert J. Boeckmann. 2006. Why Drug Testing in Elite Sport Does Not Work: Perceptual Deterrence Theory and the Role of Personal Moral Beliefs. *Journal of Applied Social Psychology* 36 (12):2909–2934.

Stump, Jake. 2007. Contractors Do Drug Tests Already. Head of Trade Group Says State is Lagging behind Private Sector. *Charleston Daily Mail.* Monday February 12. Accessed 10.2007 at http://www.actwv.org/press/2007_Drug_Test.mx.

Sun, Yu, Dongping Fang, Shouqing Wang, Mengdong Dai, and Xiaoquan Lv. 2008. Safety Risk Identification and Assessment for Beijing Olympic Venues Construction. *Journal of Management in Engineering*. January.

Sung, Hung-En, and Linda Richter. 2007. Rational Choice and Environmental Deterrence in the Retention of Mandated of Mandated Drug Abuse Treatment Clients. *International Journal of Offender Therapy and Comparative Criminology* 51(6):686-702. Accessed 10.2007 at http://ijo.sagepub.com/cgi/content/abstract/51/6/686.

Taipai Times. 2003. Russian Bugs were Everywhere. Accessed 10.2007 at http://www.taipeitimes.com/News/feat/archives/2003/09/15/2003067981.

Tarer, A., and C.S. Signorino. 2006. A Unified Theory and Test of Extended Immediate Deterrence. *American Journal of Political Science* 50(3):586-605.

Tennessee Valley Authority (TVA). 2008. *Bellefonte Nuclear Plants Units 3 &4. COL Application. Part 3: Applicant's Environmental Report – Combined License Stage. Revision 1.* ML083100295. Accessed 10.2008 at http://adamswebsearch2.nrc.gov/idmws/ViewDocByAccession.asp?AccessionNumber=ML083100559.

Thompson Hine. July 2003. Drug Testing Required on State Construction Projects in Ohio. Accessed 3.2008 at http://www.thompsonhine.com/news/nl/emp_july2003.pdf.

Thomas, Ralph C. 1977. Organized Crime in the Construction Industry. *Crime and Delinquency* 23(3):304-311.

Todd, Mike, Carol Colwill, and Dave Allen. 2002. Benchmarking for Critical Infrastructure Protection. *Information Security Technical Report* 7(2):37-49. Accessed 1.2008 at http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VJC-46NYBJP-5-T&_cdi=6091&_user=2741876&_orig=search&_coverDate=06%2F01%2F2002&_sk=999929997&view=c&wchp=dGLbVzz-zSkzS&md5=7b928c28d5ac7ef97188ed11c3401590&ie=/sdarticle.pdf.

Transportation Security Administration Employee Screening Program. Accessed 10.2007 at http://www.tsa.gov/what_we_do/layers/employee_screening.shtm.

Transportation Worker Identification Credential (TWIC) Website FAQs. Accessed 10.2007 at http://www.asdd.com/pdf/secinfo_twic_faq.pdf.

Turnbull, Wayne, and Praveen Abjayaratne. 2003. 2002 WMD Terrorism Chronology: Incidents Involving Sub-National Actors and Chemical, Biological, Radiological, and Nuclear Materials. Monterey Institute of International Studies. Center for Nonproliferation Studies. Accessed 10.2007 at http://cns.miis.edu.

Union of Concerned Scientists. September 14, 2004. Statement Submitted by David Lochbaum to the Subcommittee on National Security, Emerging threats, and International Relations, U.S. House of Representatives. Accessed 5.2008 at http://www.ucsusa.org.

United Facilities Criteria (UFC 4-010-01). October 8, 2003. DoD Minimum Anti-Terrorism Standards for Buildings. http://www.acq.osd.mil/ie/irm/irm_library/UFC4_010_01-31JUL2002.pdf.

U. S. Chamber of Commerce Coalition against Counterfeiting and Piracy (CACP). Nd. Secure Supply Chain Best Practices Tool Kit. Accessed 11.2008 at http://www.thecacp.com/NR/rdonlyres/ekj5ugvm77u346ckgltwkgehlhsbdxloq3cix25ayxvsu7ydraxj3jgdoqp2nifjhev3qzapqgwgpqduepeeymgxn4h/FinalSupplyChainToolKit1.5.07.pdf.

U.S. 107th Congress. 2002. An Act to Establish the Department of Homeland Security, and for Other Purposes (Homeland Security Act of 2002). *Public Law 107-296*. Accessed 1.2008 at http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

U.S. 107th Congress. 2002. The National Construction Safety Team Act. *Public Law 107-231*. Accessed 1.2008 at http://www.nist.gov/public_affairs/releases/hr46871.pdf.

U.S. Citizenship and Immigration Services. Updated November 11, 2007. About Form I-9, Employment Eligibility Verification. Accessed 3.2008 at http://www.wm.edu/hr/forms/About%20I-9.pdf.

U.S. Code of Federal Regulations. Part 42. Section 15801. *Public Law 109-58 Energy Policy Act of 2005*. August 8, 2005. U.S Congress (109th). Accessed 10.2006 at http://www.epa.gov/oust/fedlaws/publ_109-058.pdf.

U.S. Code of Federal Regulations. Part 11. Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material. Title 10. Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Department of Defense (DoD). 1999. DoD Insider Threat Mitigation. Final Report of the Insider Threat Integrated Process Team. Prepared by IATAC for the Defense Technical Information Center. Accessed 10.2008 at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380&Location=U2&doc=GetTRDoc.pdf.

U.S. Department of Energy (DOE). 2000. Polygraph Examination Regulation. *Federal Register* 64(242):70961-70980.

U.S. Department of Energy (DOE). 2006. Human Reliability Program: Detection of Unusual Behavior Participant Manual. Prepared by the Oak Ridge Institute for

Science and Education for the U.S. Department of Energy's Office of Health, Safety, and Security, Office of Security Policy. Washington, DC.

U.S. Department of Energy (DOE). Approved July 2006. Order 413.3A: Program and Project Management for the Acquisition of Capital Assets. Accessed 1.2008 at http://www.directives.doe.gov/pdfs/doe/doetext/neword/413/o4133a.pdf.

U.S. Department of Energy (DOE). August 26, 2005. DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. Washington, DC.

U.S. Department of Energy (DOE). September 30, 2002. DRAFT Vulnerability Assessment Methodology: Electric Power Infrastructure. Washington, DC: Office of Energy Assurance.

U.S. Department of Energy (DOE). September 28, 2001a. Vulnerability Assessment and Survey Program: Lessons Learned and Best Practices. Washington, DC: Office of Energy Assurance.

U.S. Department of Energy (DOE). September 28, 2001b. Vulnerability Assessment and Survey Program: Overview of Assessment Methodology. Washington, DC: Office of Energy Assurance.

U.S. Department of Energy (DOE). May 8, 2001. DOE P 470.1, *Integrated Safeguards and Security Management*. Washington, DC.

U.S. Department of Energy/Office of the Inspector General (DOE). June 2005. Inspection Report: Security Access Controls at the Y-12 National Security Complex. DOE/IG-0691. Accessed 1.2008 at http://www.ig.energy.gov/documents/CalendarYear2005/ig-0691.pdf.

U.S. Department of Homeland Security (DHS) Transportation Security Administration. Frequently Asked Questions Transportation Worker Identification Credential (TWIC). Accessed 2.2008 at http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm.

U.S. Department of Homeland Security (DHS). April 17, 2009. DHS Exhibit 300 Public Release BY10 / NPPD – US-VISIT – Automated Biometric Identification System (IDENT) (2010). Accessed 8.2009 at http://www.dhs.gov/xlibrary/assets/mgmt/e300-nppd-usvisit-ident2010.pdf.

U.S. Department of Homeland Security (DHS). January 29, 2008. Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes. 6 CFR Part 37. *Federal Register* 73(19):5271-5340. Accessed 5.2008 at http://a257.g.akamaitech.net/7/257/2422/29jan20081800/edocket.access.gpo.gov/2008/08-140.htm.

U.S. Department of Homeland Security (DHS). 2007. Chemical Facility Anti-Terrorism Standards Interim Final Rule 6 CFR Part 27. DHS-2006-0073. Accessed 12.2007 at http://www.ombwatch.org/info/IP_ChemicalFacilitySecurity.pdf.

U.S. Department of Homeland Security (DHS). 2007. Critical Infrastructure Protection Training Program (DIPTP). Federal Law Enforcement Training Center. Training Program Announcement and Topic Outline. Accessed 1.2008 at http://www.fletc.gov/training/programs/counterterrorism-division/critical-infrastructure-protection-training.

U.S. Department of Homeland Security (DHS). November 2007. Part II 6 CFR Part 27. Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule. *Federal Register* 72(223):65396-65435. Accessed 12.2007 at http://www.dhs.gov/xlibrary/assets/chemsec_appendixafinalrule.pdf.

U.S. Department of Homeland Security (DHS). October 2007. Privacy Impact Assessment for the Transportation Worker Identification Credential Program. Contact Point John Schwarts. Accessed 12.2007 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_twic_fr.pdf.

U.S. Department of Homeland Security (DHS). 2007. Form I-9, Employment Eligibility Verification. OMB No. 1815-0047. Accessed 10.2007 at http://www.uscis.gov/files/form/I-9.pdf.

U.S. Department of Homeland Security (DHS). September 1, 2006. Part IV 6 CFR Part 29. Procedures for Handling Critical Infrastructure Information. Final Rule. *Federal Register* 72(170):52262-52277. Accessed 5.2008 at http://www.dhs.gov/xlibrary/assets/pcii_final_rule_federal_register9-1-06-2.pdf.

U.S. Department of Homeland Security (DHS). 2006. *National Infrastructure Protection Plan.* Accessed 10.2007 at http://www.dhs.gov/nipp/.

U.S. Department of Homeland Security (DHS). July 2006. *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)*. Accessed 2.2009 at www.dhs.gov/xlibrary/assets/.../privacy_pia_usvisit_ident_final.pdf.

U.S. Department of Homeland Security (DHS). January 5, 2005. Personnel Security and Suitability Program. DHS Management Directive Number 11050.2. Washington, DC. Accessed 11.2006 at http://www.uscg.mil/hq/cg9/NAIS/RFP/SectionJ/DHS-MD-11050-2.pdf.

U.S. Department of Homeland Security (DHS). 2002. *National Strategy for Homeland Security.* July. Accessed 10.2007 at http://www.whitehouse.gov/homeland/book/.

U.S. Department of Justice (DOJ) Bureau of Justice Statistics. 2007. Justice Statistics Improvement Programs. Accessed 3.2009 at http://ojp.usdoj.gov/bjs/jrip.htm#glossary.

U.S. Department of Justice (DOJ) Office of the Inspector General Audit Division. September 2007. Follow-up Audit of the Terrorist Screening Center. Audit Report 07-41. Redacted for Public Release. Accessed 3.2009 at www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.

U.S. Department of Justice (DOJ). June 2006. *The Attorney General's Report on Criminal History Background Checks.* Washington, DC: Office of the Attorney General. Accessed 10.2007 at http://www.justice.gov/olp/ag_bgchecks_report.pdf.

U.S. Department of Justice (DOJ). 2004. The Privacy Act of 1974: Overview of the Privacy Act of 1974, 2004 Edition. Accessed 2.2009 at http://www.usdoj.gov/opcl/1974privacyact-overview.htm.

U.S. Department of Justice (DOJ). November 2002. *A Method to Assess the Vulnerability of U.S. Chemical Facilities*. National Institute of Justice. Final Version. NCJ 195171. Accessed 1.2008 at http://www.ncjrs.gov/pdffiles1/nij/195171.pdf.

U.S. Department of Justice (DOJ). June 12, 1998. Letter Opinion for the Deputy Director of the Federal Bureau of Investigation: Access to Criminal History Records by Non-Governmental Entities Performing Authorized Criminal Justice Functions. Accessed 10.2007 at http://www.usdoj.gov/olc/chriltr004.htm.

U.S. Department of Labor (DOL). 2001. Drug Testing Reduces Workplace Injuries in Construction Industry. Accessed 12.23.07 at http://www.dol.gov/asp/programs/drugs/workingpartners/whatsnew/Archives/WhatsNew-1771.htm.

U.S. Department of State (DOS). 1982. *Patterns of International Terrorism 1981*. Oklahoma City: The National Memorial Institute for the Prevention of Terrorism. Accessed 4.2008 at http://www.terrorisminfo.mipt.org/pdf/1981PoGT.pdf.

U.S. Environmental Protection Agency (EPA). 2007. 2007 Water Sector-Specific Plan. Accessed 10.2007 at http://www.epa.gov/safewater/watersecurity/pubs/plan_security_watersectorspecificplan.pdf.

U.S. Federal Emergency Management Agency (FEMA). December 2003. FEMA 427 *Primer for Design of Commercial Buildings to Mitigate Terrorist Attack*. Pp 6-1 - 6-60.

U.S. Federal Energy Regulatory Commission (FERC). October 30, 2007. Critical Energy Infrastructure Information. *18 CFR Part 388*. Final Rule. Washington, DC.

U.S. General Accounting Office (GAO). September 2003. *Nuclear Regulatory Commission Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*. GAO-03-752. Washington, DC.

U.S. General Accounting Office (GAO). July 13, 1983. *Report to the Chairman, Nuclear Regulatory Commission: Additional Improvements Needed in Physical Security at Nuclear Power Plants.* GAO/RCED-83-141. Accessed 11.2007 at http://archive.gao.gov/f0302/121935.pdf.

U.S. Government Accountability Office (GAO). March 2007. *Securing Wastewater Facilities: Costs of Vulnerability Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely. Report to the Chairman, Committee on Environment and Public Works, U.S. Senate.* GAO-07-480. Washington, DC.

U.S. Government Accountability Office (GAO). October 2007. *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List.* GAO-08-110. Washington, DC.

U.S. Government Accountability Office (GAO). 2005. *Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism. Report to the Chairman, Committee on Government Reform, House of Representatives.* GAO-05-790. Washington, DC. Accessed 8.2008 at http://www.gao.gov/new.items/d05790.pdf.

U.S. Government Accountability Office (GAO). September 9, 2004. *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain.* Testimony Before the Committee on Commerce, Science, and Transportation, United States Senate. Statement of Margaret Wrightson, Director, Homeland Security and Justice Issues. Washington, DC: U.S. General Accounting

Office. GAO-03-1155T. Accessed 7.2007 at http://www.gao.gov/new.items/d031155t.pdf.

U.S. Government Accountability Office (GAO). 2004. *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*. Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives. Statement of Jim Wells, Director National Resources and Environment. GAO-04-1064T. Accessed 10.2007 at http://www.gao.gov/new.items/d041064t.pdf.

U.S. House of Representatives Subcommittee on National Security, Emerging Threats and International Relations of the Committee on Government Reform. September 14, 2004. *Hearing on Homeland Security: Monitoring Nuclear Power Plant Security.* Serial No. 108-265. Accessed 1.2008 at http://a257.g.akamaitech.net/7/257/2422/25feb20051230/www.access.gpo.gov/congress/house/pdf/108hrg/98358.pdf.

U.S. House of Representatives Energy and Commerce Committee, Committee on Oversight and Investigations. 1993. *The Trans-Alaska Pipeline*. 103rd Congress. Accessed 10.2007 at http://energycommerce.house.gov/comdem/comact03/oi103.htm#tap.

U.S. Nuclear Regulatory Commission (NRC). nd. *Strategic Plan: Fiscal Year 2000 – Fiscal Year 2005*. NUREG-1614, Vol 2, part 1. Washington, DC; Office of the Chief Financial Officer. Accessed 11.2007 at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/.

U.S. Nuclear Regulatory Commission (NRC). nd. Section 73.57 Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees. Available at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0057.html.

U.S. Nuclear Regulatory Commission (NRC). Publishing date uncertain. *Summary and Analysis of Public Comments Received on Proposed Revisions to 10 CFR Part 26 – Fitness for Duty Programs*. NUREG 1911. Washington, DC: Office of Nuclear Regulatory Research.

U.S. Nuclear Regulatory Commission (NRC). October 17, 2008. Update on the Development of the Construction Inspection Program for New Reactor Construction Under 10 CFR Part 52. From R.W. Borchardt. SECY-08-0155.

U.S. Nuclear Regulatory Commission (NRC). October 2008. Backgrounder: Nuclear Security. Accessed 10.2008 at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-enhancements.pdf.

U.S. Nuclear Regulatory Commission (NRC). April 2008. New Reactors: What We Regulate. Accessed 5.2008 at http://www.nrc.gov/reactors/new-reactor-licensing.html.

U.S. Nuclear Regulatory Commission (NRC). Revised April 11 2008. Fingerprinting Questions and Answers. Accessed 6.2008 at http://www.nrc.gov/security/byproduct/ea-07-305q&a.pdf.

U.S. Nuclear Regulatory Commission (NRC). March 31, 2008. *Fitness for Duty Final Rule*. *73 FR 16965*.

U.S. Nuclear Regulatory Commission (NRC). February 2008. *Strategic Plan: Fiscal Years 2008–2013*. *NUREG-1614, Vol. 4*. Washington, DC; Office of the Chief Financial Officer. Accessed 3.2008 at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/v4/index.html.

U.S. Nuclear Regulatory Commission (NRC). February 27, 2008. Fingerprinting Requirements for Increased Controls Licensees. Powerpoint presentation by Chris Einberg and Tim Harris. Accessed 7.2008 at http://www.nrc.gov/security/byproduct/fingerprinting-workshop-slides.pdf.

U.S. Nuclear Regulatory Commission (NRC). February 2008. Security Orders and Requirements. Accessed 6.2008 at http://www.nrc.gov/security/byproduct/orders.html.

U.S. Nuclear Regulatory Commission (NRC). January 2, 2008. Fact Sheet: Security Spotlight. Accessed 1.2008 at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-spotlight/new-reactor.html.

U.S. Nuclear Regulatory Commission (NRC). December 5.2007. Order Imposing Fingerprinting. (IC). EA-07-305. Accessed 5.2008 at http://www.nrc.gov/security/byproduct/ea-07-305-fingerprinting-order-for-ic-licensees.pdf.

U.S. Nuclear Regulatory Commission (NRC). November 30, 2007. SECY 07-0211. Policy Issue (Notation Vote). Access Authorization and Physical Protection Requirements for Nuclear Power Plant Construction. Washington, DC: U.S. Nuclear Regulatory Commission. OUO-Security Related Information.

U.S. Nuclear Regulatory Commission (NRC). September 12, 2007. Order Imposing Safeguards Information Protection Requirements and Fingerprinting and Criminal History Record Check Requirements for Access to Safeguards Information. Accessed 7.2008 at http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=072560149.

U.S. Nuclear Regulatory Commission (NRC). Updated July 2. 2007. Frequently Asked Questions About NRC's Design Basis Threat Final Rule. Accessed 5.2008 at http://www.nrc.gov/security/faq-dbtfr.html.

U.S. Nuclear Regulatory Commission (NRC). Updated July 2. 2007. Frequently Asked Questions About Security Assessments at Nuclear Power Plants. Accessed 5.2008 at http://www.nrc.gov/security/faq-security-assess-nuc-pwr-plants.html.

U.S. Nuclear Regulatory Commission (NRC). October 31, 2006a. Part IV. Nuclear Regulatory Commission 10 CFR Parts 2, 30, et al. Protection of Safeguards Information. Proposed Rule.

U.S. Nuclear Regulatory Commission (NRC). September 2006b. Backgrounder: Nuclear Security – Five Years After 9/11. Office of Public Affairs. Accessed 1.2008 at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-enhancements.pdf.

U.S. Nuclear Regulatory Commission (NRC). August 2006c. *The Radiation Source Protection and Security Task Force Report and Executive Summary*. Report to the President and the U.S. Congress under Public Law 109-58, *The Energy Policy Act of 2005*. Accessed 1.2008 at http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2006/president-08-15-2006.pdf. [Includes discussion of personnel security/background checks.] OUO.

U.S. Nuclear Regulatory Commission (NRC). May 2006d. *Regulatory Guide 1.201* (For Trial Use): Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance. Rev 1. Office of Nuclear Regulatory Research. Accessed 12.2007 at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-201/01-201r1.pdf.

U.S. Nuclear Regulatory Commission (NRC). May 31, 2006e. SECY 06-0126. Proposed Rulemaking-Power Reactor Security Requirements (RIN 3150-AG63). Accessed 1.2007 at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2006/secy2006-0126/2006-0126scy.html.

U.S. Nuclear Regulatory Commission (NRC). 2006df. Proposed Rule. 10 CFR Parts 50, 72, and 73. RIN 3150-AG63. Accessed 4.2008 at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2006/secy2006-0126/enclosure1.pdf.

U.S. Nuclear Regulatory Commission (NRC). December 22, 2005a. NRC Regulatory Issue Summary 2005-31 Control of Security-Related Sensitive Unclassified Non-Safeguards Information Handled by Individuals, Firms, and Entities Subject to NRC Regulation of the Use of Source, Byproduct, and Special Nuclear Material. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2005/ri200531.pdf#pagemode=bookmarks&page=6.

U.S. Nuclear Regulatory Commission (NRC). July 6, 2005b. SECY 05-0120. Policy Issue Notation Vote on Security Design Expectations for New Reactor Licensing Activities. Accessed 10.2007 at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2005/secy2005-0120/2005-0120scy.html.

U.S. Nuclear Regulatory Commission (NRC). August 2004a. *Strategic Plan: Fiscal Years 2004–2009*. NUREG-1614, Vol. 3. Washington, DC; Office of the Chief Financial Officer. Accessed 3.2008 at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/v3/index.html.

U.S. Nuclear Regulatory Commission (NRC). April 23, 2004b. SECY 04-0068 Policy Issue Information. Update of the Risk-Informed Regulation Implementation Plan. Accessed 5.2008 at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2004/secy2004-0068/2004-0068scy.html.

U.S. Nuclear Regulatory Commission (NRC). March 2004c. SECY 04-0068 Attachment 2 Risk-Informed Regulation Implementation Plan. Accessed 5.2008 at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2004/secy2004-0068/attachment2.pdf.

U.S. Nuclear Regulatory Commission (NRC). April 29, 2003a. EA-03-086. Order Requiring Compliance with Revised Design Basis Threat for Operating Power Reactors. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2003/ml030740002-dbt-04-29-03.pdf.

U.S. Nuclear Regulatory Commission (NRC). April 29, 2003b. EA-03-039. Order for Compensatory Measures Related to Training Enhancements on Tactical and Firearms Proficiency and Physical Fitness Applicable to Armed Nuclear Power Plant Security Force Personnel. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2003/ml030910625-training-04-29-03.pdf.

U.S. Nuclear Regulatory Commission (NRC). April 29, 2003c. EA-03-038. Order for Compensatory Measures Related to Fitness-for-Duty Enhancements Applicable to Nuclear Facility Security Force Personnel. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2003/ml030940198-ffd-04-29-03.pdf.

U.S. Nuclear Regulatory Commission (NRC). January 7, 2003d. EA-02-261. Order for Compensatory Measures Related to Access Authorization. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2003/security-order-01-07-03.pdf.

U.S. Nuclear Regulatory Commission. February 25, 2002. EA-02-026. Order for Interim Safeguards and Security Compensatory Measures. Accessed 10.2006 at http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2002/security-order-2-25-02.pdf.

U.S. Nuclear Regulatory Commission (NRC). July 2000. *Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission. Final Report.* NUREG/BR-0058 Rev. 3. Washington, DC: Office of Nuclear Regulatory Research.

U.S. Nuclear Regulatory Commission. February 11, 1998. NRC Information Notice 98-05: Criminal History Record Information. Accessed 10.2007 at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1998/in98005.html.

U.S. Nuclear Regulatory Commission (NRC). 1989. SECY-89-030. Final Rulemaking-Fitness-For-Duty Programs.

U.S. Nuclear Regulatory Commission (NRC). 1984. Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants (NUREG-1055). Washington, DC: Division of Quality Assurance, Safeguards, and Inspection Programs. Accessed 10.2007 at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1055/html.

U.S. Nuclear Regulatory Commission (NRC). August 20, 1982a. SECY-82-352. Assurance of Quality. [ML 8209160068]

U.S. Nuclear Regulatory Commission (NRC). August 18, 1982b. IE Bulletin No. 82-01, Rev 1, Supplement 1: Alteration of Radiographs of Welds in Piping Subassemblies. Accessed 12.2006 at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/1982/bl82001r1s1.html.

U.S. Nuclear Regulatory Commission (NRC). March 31, 1982c. IE Bulletin No. 82-01: Alteration of Radiographs of Welds in Piping Subassemblies. Accessed 12.2006 at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/1982/bl82001.html.

U.S. Nuclear Regulatory Commission (NRC). September 26, 1967. 10 CFR 50.13. Attacks and Destructive Acts by Enemies of the United States; and Defense Activities. *32 Federal Register 13445*. Washington, DC.

U.S. President. August 24, 2004. Homeland Security Presidential Directive/Hspd-12. Subject: Policy for a Common Identification Standard for Federal Employees and Contractors. Accessed 10.2007 at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

U.S. President. August 27, 2004. Homeland Security Presidential Directive/Hspd-11. Subject: Comprehensive Terrorist-Related Screening Procedures. Accessed 10.2007 at http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html.

U.S. President. December 17, 2003. Homeland Security Presidential Directive/Hspd-7. Subject: Critical Infrastructure Identification, Prioritization, and Protection. Accessed 1.2008 at http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

U.S. President. September 16, 2003. Homeland Security Presidential Directive/Hspd-6. Integration and Use of Screening Information. Accessed 1.2008 at http://www.whitehouse.gov/news/releases/2003/09/print/20030916-5.html.

U.S. President. February 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC. Accessed 1.2008 at http://www.whitehouse.gov/pcipb/physical_strategy.pdf.

U.S. President. May 1998. Presidential Decision Directive/NSC-63. Critical Infrastructure Protection. Accessed 1.2008 at http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf.

U.S. Senate. 109th Congress. July 1, 2005. Nuclear Security Act of 2005. Report 109-89.

Van Staveren, Martin. 2006. *Uncertainty and Ground Conditions: A Risk Management Approach*. Oxford, UK:Butterworth-Heinemann.

Vaught, J.W., Jr. 1991. The Emergence of the Nuclear Industry and Associated Crime. Report No. AFIT/CI/CIA/91-089. Wright-Patterson AFB, OH: Air Force Institute of Technology.

Visser, P.S., and P.E. Tetlock. 2007. People as Intuitive Prosecutors: The Impact of Social-Control Goals on Attributions of Responsibility. *Journal of Experimental Social Psychology* 43(2):195-209.

Von Hepel, Frank; .Brenner, David; Lyman, Edwin. 2002. Revisiting Nuclear Power Plant Safety. Letters to the Editor. *Science* 299:201-203.

Wald, Matthew L. 2004. Bill Allows Atomic Waste to Remain in Tanks. *The New York Times*. October 10, p. 37.

Ward D.A., M.C. Stafford, and L.N. Gray. 2006. Rational Choice, Deterrence, and Theoretical Integration. *Journal of Applied Social Psychology* 36 (3): 571-585.

Watts, David. 2003. Security and Vulnerability in Electric Power Systems. 35th North American Power Symposium. Rolla, MS: University of Missouri-Rolla. October 20-21. Pp. 559-566. Accessed 10.2007 at http://www2.ing.puc.cl/power/paperspdf/PaperECE723v39Format.pdf.

Weinhardt, Lance S., Michael P. Carely, Blair T. Johnson, and Nicole L. Bickham. 1999. Effects of HIV Counseling and Testing on Sexual Risk Behavior: A Meta-Analytic Review of Published Reaseach, 1985-1997. *American Journal of Public Health* 89(9):1397-1405.

West, S., and R. Wichlund. 1980. *A Primer of Social Psychological Theories*. Monterey, CA: Brooks/Cole Publishing Company.

WestCoast. 2004. Largest Construction Project in Finland. Accessed 2.2008 at http://www.rauma.chamber.fi/linkkitiedosto.asp?taso=0&id=64.

Whitehead, D. W., C.S. Potter, and S.L. O'Connor. September 2007. *Nuclear Power Plant Security Assessment Technical Manual*. Prepared by Sandia National Laboratory for the U.S. Nuclear Regulatory Commission. A revision of NUREG/CR-13.

Willamette Week. 1981. The Washington Public Power Supply System is Plagued by Billion-Dollar Overruns, Construction Boondoggles, Doctored-Quality Control Reports, and Drug Use by Engineers and Craftsmen. Accessed 12.2006 at http://wweek.com/___ALL_OLD_HTML/25-1981.html.

Wilson, Clay. January 29, 2008 (update). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service. Report for Congress. Washington, DC: The Library of Congress. Accessed 1.2008 at http://www.fas.org/sgp/crs/terror/RL32114.pdf.

Wilson, Robert, Nora Thompson, Nicholas Ciccarello, Lindsey Whitmer, and James Hitt. April 2005. Insider Threat Deterrence and Detection Methods, Techniques, and Criteria: A Summary of Best Practices. Prepared by Survivability/Vulnerability Information Analysis Center SURVIAC Program Office for the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.

Winslow, Ron. November 7, 1984. Quality Quandary: Regulators Investigate Harassing of Inspectors at New Nuclear Plants. *Wall Street Journal.*

World Nuclear Association. August 2009. Nuclear Power in the USA. Accessed 8.2009 at http://www.world-nuclear.org/info/inf41.html.

Zhuang, Jun, and Vicki M. Bier. 2007. Balancing Terrorism and Natural Disasters – Defense Strategy with Endogenous Attacker Effort. *Operations Research* 55(5):976-991.

Appendix A: Expert Consultations and Workshop Participants

A.1 Individuals Consulted by the Project Team and TISP Workshop Participants

The following individuals were interviewed during Phase I of this project or following the TISP workshop: The interview guide used to structure these interviews is presented in Appendix A.2.

Individual	Organization	Expertise	Sector
Experts focused primarily on credible threat determination			
Clardy, Mitchell	PNNL	Security and physical protection	Govt. nuclear facilities
Cross, Sherri	PNNL	NRC permitting, threat analysis	Govt. nuclear and NPP
Garrett, Albert	PNNL	Safeguards and Security, NRC permitting	Govt. nuclear facilities, NPPs
Gority, Scott	PNNL	Physical security, threat scenario	Govt. nuclear facilities, CI
MacDonald, Douglas	PNNL	Physical security	Govt. nuclear facilities, NPPs
Pope, John	PNNL	Physical security and counter terrorism	Govt. nuclear facilities, NPPs
Garcia, Michael	DHS	Rapid vulnerability assessment, security and preparedness coordination with law enforcement	NPPs and other CI, Dams
Experienced experts on construction, construction security, and security planning			
Anderson, Todd	Catalyst Consulting, Security Consultant	Physical security system designs and installation	Banks and casinos
Behm, Michael	E. Carolina University Department of Technology Systems	Construction design for safety and sustainability	Academe
Bergtold, Greg (brief interview)	Dow Chemical Company, Director of Codes and Standards	Green buildings and sustainability	Chemical
Blancato, Louis	Dominion, LNG facility	Security Manager, former	Liquefied Natural

Individual	Organization	Expertise	Sector
		law enforcement	Gas and
Bray, Matt	Terminal 5, Heathrow Airport, Head of Security	Security planning and management	Transportation (airport)
Endicott-Popovsky, Barbara	University of Washington, Director Center for Information Assurance and Cybersecurity	Cyber Security, especially SCADA	Cyber security for power plants and dams
Fitch, Jeff Miller, Deborah	Port of Seattle, Seattle-Tacoma Airport	CI security, personnel security	Transportation (airport)
Goodson, Bruce	Rushforth-Taylor Construction	Construction Project Manager	Urban municipal and commercial facilities
Grohs, Douglas	Kiewit Construction, Senior Program Manager	Project manager, site security	Transportation (roads, bridges, railways)
Holbrook, Joanne	Avitar Technologies, Inc.	Drug testing equipment, personnel security	Security
Kent, Scott	RFI Communications and Security Systems, Account Manager	Security system integration	Casinos and larger pharmaceutical companies
Kettler, Ken	Tulalip Tribe, Mortenson Construction, Project Manager	Project manager and integrator for casino and hotel construction	Casino
Kotkiewicz, Leonard	U. S Corps of Engineers; The Infrastructure Security Partnership (TISP)	Chief, Civil Emergency Management	Emergency Management and Operations Critical Infrastructure
Konigsmark, Ken	Boeing Commercial Aviation, Supply Chain Security	Security planning and implementation	Manufacturing
Lance, Darby	Hemlock Semiconductor Corporation	Contractor Construction Safety and Security	Chemical
Leingang, L.A.	Bechtel National, Inc; Site Security Manager, DOE Hanford Waste Treatment Plant	Site security planning and management	Govt nuclear materials facilities

Individual	Organization	Expertise	Sector
	(Vitrification Plant)		
Leeper, Paul	Pantex, currently, previously at NPPs and refineries	Security Manager	Govt. nuclear facilities, NPPs, refineries
Lucci, Tony	U. S. Bank	Facility construction manager	Banks and Data Centers
Madden, Michael	Los Alamos National Laboratory, Director of Security Systems	Vulnerability assessment, physical protection, security systems	Govt. nuclear facilities
Magnusson, Jon	Magnuson Klemencic Associates, Inc, CEO	Large-scale commercial high-rise construction	Urban high-rise, international
Magouirk, Justin	Executive Director, Global Transnational Terrorism Project	Political Scientist	Terrorism
Mason, Dominic	William H. Gordon Associates, Inc.	Sr. Security Consultant, Crime prevention through environmental design	Security systems and standards
Nettleship, Suzan	Nettleship Associates, Principal	Construction management and quality assurance	Urban high rise
O'Leary, Gerald	Retired	Off-Shore Oil Development and Management	Energy (Oil and Gas Exploration and Development)
Peart, Wilber and Bets, Kurt	William H. Gordon Associates, Inc.	Security Consultants	Site construction security
Southworth, Robert J., Jr.	Urenco	National Enrichment Facility	Nuclear Industry
Stoltz, John	Jacob's Associates	A&E Program Manager	Transportation (bridge and tunnel construction)
Toomey, Christopher	PNNL	Civil engineering, reconstruction, critical infrastructure protection	Military installations; municipal infrastructure
Wadkins, Lance	Port of Tacoma, Port	Security Manager	Transportation (port)
Watson,	Oak Ridge National Laboratory	Security Manager, Spallation Neutron Source	High Energy Research

Individual	Organization	Expertise	Sector
Participants in The Infrastructure Security Partnership (TISP) Workshop			
Andrews, Marion	Defense Threat Reduction Agency (DTRA)	Threat and Vulnerability Assessments	Government facilities, including military
Brown, Ira	DTRA	Threat and Vulnerability Assessments	Infrastructure security
Bucklew, Thomas	DTRA	Threat and Vulnerability Assessments	Infrastructure security
Captain, Richard	Bechtel	Project Integration and Management	Large-Scale Construction
Dalton, Marla	TISP, Executive Director (Host)	American Society of Civil Engineers; Director, Critical Infrastructure	U.S. critical Infrastructure
Ferrera, Roland	AMEC	Construction security	Construction
Fowler, Perry	TISP, (HOST)	Associated General Contractors, Construction Management	Construction
Galloway, Gerald	University of Maryland	Professor, Civil and Environmental Engineering	Academia/ Civil Engineering and Construction
Garcia, Michael	U.S. Department of Homeland Security (DHS)	Facility Security, Vulnerability and Threat Assessment	Energy and Critical Infrastructure
Graves, Richard	Bechtel, Sr. Executive Power Services	Project Integration and Management	NPP
Heckler, Edward	U.S. Army Corps of Engineers	Construction Planning and Management	Engineering and Construction
Homes, Diane	Fluor	Construction Security	Government Facilities, Nuclear Materials
Hughes, Niav	U.S. NRC	Human Factors	NPPs
Indahl, Berne	Formerly at Boeing and U.S. Department of State	Construction Security for U.S. Embassies; Supply Chain Security	Government Facilities; Aircraft
Jordan, Roger	American Council of Engineering Companies (ACEC)		

Individual	Organization	Expertise	Sector
Konigsmark, Ken	Boeing, Head of Supply Chain Security	Supply Chain Security	Aircraft, Manufacturing
Morris, Scott	U.S. NRC,	Division of Security Policy, Access Authorization and Security Planning	NPP
Nerret, Amanda	U.S. NRC	Human Factors	NPP
Persensky, Julius	U.S. NRC	Human Factors	NPP
Raddel, Christopher	Parsons	Facility Security	Government
Rhodes, Vernon	Defense Information Systems Agency	Anti-Terrorism Officer	Secure government facilities
Skibniewski, Miroslaw	University of Maryland	Professor of Construction Engineering	Construction
Skymes, Kevin	KBR, Inc	Construction Management and Security	NPP
Warren, Roberta	U.S. NRC,	Division of Security Operations, Threat Assessment	NPP
Wright, Darian	Hemlock Semiconductor Corporation	Chemical Processing Facility Construction	Chemical
Invited Participants in the TISP Workshop, but unable to attend			
Barnes, Valerie	U.S. NRC	Human Factors	NPP
Beard, William Dexter	U.S. Department of Energy (DOE)	Y-12 Construction Security	Government Nuclear Facilities
Burrell, Michael	U.S. NRC	Access Authorization	NPP
Fisicaro, James	Nuclear Energy Institute (NEI)		NPP
Oscar, Kenneth	Fluor, VP for Strategy		Nuclear Facilities
Way, Ralph	U.S. NRC	Nuclear Security and Incident Response, Counterterrorism	NPP

A.2 Construction Security Discussion Guide
Post-9/11 Threat Considerations and Security Needs/Strategies

This work is being done for the United States' Nuclear Regulatory Commission (NRC) to help determine what security-relevant measures should be practiced during new nuclear power plant construction. As part of this work, the NRC is interested in understanding how these issues are being addressed in other private and public sector construction projects, especially those involving critical infrastructure (e.g., power plants, seaports, bridges, airports, high-rise buildings, etc).

1. Your construction security background and expertise:

a. Please describe your experience with the construction of critical infrastructure facilities and the identification and assessment of threats that might be introduced during the construction phase.

Type of facility	Location	Type of site: 1=green-field 2=contained within the perimeter of an existing access-restricted site	Time period	Your job responsibilities	Involvement in identifying or assessing threats during construction

b. Are you aware of, or have you been involved in or responsible for efforts to identify, validate, and/or evaluate the potential for 'delayed impact threats' during construction (for example, sabotage to place an explosive that could be detonated at a later time or to build system failures into critical components; malfeasance; or carelessness that could impact the safe and secure operation of critical infrastructure facilities once they are operational/in use)? _____ Please explain.

c. Do these efforts typically include experts in: [Yes/No]
_____ Physical security
_____ Cybersecurity
_____ Counterintelligence

2. Threats and Targets — Changes post 9/11:

a. Given current circumstances, do you think the U.S. and owners of critical infrastructure facilities need to be concerned about security **during the construction phase**?
_____ Please explain.

b. Do you think enough attention is given to the identification of security threats and security needs during the construction phase of critical infrastructure facilities?
_____ Please explain.

c. In your experience, what are the four highest priority threats during critical infrastructure construction that security programs are attempting to prevent?
1. _____
2. _____
3. _____
4. _____

d. Some possible 'delayed impact threats' to critical infrastructure construction projects are noted below. Can you identify others? To what extent does each constitutes a credible threat? For those you think are threats worthy of concern, where and when during the construction process could they be introduced?

What types of delayed impact threats could be introduced during construction? [Please add any others]	In your opinion to what extent is this threat a credible concern? 4=relatively high concern; 3=relatively moderate concern; 2=relatively low concern; 1=not a credible concern		For those ranked 3 or 4 – **Where** could this threat be introduced/occur? 1=campus grounds, 2=structural concrete, 3=enclosed structures, 4=software systems, 5=enclosed components such as HVAC, 6=electrical system, 7=water/sewage system, 8=other_____	For those ranked 3 or 4 – **When** (during what phase of construction) could this threat be introduced? During: 1=site preparation, 2=foundation work, 3=framing, 4=rough-ins, 5=finishing, 6=system installation, 7=other_____
	Critical infrastructure overall	Nuclear power plants		
1. Hidden explosives that could be remotely detonated at a later time				
2. Hidden surveillance devices				
3. Critical components of systems compromised somewhere in the supply chain				
4. Other_____				
5. Other_____				
6. Other_____				
7. Other_____				
8. Other_____				
9. Other_____				

e. How would you rate the risk from 'delayed impact threats' introduced during construction for the following types of facilities?
(4= relatively high risk; 3= relatively medium risk; 2=relatively low risk; 1=not a credible concern)

_____Nuclear power plants

_____Chemical plants

_____Key public sector high rise buildings

_____Key private sector high rise buildings

_____Major bridge construction

_____Construction at major airports

_____Construction at key seaports

_____Other_____

_____Other_____

f. If you rated nuclear power plants at relatively low risk, why is this?

g. If you rated nuclear power plants at relatively high or medium risk, who might target nuclear power plants during construction and why?

3. Protection strategies and their effectiveness

a. Are security, safety, and quality measures for construction projects fairly standardized in the U.S. for similar types of facilities? _____Please explain.

b. Are security requirements during the construction phase typically specified in a pre-construction security plan? _____ Please explain.

c. Is compliance with these standards uniformly high across companies and industries?_____ Please explain.

d. Have security practices during construction changed much post 9/11?_____ Please explain.

e. In your opinion, are current, typical construction security, safety, and quality standards sufficient to prevent ‘delayed impact threats’? _____ Please explain.

f. Do facility specifics (for example, facility type, location, greenfield/shared site, etc.) affect the **types** of measures needed to prevent/counter security threats during construction? _____ Please explain.

g. Do facility specifics (for example, facility type, location, greenfield/shared site, etc.) affect the **way** security measures need to be **operationalized**? _____ Please explain.

h. In your opinion how important are the following types of security-relevant measures in addressing 'delayed impact threats' (please keep construction of nuclear power plants in mind)? For those you consider important, please describe 'best practice' and how common practice differs from 'best practice.'

General Measures	Importance as a construction security measure 4= very important 3= fairly important 2= not very important 1= detrimental/ counterproductive	For those ranked 3 or 4 – In your opinion what would be considered 'best practice' in this area?	For those ranked 3 or 4 – Does common practice in this area differ from this 'best practice' and warrant enhancement?
Life-cycle approach to security design/planning, including threat and vulnerability assessment during construction phase			
Preconstruction security plan			
Security-relevant contract specifications			
Security-relevant liability agreements			
Security oversight of suppliers of key components/ systems			
Security awareness and education			
Security-informed quality assurance programs			
Management support and involvement			
Good labor relations			
Decisive enforcement agreements and actions			

i. In your opinion how important are the following specific types of security measures in preventing 'delayed impact threats' during construction (please keep construction of nuclear power plants in mind)?

Types of Measures	Importance as a construction security measure 4= very important 3= fairly important 2= not very important 1= detrimental/ counterproductive	For those measures rated 3 or 4 in effectiveness		
		What would you consider to be 'best practice' in this area?	Does common practice differ from 'best practice?' [Yes/No]	Is enhancement warranted? [Yes/No]
Physical Access Controls				
Badging/prox cards				
Perimeter access/exit control (gates, locks, guards, sensors, etc)				
Interior access control (locks, biometrics, etc)				
Intrusion detection and alarms				
Security seals or other container intrusion detection devices				
Other_____				
Administrative Access Controls				
Employment criteria (e.g., US Citizenship;)				
Identify verification requirements (documents; fingerprints; biometrics)				
Background screening (fingerprints, criminal checks)				
Access authorizations/badges				
Escort program				
Rules/restrictions on what can be brought in/out				
Documentation/chain-of-custody requirements				
Security seals and/or tamper-indicating devices				
Quality control and work rules that focus on enhancing security				
Other_____				

Types of Measures	Importance as a construction security measure 4= very important 3= fairly important 2= not very important 1= detrimental/ counterproductive	For those measures rated 3 or 4 in effectiveness		
		What would you consider to be 'best practice' in this area?	Does common practice differ from 'best practice?' [Yes/No]	Is enhancement warranted? [Yes/No]
Monitoring/Inspection/ Testing				
QA monitoring				
Drug testing (pre-employment, for-cause, post-incident, random)				
Behavioral observation/monitoring program				
Materials/ Component inspection/testing, including sampling and non-destructive evaluation (NDE)				
Vendor background/site checks				
Pre-delivery vendor and component oversight/observation				
Built-in system controls/detectors				
Roving patrols				
Searches/trace analyzers/dogs – (entry/exit; random)				
Additional supervision/ construction oversight				
Red Team security oversight				
Other_____				
Other Measures				
Other_____				
Other_____				

j. In your view does having drug users or heavy drinkers on a construction site pose a potential security risk (please keep construction of nuclear power plants in mind)?_____ Why or why not?

Does this risk go beyond theft? _____ Please explain.

k. In your experience, what kind of drug and/or alcohol testing **is** commonly practiced during the construction of critical infrastructure? What do you think **should be** practiced in the construction of critical infrastructure, such as nuclear power plants?

Personnel Categories	Random testing		Pre-employment testing		Post-incident testing		For-cause testing	
	Is this commonly practiced for this category of worker? [Yes/No]	Should it be practiced for this category of worker? [Yes/No]	Is this commonly practiced for this category of worker? [Yes/No]	Should it be practiced for this category of worker? [Yes/No]	Is this commonly practiced for this category of worker? [Yes/No]	Should it be practiced for this category of worker? [Yes/No]	Is this commonly practiced for this category of worker? [Yes/No]	Should it be practiced for this category of worker? [Yes/No]
First line supervisors								
Key QA personnel								
Security personnel								
All construction workers with access to critical areas								
Everyone on the site								

l. In your experience, what kind of behavioral observation training and behavioral observation measures **are** commonly practiced during the construction of critical infrastructure? Do you think behavioral observation training and observation measures **should be** practiced during the construction of critical infrastructure?

Personnel Categories	Is behavioral observation training commonly provided to this category of worker? [Yes/No]	Should behavioral observation training be provided to this category of worker? [Yes/No]	Are behavioral observation measures practiced for this category of worker? [Yes/No]	Should behavioral observation measures be practiced for this category of worker? [Yes/No]
First line supervisors				
Security personnel				
Workers				

m. In your experience, what kinds of access controls **are** commonly implemented during the construction of critical infrastructure? What access controls do you think **should be** implemented in the construction of critical infrastructure, such as nuclear power plants?

Personnel Categories	Pre-access identification verification		Pre-access local criminal investigation		Pre-access fingerprinting and national criminal investigation		Badge access controls within site perimeter—i.e., additional access controls to key areas of construction site	
	Is it practiced? [Yes/No]	Should it be practiced? [Yes/No]	Is it practiced? [Yes/No]	Should it be practiced? [Yes/No]	Is it practiced? [Yes/No]	Should it be practiced? [Yes/No]	Is it practiced? [Yes/No]	Should it be practiced? [Yes/No]
First line supervisors								
Key QA personnel								
Security guards								
All construction workers with access to critical areas								
Everyone on the site								

n. Do you think that a strong behavioral observation program offsets the need for: [Yes/No]

_____ Rigorous background checks?

_____ Random drug testing?

_____ Access controls and escort requirements within the perimeter of the construction site?

Please explain why or why not.

6. Benefits and Costs of an Effective Program to Address Construction Security Threats

a. Please identify what you consider the key components of an effective security program for the construction-phase of critical infrastructure facilities and then indicate what you think is the relationship between the costs and benefits of such a program. Do you think such a program would be cost prohibitive?

What do you consider the key components of an effective security program for the construction-phase of critical infrastructure facilities (please keep construction of nuclear power plants in mind)?	What do you think is the relationship between the costs and benefits of implementing such a construction-phase security program for critical infrastructure facilities? 4=benefits outweigh costs by a large margin 3=benefits outweigh costs by a small margin 2=costs outweigh benefits by a small margin 1=costs outweigh benefits by a large margin	In your view, would implementing such an effective security program during the construction-phase of critical infrastructure facilities be cost prohibitive? Please explain. Yes=cost prohibitive No=not cost prohibitive
1. 2. 3. 4. 5.		

7. Lessons Learned / Best Practices:

a. Are there any relevant lessons you have learned from your experience that might be applicable to those constructing nuclear power plants? _____ Please explain.

b. Would it be useful to have a set of guidelines for security during the construction of critical infrastructure? _____ Please explain. If yes, who do you think should be involved in developing the guidelines?

c. In your opinion is it effective and efficient to develop a security plan prior to construction?_____ Why or why not?

d. Would you be interested in being part of a community of practice that addresses these issues? _____ Please explain.

e. Can you recommend others knowledgeable about construction security and/or threat assessment that we should talk with?

Appendix B. Initiatives by U.S. Governmental Agencies and Private Sector Entities to Enhance Safety and Security of Critical Infrastructure

B.1 Introduction

Since 2001, the entire security context of the United States has changed. A broad array of directives, regulations, and programs focused on improving security of the critical infrastructure and preventing terrorists from introducing, acquiring, or deploying weapons of mass effect have been undertaken. Many of these initiatives have impacted individual workers and citizens by requiring the establishment of true identity, review of criminal history, and submission to screenings and searches. Requirements for workers to establish true identity and demonstrate good character, trustworthiness, and reliability as a condition of employment have extended into many businesses and sectors. The U.S. Nuclear Regulatory Commission (NRC) has issued a number of Orders implementing enhanced security measures, including requirements for fingerprinting and criminal history checks for an expanded list of personnel at operating facilities.[58]

With the increased emphasis on security and greater appreciation of the need to protect against terrorist attacks within the continental United States following 9/11, security experts and the public are now discussing whether a life-cycle approach should be applied to security. Such an approach would attempt to fully identify and address security and security/safety interface issues throughout the life cycle of a NPP and as early in the life cycle as possible. The NRC and the nuclear industry have embraced the need to reexamine nuclear power plant (NPP) security for operating NPPs, but there is somewhat less consensus about adopting a life-cycle approach to security for critical infrastructure (CI). Advocates argue that doing this could:

- Decrease plant vulnerabilities;
- Decrease conflicts and promote synergies in achieving security and safety objectives; and
- Promote cost effectiveness by increasing the effectiveness and efficiency of providing security throughout the life cycle of the plant.

Several of the major federal agency initiatives undertaken to enhance homeland security have focused on developing and implementing requirements, technologies, and processes to establish the true identity of individuals and to maintain confidence in that identity through the provision of badges or cards that contain or are keyed to this information. A consistent theme in the enhanced security procedures and requirements being developed post 9/11 is to increase assurance that individuals with unescorted access to secure areas of critical infrastructure or to information systems are not terrorists or linked to terrorists. Many of these efforts have been focused on federal employees and contractors, but others, such as the Customs and Trade Partnership

[58] These orders include: (1) EA-02-026 Interim Safeguards and Security Compensatory Measures (February 25, 2002); (2) EA-02-261 Compensatory Measures Related to Access Authorization (January 7,2003); (3) EA-03-038 Compensatory Measures related to Fitness-for-Duty Enhancements Applicable to Nuclear Facility Security Force Personnel (April 29, 2003; (4) EA-03-039 Compensatory Measures related to Training Enhancements on Tactical and Firearms Proficiency and Physical Fitness Applicable to Armed Nuclear Power Plant Security Force Personnel (April 29, 2003); (5) EA-03-086 Requiring Compliance with Revised Design Basis Threat for Operating Power Reactors (April 29, 2003).

Against Terrorism (C-TPAT), the Maritime Transportation Security Act (MTSA), and the Chemical Facility Anti-Terrorism Standards (SFATS) address both public and private sector personnel. For example, the Energy Policy Act of 2005 expanded requirements for fingerprinting and extended the definition of facilities for which sabotage penalties apply to include (among other things) those under construction. These initiatives illustrate the changing context in which NPP construction will take place and the types of security measures being applied in other sectors. Therefore, a brief description of some of the key initiatives and requirements are summarized below.

B.2 Summary of Key Initiatives by Sector

Presidential Directives and the Department of Homeland Security

Presidential Decision Directive/NSC-63 (1998) (available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm) identified the vulnerability of the nation's critical infrastructure. It identified as critical infrastructure those physical and cyber-based systems essential to the minimum operations of the economy and government including, but not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private. This Directive set out a goal of achieving and maintaining the ability "to protect the nation's critical infrastructures from intentional acts that would significantly diminish" (a) the abilities of the federal government to perform essential national security missions and to ensure the general public health and safety; (b) the abilities of state and local governments to "maintain order and to deliver minimum essential public services;" and (c) the abilities of the private sector to "ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services." The Directive asserts that: "Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States." The Directive established a public-private partnership to reduce vulnerability and to develop a National Infrastructure Assurance Plan. The U.S. Department of Energy (DOE) was designated as the lead agency for sector liaison with the electric power sector. This directive authorized the Federal Bureau of Investigation (FBI) to expand its organization to include a full scale National Infrastructure Protection Center.

Homeland Security Presidential Directive 6 (HSPD 6) (available at: http://www.fas.org/irp/offdocs/nspd/hspd-6.html), issued in September 2003, states the policy concerning integration and use of screening information and directs the Attorney General to establish an organization to "consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes." (This became the FBI-administered Terrorist Screening Center, which houses the terrorist screening center database.) HSPD 6 directs the heads of executive departments and agencies, to the extent permitted by law, to provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. Further, it directs the heads of executive departments and agencies to conduct screening using such information at all appropriate opportunities. The stated purpose of the Directive is to "[F]urther strengthen the ability of the United States Government to protect the people,

property, and territory of the United States against acts of terrorism, and to the full extent permitted by law…."

Homeland Security Presidential Directive 7 (HSPD 7) (available at: http://www.fas.org/irp/offdocs/nspd/hspd-7.html), issued in late 2003, states that it is U.S. policy to "enhance the protection of our Nation's CI and key resources against terrorist acts that could:

(a) Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
(b) Impair Federal departments' and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
(c) Undermine State and local government capacities to maintain order and to deliver minimum essential public services;
(d) Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
(e) Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
(f) Undermine the public's morale and confidence in our national economic and political institutions."

Homeland Security Presidential Directive 12 (HSPD 12) (available at: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html), issued in 2004, reflects the determination to enhance the protection of U.S. CI. HSPD 12 "mandates the development and implementation of a government-wide standard for a secure and reliable new identification card (PIV – Personal Identity Verification Card) issued to Federal employees and contractors who access federal facilities and information systems. The overall goal of HSPD-12 is to "achieve appropriate security assurance by verifying the identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems."

The rationale for this directive was that "[W]ide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."

HSPD 12 directs the Secretary of Commerce to promulgate a federal standard for secure and reliable forms of identification that:

- Is issued based on sound criteria for verifying an individual employee's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically;
- Is issued only by providers whose reliability has been established by an official accreditation process; and
- Includes graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

The directive does not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

The National Institute of Standards and Technology (NIST) was assigned responsibility for evaluating and specifying the biometric data standards for the personal identity verification (PIV) process (NIST 2007). Although this considered multiple biometric measures, fingerprints (complete image and a mathematical representations called minutia) and facial recognition received the greatest attention. A key consideration and goal of this effort is to enhance interoperability, which has historically been a significant barrier to the effective utilization of these tools. NIST Special Publication (NIST SP) 800-76-1, which documents the biometric data specifications, (NIST SP) 800-78, which specifies cryptographic algorithms and key sizes for the PIV, and Federal Information Processing Standards (FIPS) Publication 201, which sets out the U.S. federal government standard PIV requirements for federal employees and contractors, establish the technical requirements of HSPD 12. The "smart-card" to be used to demonstrate identity verification is expected to include two fingerprints, a personal identification number the cardholder would know, an identifying number unique to each card, and a digital signature. Office of Management and Budget (OMB) Memorandum 05-24 indicates that construction contractors (e.g., brick layers, plumbers, welders, etc.) must be put through the FIPs-201 badging process and have PIV/smart card badges if they will be accessing government facilities and/or information technology systems on a regular basis for a period in excess of 6 months. (See HSPD-12 FAQs at http://www.idmanagement.gov/content/hspd12_faqs_policy.htm.) In order to obtain a PIV card, an individual must complete Form I-9 (Employment Eligibility Verification) and provide for employer inspection documentation that establishes the individual's identity and employment eligibility. Form I-9 was first required by the Immigration Reform and Control Act of 1986. All employers are required to verify employment eligibility for every employee hired, and to retain the I-9 form for at least three years or for one year after employment of the individual ends, whichever is longer. Employers are responsible for re-verifying work authorization documents if the documents used in the verification expire.

The REAL ID Act of 2005, contained in Public Law 109-13 (available at http://www.ncsl.org/standcomm/sctran/REAL_ID_Act_of_2005.htm or http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109.pdf), was signed into law on May 11, 2005. In January 2008, the Department of Homeland Security issued the Final Rule that established minimum standards for state-issued driver's licenses and identification cards. According to the DHS, REAL ID is "a nationwide effort to improve the integrity and security of state-issued driver's licenses and identification cards, which in turn will help fight terrorism and reduce fraud." (Accessed 5.2008 at http://www.dhs.gov/xprevprot/programs/gc_1172767635686.shtm.) One of the key bases for REAL ID was that state-issued driver's licenses are the primary identifier for individuals attempting to access federal facilities, board federally-regulated commercial aircraft, and enter nuclear power plants, and that terrorists know this and actively seek this type of identification.

These regulations set standards for states to meet the requirements of the REAL ID Act, including:

- Information and security features that must be incorporated into each card;
- Proof of identity and U.S. citizenship or legal status of an applicant;
- Verification of the source documents provided by an applicant; and
- Security standards for the offices that issue licenses and identification cards.

States may seek an extension of the compliance deadline to May 11, 2011. The result of this requirement is that state-issued driver's licenses will reflect verification of the individual's true identity, immigration status, and residential location, and will be machine readable and incorporate security protections. A number of implementation issues have been identified, including protection of individual privacy.

The Immigration Reform and Control Act (IRCA) of 1986 (Public Law 99-603, 100 Statute 3359, available at https://www.oig.lsc.gov/legis/irca86.htm), was passed by Congress and signed by President Reagan in November 1986. It made it illegal to knowingly hire or recruit illegal immigrants and required employers to attest to their employees' immigration status. It also granted amnesty to certain illegal immigrants and a path toward legal status for certain agricultural seasonal workers. In addition, it introduced the I-9 Form, also known as the Employment Eligibility Verification Form, which every employee hired in the U.S. after November 6, 1986 must complete. The I-9 Form requires employees to present documents to the employers that verify their identity and legal authorization to accept employment in the U.S. The IRCA is now implemented by the United States Citizenship and Immigration Services (USCIS), which became a bureau of the DHS in 2003 and performs functions formerly the responsibility of the U.S. Immigration and Naturalization Service (INS) of the Department of Justice.

Energy Sector

A number of Federal agencies have ownership or regulatory roles in the energy sector, including the U.S. Department of Energy (DOE), the U. S. Nuclear Regulatory Commission (NRC), the U.S. Department of the Interior (DOI), and the U.S. Environmental Protection Agency (EPA). The Energy Policy Act of 2005 included directions for each of these agencies.

The Energy Policy Act of 2005 (EPAct of 2005), Subtitle D Nuclear Security (PL 109-58, available at: http://www.epa.gov/oust/fedlaws/publ_109-058.pdf) in **Section 651, Nuclear Facility and Materials Securit**y, amended Chapter 14 of the Atomic Energy Act of 1954 by adding requirements for security evaluations (Section 170D) and design basis threat rulemaking (Section 170E) for nuclear facilities. **Section 652, Fingerprinting and Criminal History Record Checks**, amended section 149 of the Atomic Energy Act of 1954 by requiring each individual or entity that is "licensed or certified to engage in an activity subject to regulation by the Commission, to have filed an application for a license or certificate to engage in an activity subject to regulation by the Commission, or to have notified the Commission in writing of an intent to file an application for licensing, certification, permitting, or approval of a product or activity subject to regulation by the Commission" to require fingerprinting of any individual who is permitted unescorted access to (a) a utilization facility; or (b) "radioactive material or other property subject to regulation by the Commission that the Commission determines

to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks;" or is (c) "permitted access to safeguards information under section 147." This section also states that the Commission "may require a person or individual to conduct fingerprinting under subsection a.(1) by authorizing or requiring the use of any alternative biometric method for identification that has been approved by the Attorney General and the Commission, by regulation."

In **Section 655. Sabotage of Nuclear Facilities, Fuel, or Designated Material**, the EPAct of 2005 amended section 236a of the Atomic Energy Act of 1954 by inserting "any production, utilization, waste storage, waste treatment, waste disposal, uranium enrichment, uranium conversion, or nuclear fuel fabrication facility subject to licensing or certification under this Act during construction of the facility, if the destruction or damage caused or attempted to be caused could adversely affect public health and safety during the operation of the facility" in the delineation of the subject facilities. It also replaced the term "intentionally and willfully" with "knowingly" in each place it appears in this section. [Title 42, Chapter 23, Division A, Subchapter XVII, Section 2284]. **Section 670E. Design Basis Threat Rulemaking,** directs the NRC to initiate a rulemaking to revise the design basis threat (DBT) and to take into consideration the following twelve factors:

1. The events of September 11, 2001;
2. An assessment of physical, cyber, biochemical, and other terrorist threats;
3. The potential for attack on facilities by multiple coordinated teams of a large number of individuals;
4. The potential for assistance in an attack from several persons employed at the facility;
5. The potential for suicide attacks;
6. The potential for water-based and air-based threats;
7. The potential use of explosive devices of considerable size and other modern weaponry;
8. The potential for attacks by persons with a sophisticated knowledge of facility operations;
9. The potential for fires, especially fires of long duration;
10. The potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals;
11. The adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility; and
12. The potential for theft and diversion of nuclear materials from such facilities.

The Federal Energy Regulatory Commission (FERC), an independent agency that regulates the interstate transmission of electricity, natural gas, and oil, has implemented rulemakings to increase security of the U.S. electrical system. FERC is responsible for reviewing proposals for the construction of liquefied natural gas (LNG) terminals and interstate natural gas pipelines and for licensing hydropower projects. The EPAct of

2005 expanded FERC's regulatory responsibilities. However, FERC does not have jurisdiction over the approval of the physical construction of electric generation, transmission, or distribution facilities or the regulation of nuclear power plants.

Reflecting the increased concern for security of critical infrastructure following September 11, 2001, Public Law 02-1-000 "Treatment of Previously Public Documents" issued on October 11, 2001, restricted access to documents that had previously been made available to the public. FERC subsequently promulgated a number of rulemakings concerning **critical energy infrastructure information (CEII)** intended to clarify and adapt procedures for gaining access to CEII that would otherwise not be available under the Freedom of Information Act. The Final Rule Order No. 630 was issued in September 2006. CEII limits dissemination of information that refers to "specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

- Relates details about the production, generation, transmission, or distribution of energy;
- Could be useful to a person planning an attack on critical infrastructure;
- Is exempt from mandatory disclosure under the Freedom of Information Act; and
- Gives strategic information beyond the location of the critical infrastructure." (FERC website accessed 5.2008 at http://www.ferc.gov/legal/ceii-foia/ceii.asp#skipnavsub).

FERC issued a series of orders to specify and clarify these requirements, including Order numbers 702, 683, 683-A, 649, and 683. Some of these orders, in response to public response to the restrictions on information dissemination, modify the restrictions. CEII allows owners and operators, including employees and officers, to obtain CEII relating to its own facility directly from FERC and to authorize their agents to also obtain this information for their facility.

The North American Electric Reliability Council (NERC), an industry organization, deals with the U.S. electricity sector, including the transmission grid. Although Homeland Security Presidential Directive 7 clarifies that DOE is the lead agency with which the energy industry will coordinate responses to energy emergencies, the DOE has limited authority in the infrastructure assurance area. Portions of DOE's energy infrastructure security and assurance activities were transferred to the U.S. Department of Homeland Security in 2003, which also has no regulatory authority to force utilities to implement security initiatives. NERC, an industry organization that promotes the reliable operation of the electric system and was designated sector coordinator for the private electric utility sector in Presidential Decision Directive 63 (1998), has retained responsibility for promulgating and overseeing reliability guidelines for the electric power industry. However, it does not have enforcement authority, and therefore compliance with its guidelines is voluntary for electric utilities. NERC is responsible for assessing sector vulnerabilities and developing plans for the utility sector to reduce system vulnerabilities. It operates the Information Sharing and Analysis Center (ISAC) for the electric utility industry. (Based on Abel 2005.) Security-related initiatives include measures to protect critical infrastructure information, establish protective buffer zones around critical power facilities, and to establish a National Emergency Energy Spare Parts Program.

Security for the Liquefied Natural Gas (LNG) Infrastructure. As characterized by Parfomack's (2007) review for Congress, because the U.S. LNG infrastructure is highly visible, easily identified, and has a potential for catastrophic consequences from a serious accident or attack, it is considered a potential terrorist target. The LNG infrastructure consists of large tankers, seven import terminals, and inland storage plants. According to Parfomak (2007), public concerns about LNG risks, along with a perceived national need for greater LNG imports, have led some in Congress to examine the adequacy of security provisions in federal LNG regulation. LNG infrastructure security is overseen by the U.S. Coast Guard, which has lead responsibility for LNG shipping and marine terminal security under the Maritime Transportation Security Act of 2002 and the Security and Accountability for Every Port Act of 2006. The Office of Pipeline Safety and the Transportation Security Administration each have security authority over LNG storage plants within gas utilities and some security authority for LNG marine terminals. The Federal Energy Regulatory Commission (FERC) approves the siting, with some security oversight, of on-shore LNG marine terminals and certain utility LNG plants. Parfomack outlines the debate about the likelihood of a terrorist attack on the U.S. LNG infrastructure, in which industry representatives and FERC are characterized as believing that NG facilities are relatively secure compared to other hazardous chemical infrastructures that receive less public attention. One issue is that LNG tanker crews are almost uniformly non-U.S. citizens. According to Parfomack's review, heightened public scrutiny of LNG facilities has increased the cost and complexity of LNG terminal siting and required them to be sited further from major gas markets, although construction of several new import terminals has been approved.

Transportation Sector (especially Maritime)

The Transportation Worker Identification Credential (TWIC) Program, a DHS Transportation Security Administration (TSA) and U.S. Coast Guard initiative, has devoted several years to addressing the infrastructure and technology requirements for establishing a usable, secure system of personnel identification and the issuance of a joint final rule governing its use. The purpose of the TWIC program is "to ensure that only authorized personnel who have successfully completed a security threat assessment have unescorted access to secure areas of maritime facilities and vessels" (DHS October 2007).

The TWIC will include a photo and a reference fingerprint biometric that positively links the credential holder to the identity of the individual who was issued the credential. The program has been designed to be used with access control readers that recognize the credential and the information encrypted on it to identify authorized individuals.

The TWIC program conducted a prototype phase in which a variety of technologies and processes were tested, and which addressed one of the most important concerns of workers and employers subject to these new requirements: the criteria for disqualification for employment. According to the TWIC website (Available at: http://www.tsa.gov/what_we_do/layers/twic/index.shtm): "The TWIC program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act, or MTSA, and all U.S. Coast Guard credentialed merchant mariners. An estimated 750,000 individuals will require TWICs."

Enrollment and issuance of the credential is planned to take place over an 18 month period. To obtain a TWIC, an individual must provide biographic and biometric information such as fingerprints, sit for a digital photograph, and successfully pass a security threat assessment conducted by TSA.

The program has established two types of criminal offenses that would disqualify an individual from receiving a TWIC: Permanent and Interim, which covers a seven-year period preceding the date of application. Permanent disqualifications, not subject to waiver, include:

- Conviction of any of the following felonies (ever):
  - Espionage or conspiracy to commit espionage;
  - Sedition or conspiracy to commit sedition;
  - Treason or conspiracy to commit treason; and
- A federal crime of terrorism as defined in 18 U.S.C. 2332b(g) or comparable state law, or conspiracy to commit such a crime.

The program provides a waiver mechanism (for individuals who clearly have committed a disqualifying criminal offense (itemized at http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm#Crimes) or have been declared mentally incompetent, but believe they are rehabilitated to the extent that they should be granted a TWIC) as well as an appeal process.

Possession of a TWIC does not guarantee access to secure areas because the owner/operator controls which individuals are given unescorted access to the facility or vessel. Rather, TWIC is intended to provide a secure, verified credential that can be used in conjunction with the owner/operator's risk-based security program that is required in security regulations issued by the Coast Guard. TSA will make available a list of invalid credential numbers to facility and vessel operators for use in insuring that holders of revoked credentials are not able to access secure areas without an escort. Concerns about the cost and durability of the automated credential readers have led TSA and the Coast Guard to modify the program to include visual review of the TWIC by owner/operators at access points. Enrollment in the program started in October 2007 at the Port of Wilmington.

The Maritime Transportation Security Act (MTSA) of 2002 (Available at: http://www.tsa.gov/assets/pdf/MTSA.pdf) requires the Coast Guard to conduct a vulnerability assessment for each port and directs the federal government to issue a biometric transportation security credential to any individual with unescorted access to secure areas of facilities and vessels and all mariners holding Coast Guard issued credentials or qualification documents. The MTSA also specifies that all U.S. port facilities deemed at risk for a "transportation security incident," such as LNG marine terminals, fossil fuel processing and storage facilities, and cruise ship terminal facilities, must prepare and implement security plans for deterring such incidents to the "maximum extent practicable." Through the MTSA, Congress directed the federal government to issue a biometric security credential to individuals with unescorted access to secure areas of facilities and vessels, and all mariners holding Coast Guard-issued credentials or qualification documents, on the basis that controlling access to secure areas is critical to enhancing port security.

The TSA Hazmat Threat Assessment Program (Available at: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/enforce_tsa.xml) requires the collection of biographical information and fingerprints from applicants who wish to obtain a new Hazardous Materials Endorsement (HME) on their state-issued Commercial Driver's License (CDL). This requirement became effective for new applicants on January 31, 2005. Individuals wishing to renew or transfer an existing HME were required to submit biographical information and fingerprints beginning May 31, 2005.

TSA Employee Screening Program, implemented in 2006 (Available at: http://www.tsa.gov/what_we_do/layers/employee_screening.shtm), deploys roving patrols of Transportation Security Officers to inspect workers, their property and vehicles, and to ensure that access protocols are being followed, even though all workers are subject to a security threat assessment prior to receiving credentials and access privileges. These assessments consist of criminal history records checks and vetting against terrorist watch lists. These assessments are required not only for airport personnel, but also individuals with access to public areas that possess airport credentials, which include taxi drivers, parking lot attendants, vendors and shuttle bus drivers who have identification issued by the airport.

Commerce/Transportation Sector

Department of Homeland Security U.S. Customs and Border Security's Customs-Trade Partnership Against Terrorism (C-TPAT), a post 9/11 Customs and Border Protection (CBP) initiative (Available at: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml), is a public-private partnership that has developed security guidelines designed to increase security of the supply chain of materials entering the United States. The current security guidelines for C-TPAT program members address a broad range of topics including personnel, physical, and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing. Companies that apply to C-TPAT must sign an agreement with CBP that commits their organization to the program's security guidelines. These guidelines enable members to develop a customized solution, while providing a clear minimum standard that approved companies must meet. Minimum security criteria have been established for marine port authority and terminal operators, customs brokers, air carriers, rail carriers, foreign manufacturers, highway carriers, importers, and sea carriers.

Law Enforcement Sector

The FBI-Administered Terrorist Screening Center (TSC) (Available at: http://www.fbi.gov/terrorinfo/counterrorism/faqs.htm) was established in the fall of 2003 to consolidate terrorist watch lists and provide operational support around the clock to federal screeners, thus enabling "all government agents to run name checks against the same comprehensive list with the most accurate, up-to-date information" about potential terrorists and persons with links to violent gangs and to receive results and technical support quickly. The FBI has undertaken a concerted effort to develop and deploy

information technology that enables progressive fusion of information from multiple sources and lists and that applies increasingly powerful matching algorithms. Because terrorists may not have criminal records, the TSC is seen as serving a complimentary function to the FBI's integrated automated fingerprint identification system and its criminal record check process (IAFIS). IAFIS was established in 1999 and is used to establish true identity and identify past criminal records. The TSC database consolidates information from watch lists maintained by multiple agencies. In 2008, this included twelve databases from agencies within the Department of State, the Department of Homeland Security, the Department of Justice, the FBI, the Marshals Service, the Department of Defense, and the Air Force.

In 2005, the FBI established the **Terrorist Screening Records System (TSRS)** that encompasses the government's consolidated terrorist watch list information, operational support records, and records related to complaints or inquiries (10 FR 43715). The TSRS is exempted from a number of the requirements specified in the Privacy Act of 1974 (5 U.S.C. § 522a). The TSRS contains classified and unclassified information about known or suspected terrorists, individuals screened by the TSC as possible watch list matches, individuals who are misidentified as watch list matches, individuals who submit redress inquiries, and information about encounters with all of these individuals (Electronic Privacy Information Center (EPIC) 2005).

The National Protection and Programs Directorate of DHS implements the **Automated Biometric Identification System (IDENT)** that maintains electronic records including fingerprints, pictures, biographic, and encounter-related information. IDENT was originally developed in 1994 for the Immigration and Naturalization Service (INS). Following INS's incorporation into DHS, the scope and purpose of the system expanded to be the primary DHS system for biometric identification and verification of individuals encountered across the DHS mission areas. According to the DHS, IDENT has become the "largest fingerprint repository and most efficient matching system in the world," with over 91 million individual fingerprint records, which it forecasts will grow at a rate of 20 million new fingerprints per year. It also contains biometric data for "legitimate travelers to the US, immigration benefit seekers, and immigration violators," and watchlist data – information on known or suspected terrorists, criminals, sexual offenders, domestic and international fugitives, officer safety threats, military detainees, other persons of interest, and other egregious offenders. IDENT receives an individual's fingerprints and compares them against stored fingerprint records. (DHS Exhibit 300 2009).

Water Sector: Water Infrastructure and Dams

The Environmental Protection Agency (EPA), which regulates the safety of public water supply systems under the Safe Drinking Water Act of 1974, has collaborated with other federal, state, and local agencies following the terrorist attacks of 2001 to develop guidelines, voluntary protocols, and tools for securing water systems and preparing emergency response plans, and has encouraged the conduct of vulnerability assessments. According to a Congressional Research Service report (Copeland 2007), there were no federal standards or agreed-upon industry best practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery, although Congress has required community water systems to assess their vulnerability to a terrorist attack. In addition, the EPA is not authorized to require water infrastructure

systems to implement specific security improvements or meet particular security standards. In 2004, this partnership resulted in publication of three guidance documents and a set of voluntary standardized best engineering practices. In addition, EPA created a National Homeland Security Research Center and a Water Security Division. Review of the materials describing these EPA activities found no specific focus on security during the construction phase of water infrastructure or recommendations concerning security during construction.

U.S. Army Corps of Engineers and Bureau of Reclamation – The Corps and the Bureau have received appropriations to support risk assessment of needed security improvements. Physical hardening and other protective measures have been undertaken. The Bureau's security budget includes a law enforcement program (guards and surveillance) and facility fortification. The Corp's budget covers recurring security costs (i.e., guards and monitoring) for administrative buildings and other general use facilities (Copeland 2007:10). No discussion of security during construction was found.

Appendix C: Summary of TISP Construction Security Workshop

C.1 Origin of the TISP Workshop

In the course of the initial investigations for this project, the project team contacted TISP, a public-private partnership established shortly after 9/11, for its expertise on CI security. The partnership includes representatives from the design, construction, operation, and maintenance communities; local, state, and federal agencies; academe; and other related organizations. TISP's membership spans organizations that operate all types of critical infrastructure. Its mission is to promote collaboration in developing and implementing cost-effective solutions that enhance the resilience of the nation's critical infrastructure by leveraging the partnership's collective resources and expertise. TISP representatives indicated that they had not yet focused attention on the construction aspect of CI protection, but were interested in doing so. Noting that the objectives of this NRC project fell squarely within their mission, TISP offered to host a workshop of experts on security during CI construction. Because TISP's mission covers CI in general, the workshop scope addressed CI construction in general, with particular attention to NPP construction as an example case in point. The project team participated in this workshop and TISP drew upon the analytical approach and preliminary information about potential threats and protective measures developed for this project to structure the workshop discussions. The project team worked with TISP leadership to prepare for the workshop, follow up on recommendations made during the workshop, and to analyze the workshop results.

C.2 Purpose and Limitations

The TISP workshop was held in Washington, DC in February 2008. TISP's primary goals for the workshop were to a) initiate a dialogue on security during the construction of CI facilities among its members and b) to provide a forum for considering protection priorities and the types of protective strategies and measures that might be warranted and cost effective, using the construction of NPPs as a specific case study.

The purpose of the one-day workshop was to bring experts together to

1. Conduct face-to-face interactive discussions on the topic of CI construction security in general, to:
   - ✧ Further assess the rationale for addressing security during CI construction and increase awareness of potential security concerns during the construction phase;
   - ✧ Discuss the analytical framework that would be appropriate for identifying and evaluating construction security threats and protective measures; and
2. Conduct more focused breakout sessions directed at two particular types of CI, NPPs and another type of CI facility to be selected by the group, to:
   - ✧ Apply and further refine the general framework to examine construction security in these particular CI sectors;
   - ✧ Begin to identify the potential security threats, assess their relative risks and propose possible solutions in these two CI sectors.

For simplicity, TISP focused the workshop on security for CI facilities being constructed on separate/greenfield sites to allow workshop participants to focus on the attributes of the facility under construction separate from consideration of spill-over impacts from adjacent facilities. Earlier benchmarking had established that the security requirements for construction at shared sites, where the CI facility under construction was proximate to or integrated within an operating facility of the same type, were influenced by the security requirements of the operating facility. CI facilities under construction were often subject to the same security requirements as were in place at the operating facility on the shared site.

In designing the workshop, TISP recognized the need to start with a broad scope, given feedback from its membership that the issue of security during the construction phase of critical infrastructure facilities had received little focus or prior discussion. Based on response from invited participants, TISP also determined that the initial workshop should be limited to a single day. Given this, TISP's goals for the workshop were to introduce and discuss a framework and methodology for determining the need for and possible approaches to security during construction, raise awareness of this aspect of security for U.S. CI, and bring experts with multi-sectoral experience into the discussion of NPP construction security issues and protection needs. It was clear that there would be insufficient time in a one-day workshop to reach specific conclusions or develop comprehensive recommendations. Therefore, TISP indicated that it would consider hosting follow-up workshops during which topics could be addressed in greater depth. One such topic, identified during workshop planning, was to look more carefully at security considerations during NPP construction at shared sites proximate to or integrated within operating facilities to examine how the intersection of construction and operation activities may present security risks that are qualitatively or quantitatively different than the risks associated with NPP operations alone. A possible goal of this follow-up workshop would be to affirm that the protective measures in place for operating NPPs are necessary and/or sufficient to address the security concerns associated with the more complex mixed activity situation.

Acknowledging the potential for this longer-term framework, the 2008 TISP workshop sought to determine:

- The extent of expert consensus about potential threats to CI under construction and appropriate security measures;
- Areas of disagreements, uncertainties, or lack of information;
- What issues warranted further examination and perhaps more focused workshops, and;
- How best to proceed.

C.3 Workshop Planning and Structure

TISP drew upon its broad network to assemble experts capable of examining the issue of CI construction security in general and NPP construction security in particular. TISP identified and invited many of the CI experts and invited the NRC to identify and invite experts in the nuclear domain. A list of the names and affiliations of the 26 workshop participants is included in Appendix A. The agenda and background materials for the workshop are shown at the end of this appendix in Section C.8.

In preparation for the workshop, TISP requested the project team to provide a draft analytical approach and framework based on the preliminary information it had developed from its consultations with experts as a starting point for the workshop discussion. The workshop participants would vet and refine the framework and methodology, which would be used in the breakout sessions to guide the examination of construction security for the two case examples. TISP also requested the project team to provide short overview discussions on the following topics:

- Personnel security (including fitness for duty and access authorization);
- Information security;
- Supply chain security; and
- Issues pertaining to management roles, responsibilities, and commitment to ensuring construction security.

TISP designed the workshop to be interactive. Following introductions and a general overview of the goals and schedule for the day, the project team presented a draft version of the systems-based, life-cycle approach with a cost-benefit orientation (discussed in Chapter 2, and led the workshop discussion about its utility for the workshop topic, alternative approaches, and recommended updates and changes. The whole group of participants then participated in a series of presentations and expert discussion about (1) the nature and existence of threats of potential concern for CI facilities under construction; (2) methodologies for identifying and assessing threats; (3) target desirability/vulnerability; (4) immediate versus delayed impact threats; (5) intentional versus unintentional activation of threat pathways; and (6) types of threats that might occur to CI facilities during construction. During the first set of breakout sessions, participants applied the analytical process to identify credible threats and threat pathways during the construction phase of NPPs and other participant-selected types of CI facilities. In the subsequent breakout sessions, participants discussed how they would apply the analytical approach to design a protective strategy for either an NPP under construction or another type of CI facility. Participants were asked to discuss whether typical construction practices would be likely to address the identified threats adequately and, if not, to identify what other security measures might be needed. Based on these discussions, the participants were given another opportunity to critique the proposed framework and analytical process and suggest further revisions. The whole group then discussed areas of agreement, outstanding issues, and recommended next steps.

The general discussions among workshop participants resulted in:

- A vetted, further refined framework and analytical process for examining construction security;
- A more robust view of expert opinion regarding
  - Security during the construction phase for various types of CI;
  - The key security issues;
  - Ways to more effectively and efficiently address the issue of CI construction security and some of the challenges in involved in their implementation; and
- A conceptual representation of an approach for developing a security strategy for the construction phase of a facility's life cycle.

The workshop breakout sessions focusing on NPPs during construction included:

- A systematic discussion to assess, prioritize, and address threats associated with NPP construction;
- Identification of protective measures that might be applied during NPP construction; and
- Discussion of the role of security managers during complex construction projects and their relationship to overall project construction management.

Participants in the breakout sessions on construction security considerations for other CI facilities discussed how the attributes of several different types of CI facilities (conventional power plants, electrical grid/transmission systems, internet and financial systems) and their functions affected the security issues they might face. They then focused their attention on security issues for conventional electrical generating (power) plants during construction. The results from these breakout sessions are incorporated into the following sections, as pertinent.

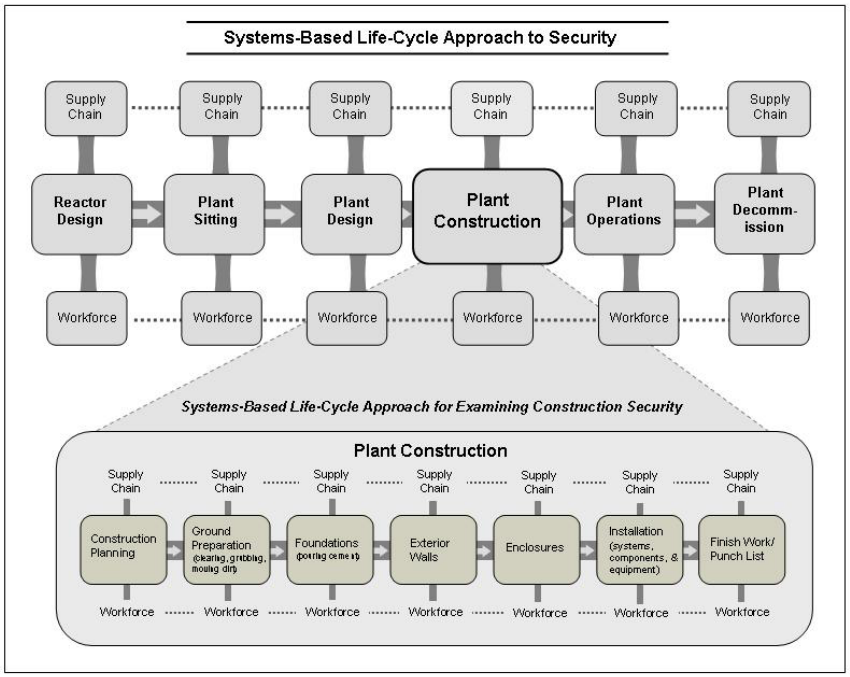
C.4 Framework and Analytical Approach

To establish a common base for departure, the workshop started with a discussion of the purpose of the workshop, CI and threats, and the frameworks and methodologies for addressing construction security issues. The project team briefly described the approaches and analytical frameworks it had developed from earlier discussions with experts and review of the literature and used to structure the workshop discussions and breakout sessions. The workshop participants were asked to consider these analytical approaches, discuss how they compared to the approaches the participants used in their work, offer suggestions about modifications or alternatives, and then apply the revised approaches/methodologies in their workshop session discussions.

Systems-Based, Life-Cycle Approach with a Cost-Benefit Orientation

The project team provided a brief overview of the three major components – systems, life cycle, and cost-benefit – of this approach, which are described in some detail in Chapter 2, and asked workshop participants to discuss and critique a systems-based, life-cycle approach with a cost-benefit orientation. Figure C.1 shows the illustration of this approach presented at the workshop.

Figure C.1 The Proposed Systems-Based Life-Cycle Analytical Approach



Several workshop participants observed that this framework introduced important perspectives into the consideration of construction security and that it highlighted a potential need to assemble experts in the different life-cycle phases and facility/plant systems for a face-to-face discussion because few individuals would have the expertise to address all aspects of the framework. Workshop participants critiqued the framework and agreed that the systems-based life-cycle approach did encourage consideration of cross-phase opportunities and impacts and that it could be useful in developing security strategies for NPPs and other CI facilities as well. They observed that implementing the proposed analytical approach would require assembling the individuals with the necessary range of expertise, authority, and responsibility and that these individuals were typically scattered across different organizations and organizational units. Therefore, implementing a full-fledged analysis using the analytic framework would constitute a large effort. However, the workshop participants generally agreed that the analytical approach could be useful even if used only as a framework and guide to thinking. They also acknowledged that it provided a useful overall framework for the workshop.

Several workshop participants pointed out that when attempting to deal with security issues it is important to be aware that perspectives on risk vary across organizations and individuals. Therefore, individuals with different roles and responsibilities are likely to have notably different perspectives on risk. They emphasized that in planning risk-related initiatives such as construction security it is important to identify and address these differences. In particular, they recommended that the mechanisms that govern how risks are shared/allocated between the owner of the facility and the construction contractors be specifically examined. In designing measures to increase security, several workshop participants suggested that it would be useful to consider the orientation toward risk held by key decision makers. They pointed out that some

individuals were likely to subscribe to a strategy of risk ignorance while others would employ strategies to transfer risks to others. They predicted that only a subset would undertake active and informed risk management.

Vulnerability Assessment Framework

The project team also briefly outlined the five-component vulnerability assessment framework shown in Figure C.2 and described how it had been used in structuring the workshop. The discussion leaders then asked participants to offer suggestions for modifying this framework, and then to apply the revised framework, in conjunction with the systems-based life-cycle approach with cost-benefit orientation, in the workshop discussions. They also asked participants to comment on the information, expertise, steps, and challenges involved in developing a security strategy for CI during construction that would be informed, robust, and cost-effective.

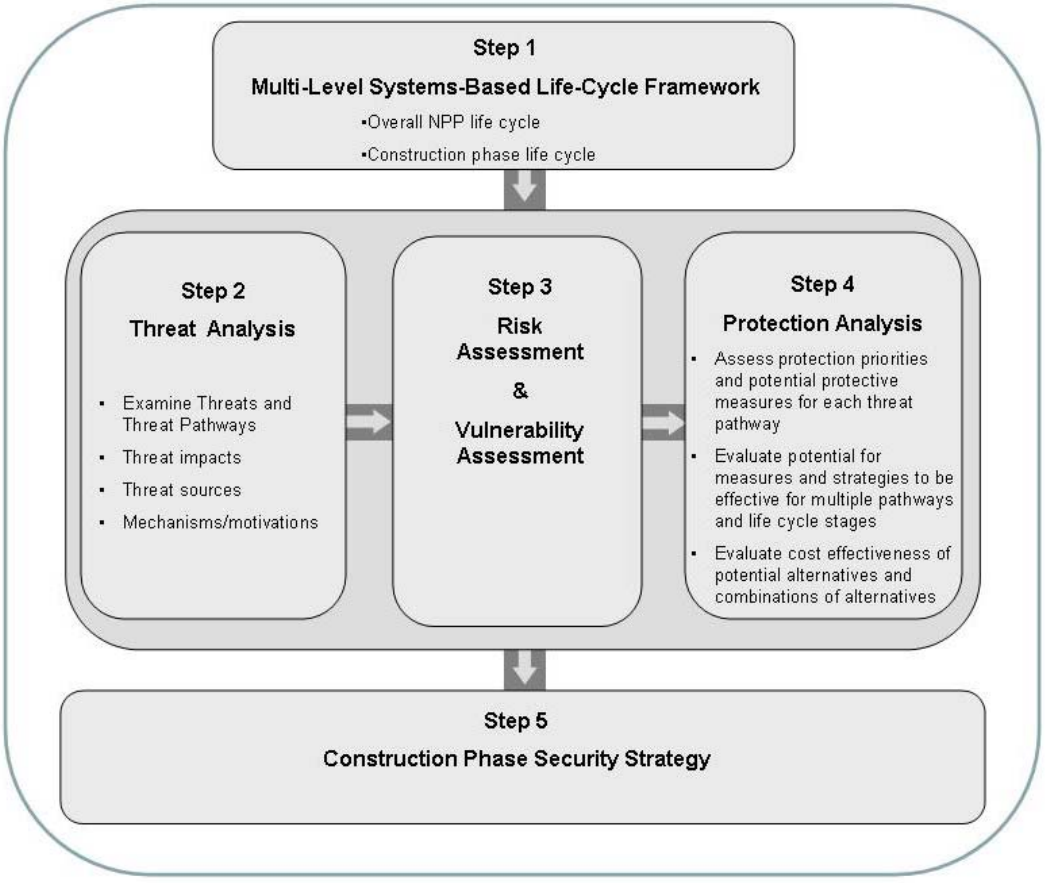


Figure C.2 Proposed Five-Step Process for Developing a Construction Security Strategy

Recognizing time, information, and expertise limitations, the discussion leaders then called upon the group to draw upon the best resources available in their sessions to apply this approach in their discussions of the agenda topics with the goal of generating some of the information that would be used in developing a security strategy for CIs

during construction. They asked participants to (1) discuss the types of knowledge and analytical methods that they would expect to be used in each step or component; (2) apply the knowledge and analytical methods they had available to provide their expert opinion about the results of each step; and (3) note, in general, what other kinds of information or analyses would be needed to develop a robust strategic security plan. Although the breakout sessions were designed to focus on NPPs or one other type of CI facility to be chosen by the group, the participants were asked to consider the applicability of the approach to other types of CI facilities and other life cycle phases.

The following summarizes the description of the proposed vulnerability assessment framework provided to the workshop participants and the discussions that ensued.

Step 1: Develop a Systems-Based Life-Cycle Approach with Cost-Benefit Orientation for Construction Security

As illustrated in Figure C.1, the systems-based life-cycle component represents knowledge about how the facility is designed and built, where it is located, characteristics of the workforce needed for each phase of the life cycle, and what components will be brought in from off-site. It also represents knowledge and information about the systems of the particular type of facility, their life history within the overall life cycle of the facility, and their interdependencies, as well as the protective measures that are in place. Those providing this information would have access to and knowledge about plant diagrams, timelines, work schedules, and to engineering specifics. The information represented in this component would typically be focused on the physical attributes of the facility, its components, systems, and the personnel conducting the activities of the different life cycle phases as well as factors external to the facility that have a planned interaction with it. When combined with the knowledge and information from other components, this facility-based information about systems and life cycle is needed by other experts in the subsequent steps of the process.

Step 2: Threat Analysis – Identify Construction Security Threats and Threat Pathways (Attack Vectors)

The next step in the analytic process represents knowledge and methods to characterize and anticipate potential threats and possible threat pathways for each phase of the life cycle, with special attention, because of the focus of the workshop, to the construction phase. In conjunction with the knowledge represented in Step 1, the characterization and analysis can be focused on a phase of the life cycle, a system, process, or an activity. The knowledge used in this step includes knowledge about the plant and its life cycle, but also draws on specialized knowledge about the threat environment and what has happened elsewhere and applies analytic tools and data to characterize potential threats as they might be manifest at a particular type of facility in a particular location or by a particular source. Depending upon the stage and purpose of the analysis and the resources available, a threat assessment can be primarily conceptual or highly analytic. The ideal would be to identify possible threats in each phase of the life cycle and determine their connection to the construction phase. In conducting this portion of the analysis, the goal is to apply a framework that helps ensure that the entire range of potential threats is considered, including:

- Immediate and delayed impact threats;
- Intentional and inadvertently-caused threats;
- Threats caused by insiders, outsiders, and insiders colluding with outsiders.

Ideally, the analysis conducted in this component would examine all the potential threat pathways by which each of these types of threats might be implemented. For the TISP workshop, time constraints, security considerations, and limited access to information dictated that only generic, (rather than specific potential threats and threat pathways) could be identified, and that threats originating in other life-cycle phases could be identified only illustratively.

Step 3: Risk and Vulnerability Assessment – Assess Security Risks and Vulnerabilities

This step reflects expertise in risk and vulnerability assessment, along with information about threats and facility characteristics and the ability to evaluate potential threats relative to the characteristics of the targeted assets. Vulnerability assessment is used to determine whether potential threats represent credible concerns by characterizing the potential consequences, taking protective measures into account. To accomplish this thoroughly, experts in each of the threat areas and appropriate risk and vulnerability assessment experts would conduct risk and vulnerability assessments to determine each threat's relative risk (probability X consequences), each facility's vulnerabilities, and the priority given to preventing particular consequences. Because a robust risk assessment was well beyond the scope of the TISP workshop, the proposed analytic approach was simplified. The workshop participants discussed the risks and vulnerabilities associated with the types of potential threats that had been and were being identified. They then drew upon information about facility attributes to provide best judgment estimates of the relative risks those potential threats posed, noting their perceptions of the probabilities and the likely and worst case consequences of those potential threats.

Step 4: Protection Analysis – Identify Alternative Protective Measures to Address Risks and Vulnerabilities and Evaluate their Costs and Benefits

In step 4, knowledge about the facility and the construction process is combined with information about potential threats, threat pathways, and vulnerabilities to identify when and where potential threats of greatest concern might occur and to identify and evaluate alternative protective measures to address those vulnerabilities. Once risks and vulnerabilities are understood and located temporally and spatially, analysis of potential protective measures can be used to fine tune strategies and to focus on the locations, activities, and workers of concern. The expertise needed for this step is the ability to identify and evaluate which protective measures (applied to which people and/or to which locations or activities) would provide the greatest benefit in terms of preventing, deterring, detecting, or mitigating the potential threat or disrupting the threat pathway.

To provide a starting point for the discussion of protective measures, the project team provided a list and brief overview of the protective measures the experts consulted prior to the workshop thought would be of greatest utility in addressing construction security threats. This list is presented in Section A.8. Although generally derived from protective measures employed at operating facilities, the list included measures beyond those

customarily used for CI facilities during construction, including protective measures in the following areas:

- Personnel security (including fitness for duty (FFD) and access authorization (AA));
- Information security;
- Supply chain security; and
- Organizational and management strategies to address management roles, responsibilities, and commitment to construction security.

In the interest of time, after discussing the areas where protective measures might provide the greatest utility, the breakout session discussions narrowed the focus to personnel security measures to allow some specificity and consideration of implementation (targeting and timing) and cost-effectiveness.

Step 5: Complete the Analysis – Develop an Informed, Robust Protection Strategy

The final step is to complete the analysis by integrating the security considerations associated with the construction phase within the larger systems-based, life-cycle, cost-benefit framework to:

- Evaluate whether construction security needs might be more effectively addressed by actions taken in earlier phases of the life cycle;
- Promote synergies in security as well as safety, QA/QC, and other measures across the entire life cycle; and
- Identify ways to enhance the effectiveness and safety of the transition from construction to plant operations.

Figure C.3 illustrates this step.

C.5 Summary of Workshop Discussions about Security Concerns and Potential Threats during CI Construction

General Discussion about the Topic of CI Construction Security

The workshop participants agreed that construction security has not been adequately examined in most of the CI sectors, but noted that in several sectors, including nuclear power, this is beginning to change. The participants attributed this, in part to the dramatic consequences and widespread visibility of the security failures during the construction of the U.S. Embassy in Russia and the terrorist attacks in the U.S. and on CI and iconic facilities around the world. Some participants also pushed-back against requirements to assess threats and implement security measures on the grounds that enhanced security measures to protect against terrorist threats were not necessary.

The workshop participants agreed that, consistent with the DHS and TISP emphasis on prioritizing efforts based on sound analysis, it was important to look across the CI sectors and systematically examine threats and security needs for facilities under construction. They agreed that such an examination would require expertise in

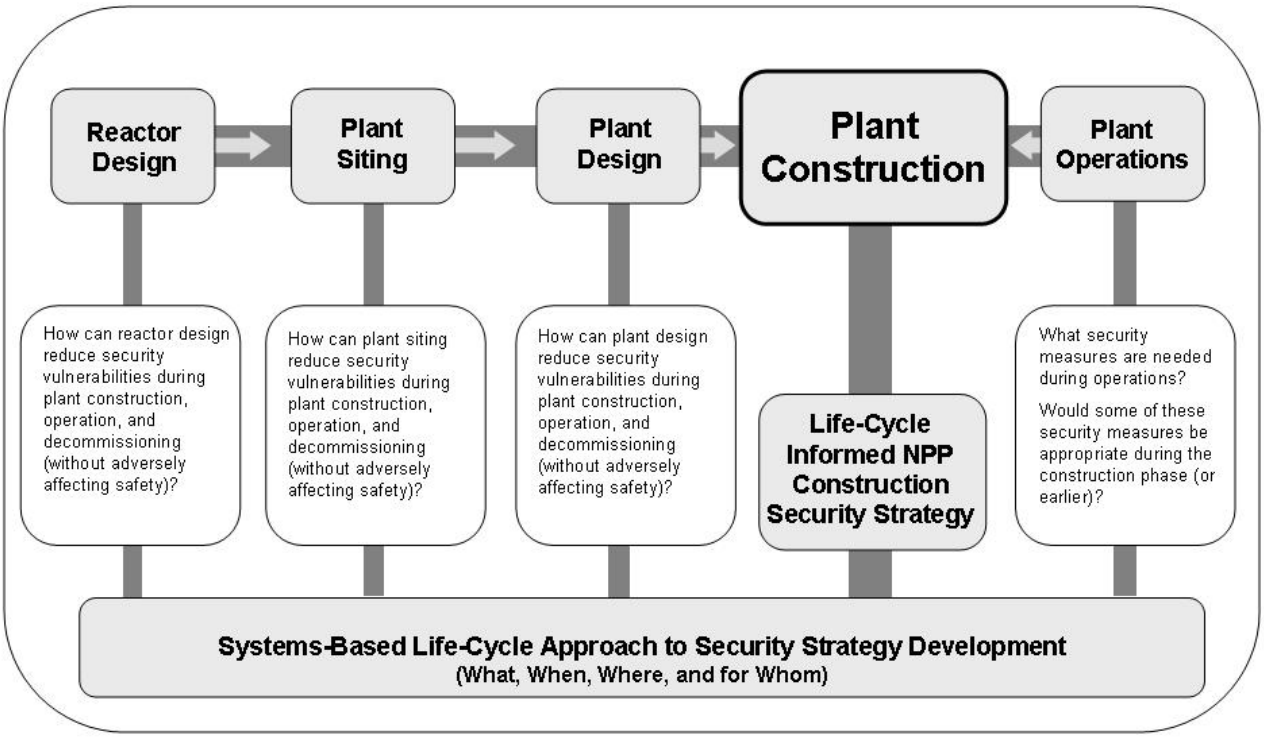


Figure C.3 Completing the Analysis to Develop a Construction Security Strategy

counterintelligence, security, construction processes, facility operating characteristics, and threat, risk, and vulnerability analysis. They observed that CIs that had the potential to threaten public health and safety, if successfully attacked, probably had different threat profiles from those that did not. They thought that these differences needed to be better understood. They also noted that the identification of credible threats did not necessarily mean that management or mitigation of those threats would fall within the jurisdictional authority of any – or a particular – regulatory entity, and that addressing issues of responsibility and authority would constitute a study in itself. Indeed, the DHS and TISP representatives confirmed the centrality of issues about roles, responsibilities, authorities, and funding in the post-2001 efforts to enhance U.S. critical infrastructure security.

Consequently, although the workshop participants expressed the opinion that TISP workshop was a beneficial first step, they cautioned that the workshop discussions could only make a start on the issues. They recommended conducting another workshop specifically focused on examining the nature and timing of security measures needed during the construction phase. If warranted, they recommended conducting another follow-up workshop to consider how responsibility for requiring and implementing those measures should and could be assigned.

The workshop participants agreed that it would be useful to consider which of the security measures utilized or required for an operating facility would be needed and effective during the construction phase and analyze when and to whom they should be applied. However, they warned that, although this analysis would be useful and

necessary, it should not be the only way the issue was addressed. In the view of a number of workshop participants, the security threats and protection needs of the construction phase warranted examination on its own merits so that the facility's systems and life cycle could be appropriately addressed. The recommended that this analysis draw on logical analysis, the available literature, evaluations of existing programs and candidate measures, and recommendations about best practices and cost-effectiveness from a wide range of facilities. They asserted that this would provide a more solid basis for determining (1) whether and to what extent security measures required during NNP operation were appropriate for the construction phase and, equally important; and (2) whether, and to what extent, there were security threats during the construction phase that required different strategies from those needed for operating plants (and that would be insufficiently addressed by imposition of the operating requirements). They pointed out that there may be threats that are unique to the construction phase that require measures not needed or effective for operating plants. The next section presents the more specific expert views regarding NPP construction security expressed during the breakout sessions on NPPs.

Potential Threats of Concern for CIs during the Construction Phase

The workshop had two scheduled sets of breakout sessions:

- The first breakout sessions focused on examining potential construction security threats. One breakout group addressed NPPs under construction and the other chose to address conventional power plants, after a brief discussion of electricity grids and classified spaces and facilities. This report focuses on the results for NPPs, supplemented with information from the other breakout discussions, as applicable.
- The second set of breakout sessions examined protection needs and options for the same two types of CI facilities – NPPs and conventional power plants.

The NPP breakout session participants represented expertise in regulation; NPP security, threat assessment, and counterterrorism; supply chain management and security; threat assessment; risk assessment/vulnerability assessment; NPP and general construction management; civil engineering; and security policy, planning, and implementation.

Potential Threats Identified and Reviewed

In preparation for the workshop, the TISP organizers asked the project team to provide the list of potential threats identified by the experts they had consulted prior to the workshop. This list was included in the breakout session instructions (see Section C.8 and Table C.1) as a starting point for the discussions about threats. The instructions were intended to help prepare the participants by describing three types of threats:

- Immediate and delayed impact threats;
- Intentional and inadvertently-caused threats; and
- Threats caused by insiders, outsiders, and insiders colluding with outsiders.

In the first breakout sessions, the participants were asked to review the preliminary list of potential threats and identify any additional threats of potential concern that were not on

the list. The discussions then focused on participants' views about the differences between immediate and delayed impact threats and the types of consequences that might result from them, and consideration of how facility characteristics might affect the potential for delayed impact threats. Because of time constraints, the breakout sessions focused primarily on the rationale of and potential for delayed impact threats, the preliminary list of which included:

- Hidden explosives;
- Hidden surveillance devices;
- Hiding/storing other materials such as weapons or explosives that may be used later to attack or compromise the NPP once it is operational;
- Obtaining critical information during the construction phase that can be used later to attack or compromise the NPP once it is operational;
- Compromised construction materials through either fraud, theft, crime, or intentional tampering;
- Compromised critical systems, including safety- and security-related systems, structures, and components [SSR-SSCs] through either fraud, theft, crime, or intentional tampering;[59]
- Accumulated errors due to blundering, ineptitude, impairment, language barriers[60] that remain undetected and could impact operational effectiveness, safety, and/or security; and
- Bio/chemical agents introduced clandestinely onto the site.

The breakout session participants suggested adding compromised or deficient major components other than critical SSR-SSCs to the list of potential delayed impact threats. Several participants noted that current construction often uses modular construction and that many facility components are built off-site and then transported to the construction site for final assembly. Workshop participants thought that this could make the components vulnerable to quality control failures, fraudulent substitutions, tampering, or sabotage during fabrication or transit because these types of problems have occurred frequently in the past on large-scale construction projects. They pointed that although

[59] Safety-related SSCs are defined as "Those structures, systems, and components that are relied on to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capacity to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in Title 10 of the Code of Federal Regulations (10 CFR), Section 50.34(a)(1)." Security-related SSCs are "those structures, systems, and components that are relied on to implement the physical security and safeguards contingency plans (1) required by 10 CFR Part 73 ….or (2) included in the combined license application …." (U.S. NRC November 30, 2007 SECY-07-0211).

[60] A number of studies have called attention to the growing percentage of non-native English speakers in the construction industry and the role inadequately addressed language barriers have played in construction-industry fatalities. For example, O'Malley (2001) points out the increasing percentage of Hispanic workers in the construction industry, including those in unionized jobs. Although starting in the relatively unskilled jobs, an increasing number of Hispanics are moving into the operation of equipment. The International Union of Operating Engineers (IUOE), for example, has identified the language barrier as a sufficiently significant problem to workplace safety that they have established a National Hispanic Outreach Program. Although focused on the residential construction industry, a study sponsored by the National Association of Home Builders found that approximately 29% of the workers in this industry during the period 2003-2006 were foreign-born. The U.S. Department of Labor estimated that in 2006 about 28% of all construction workers were non-natives to the U.S. (*Nation's Building News* 2008.)

not necessarily intended to create a delayed impact threat, compromise of materials and components had the potential to do so.

Potential Threats Identified by Workshop Participants to be of Greatest Concern for NPPs

The NPP breakout session participants considered the following threats to be of greatest concern during NPP construction:

- Compromised SSR-SSCs;
- Compromised or deficient major components or materials;
- Acquisition of information that could be of use later to attack or compromise the plant once it is operational;
- Accumulated errors resulting from blundering, ineptitude, or language barriers that remain undetected and potentially impact operational effectiveness, safety, and/or security; and
- Theft, vandalism, or sabotage to cause direct impacts.

The NPP breakout session participants tended to apply an endogenous risk assessment perspective in their consideration of these threats (meaning that risk is affected by human intervention and, therefore, by both existing practices and supplemental protective measures, which could reduce the potential risk to a level of lesser concern).[61] This breakout group acknowledged the potential of some delayed impact threats, but considered them to be of lesser concern because they thought that it would be reasonable to implement measures that would protect against them. The NPP breakout session participants did not consider explosives concealed in walls or components to be as serious a concern as some of the other potential delayed impact threats because they thought that detecting and protecting against hidden explosives was not nearly as difficult as protecting against some of the others. They reduced the level of concern about potential hidden explosives on the grounds that burying explosives in layers of concrete to avoid detection would present difficulties with remote control devices, and that it would be possible to detect explosives not concealed in this way by a sweep, potentially using sniffer dogs, at the end of plant construction. [62]

The breakout session on conventional power plants agreed that pathways for delayed impact threats could exist, but judged the incentive to delay impact at a conventional power plant to be considerably less than for NPPs. This is because disabling or

[61] See Crocker and Shogren's (1999) article in the *Handbook of Environmental and Resource Economics*. They point out that this perspective on risk assessment is more realistic because it takes into consideration the net of the interaction between exogenous risks and actions taken to reduce exposure to or the consequences of that risk.

[62] The successful smuggling onto the site and detonation of explosives at the nearly completed Spanish Lemoniz reactor indicates that this type of threat cannot be dismissed as a concern. Because the breakout session discussion was focused on the potential for delayed versus immediate impact threats, the discussion did not focus on the potential for a Lemoniz-type incident, where the explosives were apparently not buried within the structure, but were brought on site toward the end of the construction phase. Although methods for detecting explosives have improved considerably since the 1970s and physical security measures, if appropriately applied, should therefore be effective in detecting efforts to smuggle explosives onto the site or conceal them for later use, subsequent discussions with experts indicate that this threat should be among those considered of high concern.

destroying a nearly completed conventional plant would have similar consequences and symbolic impact as disabling or destroying an operational plant.

The conventional power plant breakout session participants had a different opinion about hidden explosives from the NPP group. They thought the potential for hidden explosives to be a serious concern. The potential for technology that allowed explosives to be positioned nearby rather than requiring them to be place on-site influenced this assessment. They also pointed out that conventional power plants are not typically located within large sites with owner-controlled buffer zones, as NPPs are, and that conventional plants would therefore be less protected from explosives positioned nearby than NPPs would. This was because conventional plants would lack the buffer zones and robust plant design that protected NPPS from this type of threat. This discussion led the conventional plant group to note that it was important to determine when in the construction life cycle of NPPs control over the buffer zone was established in order to evaluate this potential threat.

Neither breakout group thought that hidden surveillance devices were an immediate or delayed impact threat of particular concern during the construction life cycle, given the function of the facilities and the nature of information discussed and stored at them. Neither breakout group identified NPPs or conventional power plants during construction as the most likely targets for biological/chemical attacks, given their geographic locations and functions (i.e, not major gathering or transit places for large numbers of individuals), and therefore did not consider potential biological/chemical threats to be among the highest construction security concerns.

Discussion of Threats, Risk, and Vulnerabilities (Probabilities, Consequences, Threat Pathways/Vectors) during Construction

In comparing their discussions of threats, workshop participants noted that NPPs' potential to become a threat to public health and safety if attacked after fuel arrived on site not only made them more desirable than conventional power plants as potential targets but also created the potential for terrorists/saboteurs to have an interest in perpetrating delayed impacts. They generally concluded that the modest difference in consequences from an attack on a conventional power plant before and after it became operational reduced the relative desirability of delayed impact strategies for conventional power plants. However, consideration of both NPPs and conventional power plants led participants to agree that there were threats to the safety and security of the workforce, the plant, national critical infrastructure assets, and the neighboring communities that appeared to justify security measures during the construction phase of both types of facilities.

The workshop breakout groups then used the information gained from the discussion of threats in their discussions of the risks and vulnerabilities of the two types of facilities to those potential threats.

Critical Safety- and Security-Related Systems, Structures, and Components (SSR-SSCs)

The NPP breakout session participants noted that as the nuclear industry begins to address construction security, attention is being focused on safety- and security- related systems, structures, and components (SSR-SSCs). The potential for delayed impact at

NPPs is apparent, according to the workshop participants. Although it may be possible for SSR-SSCs to be compromised on-site either intentionally or inadvertently (such as from deficient materials, incorrect techniques, or faulty construction), some participants thought that a potentially bigger, less recognized issue involved the supply chain and off-site contractors and personnel who might have access to SSR-SSCs. Some of the NPP breakout session participants thought that the design and build stages of the SSCs that occur off-site presented a greater opportunity to compromise these systems than the work conducted on-site. Reflecting the endogenous risk assessment perspective, they argued that there was greater recognition of the need to select and oversee workers on site and to impose quality assurance and control measures to on-site activities than to apply those measures to the supply chain entities and workers. The workshop participants confirmed that supply-chain security issues are just beginning to be assessed and addressed for power plant construction.

Workshop participants in both breakout groups also raised concerns about the vulnerability of software systems, but this vulnerability was considered a more serious issue by the NPP group because of the potential for failure to result in greater risks to the public and environment. Although they agreed that security of the supply chain for critical software systems has probably received the most attention and effort to date, some participants in the NPP breakout session felt that it remained a major security concern. The reasons given for this concern were their expectations that software systems would play a larger, more important role in the next generation reactors, and their skepticism that reactive protective measures (detecting compromises after the fact) were feasible and could be effective. They expressed the view that proactive protective measures were still based on educated guess-work and that proactive prevention measures were likely to be outwitted before the software systems reached the end of their scheduled service.

Compromised or Deficient Components and/or Materials

Workshop participants noted that compromised or deficient components or materials have long been a major QA/QC concern from a safety perspective and are now being addressed from a security perspective as well. The materials and construction processes thought to be of greatest potential concern include cement, rebar, steel, rivets, and welds.[63] The threat pathways in these cases are primarily supply chain fraud or sabotage and unintentional on-site construction errors or intentional on-site fraud or sabotage. A workshop participant expert in modular construction noted that modular construction of both physical and software components, often by a variety of sub-contractors to the prime construction contractor, added off-site production, transportation, and assembly/integration steps that created potential security vulnerabilities. He argued that this warranted more careful examination than he was aware had occurred. He suggested that there was research on security for modular software development that might provide some insights, but cautioned that the

[63] Lean and Owen (2008) reported that the French nuclear safety agency (ASN) uncovered a series of defects in the construction of a reactor at Flamanville in Normandy being built by Areva, including a quarter of the welds in its steel liner ("a crucial line of defence if there were to be an accident") that were not in accordance with welding norms, and cracks in the concrete base, which is also essential to safety. Similar defects were reported to have been found at the Olkiluoto 3 NPP in Finland, also being built by Areva. The report cites an independent nuclear expert (John Large) as saying that the French and Finnish sites reflect a lack of recent experience in building nuclear reactors and that similar problems could arise at other locations.

significant differences between software and physical component construction/development processes would need to be taken into account in interpreting these findings. None of the other workshop participants were expert in this area, and the breakout group agreed that consultation with individuals knowledgeable in this area as a follow-up to the workshop would be useful.

Critical Information

The NPP breakout session participants identified the ability for unauthorized individuals to acquire information about the facility and the safety and security systems over the course of the construction phase as another potential threat of concern that warranted further examination. Some participants noted that the significance of this pathway was reduced because much of this information was already available from open sources. They pointed out that the approved standard NPP reactor designs are available. However, in the course of this discussion, some participants emphasized that the efforts made to protect information about the unique layout of the plant, particulars of the security systems and security procedures, personnel and physical security plans and other safeguards information that is not publicly accessible indicated that protecting this information was still important. The group generally agreed that unauthorized access to this information did constitute a potential threat worthy of concern.

The NPP breakout group discussed whether there should have been more stringent information control at the reactor design phase. Although the NRC does not regulate the entities involved in reactor design, questions were raised about whether it could, or should, have attempted to establish information controls as part of the advanced reactor certification process. In any event, as one of the participants pointed out: “this ship has left the harbor.” There was agreement, however, that it would be worthwhile to determine if additional measures to control access to information during subsequent phases are necessary and, if so, what information should be controlled and how that control could be effectively implemented.

Both breakout groups discussed the issues and challenges created by the fact that construction sites typically have “busy borders,” with many people and vehicles entering and leaving all the time, and that site management practices often exert limited control over the movement of vehicles, individuals, or materials within the site until late in the construction life cycle. The NPP breakout group noted that the NEI is considering how access to the portions of the construction site where SSR-SSC activities are being conducted could be limited by making these access controlled areas. The breakout session participants agreed that the extent to which access to these areas could and should be restricted and the workers with access to the restricted areas should be screened/selected and monitored warranted further examination.

The breakout group also discussed whether there was critical information that could be obtained by an individual with access to the construction site before SSR-SSC activities began and, thus, before these controlled areas would be established. For example, the question was asked whether an individual could obtain information about the physical location of and points of intersection between the different plant systems, particularly the location of “common nodes” (where multiple systems came together) that might affect plant vulnerability. They also discussed the potential for individuals to acquire critical information from outside the site boundaries, either by working on or observing aspects

of the supply chain, interacting with individuals working on the site, or observing the site and the individuals and materials entering and leaving. They pointed out that the size of the site, its topography, the size and extent of control over a buffer area around the site, as well as the nature of the supply chain and its security, would affect the amount of information that could be gathered in this way. They recommended further examination of the ability of knowledgeable individuals to obtain safety or security-sensitive information by observation or inquiry and when during the construction process this could occur. The results of this examination would determine the need to consider potential protection measures.

Accumulated Errors

Detecting human errors during construction, just as detecting compromised or substandard materials and parts, has traditionally been considered a QA/QC and safety issue for NPPs. QA/QC efforts have focused on ensuring the quality of work and materials that have the potential to affect operational effectiveness, safety, and security. NPP breakout session participants recommended a different approach that placed greater emphasis on preventing errors, supplemented by careful attention to measures for detecting and correcting errors. They pointed out that eliminating the opportunities for errors requires a focus on prevention that includes strategies that go beyond the traditional QA/QC focus on detection and mitigation.

Participants noted a number of reasons for concern that errors that could jeopardize safety and security might creep into plant systems during the construction process. They cited: a) language barriers; b) the persistently high rates of drug and alcohol abuse of construction workers; c) the challenges associated with the first-time construction of new designs; d) inexperienced managers; e) a workforce lacking recent or direct experience with nuclear facility construction; and f) the challenges of maintaining a consistent focus on quality by all contractors and vendors. The problems experienced in the aerospace industry with new modularized construction processes were pointed out, particularly the challenges of managing and integrating the modularized supply chain. The breakout session participants noted the problems that the nuclear industry had experienced with QA/QC programs during the first wave of NPP construction as examples of these challenges. Some participants noted that similar problems were being reported at the new NPPs being built in Europe. The NPP breakout session participants discussed whether QA/QC measures and protocols for plants during construction were sufficiently explicit about how security was to be taken into account, given the increased concern about insider threats.

Some of the breakout session participants expressed the viewpoint that, given the characteristics of the construction workforce and construction process, a variety of protective measures would be needed to ensure quality and prevent errors that could jeopardize safety and security. Candidate protective measures included:

- Enhanced personnel security measures;
- More rigorous employee screening;
- Fitness for duty measures;
- Behavioral monitoring;
- Closer supervision;

- Increased peer-checking (2-person rule); and
- Improved communication strategies (for example providing instructions and other critical information in the languages spoken by the workers).

During this discussion, several participants emphasized the importance of effective management. They pointed out that the effectiveness of protective measures was dependent on effective management. They recommended encouraging the organizations building NPPs s to implement the best available construction planning and management practices and to use technologies available to design workflow, monitor work activities and material quality, and control and track worker and material movements on site.

Participants in the NPP breakout session made the point that errors during NPP construction, including errors that are detected and eliminated, may have unforeseen but important consequences. For example, an NPP construction process seen as flawed and error-prone could undermine public confidence in the safety of the plant by raising questions about how many mistakes were not being detected and corrected. Some breakout session participants argued that measures to prevent errors from occurring were likely to be more cost-effective than those that would be needed to identify and correct errors after they had occurred. Based on these discussions, the breakout session participants agreed that the protective measures identified above should be among those considered for implementation.

Theft, Vandalism, and Sabotage

The workshop discussions noted that increased globalization has prompted reevaluation of how the traditional dominant construction security concerns of theft, vandalism, and sabotage need to be addressed. Participants pointed out that theft now is not merely as an issue at the construction site, but along the entire supply chain. Theft and substitution along the supply chain were considered of particular concern for SSR-SSCs. One of the workshop participants, who manages supply chain security for an aerospace company, described the industry-specific information he had assembled in his efforts to convey the nature of the problem and the need for intervention to the various organizational stakeholders. He advised that those attempting to gain organizational support for supply chain security needed to recognize the different risk perspectives held by different stakeholders and provide concrete, vivid information illustrating the vulnerabilities along the supply chain and the adverse consequences that could result if they were not addressed. The other workshop participants asked whether lessons learned about supply chain security in other sectors could be assembled so their applicability to NPP construction security could be evaluated. They encouraged TISP to take on the task of disseminating this information through its network.

The breakout session participants agreed that immediate impacts from sabotage during construction had the potential to create both an economic impact on the specific plant owner and neighboring communities as well as widespread impacts on the industry as a whole. Some participants took the position that the potential for acts of sabotage against CI to have significant impacts on the country warranted more attention from industry and the federal government than it had received to date. However, they noted that the nature of the consequences of direct impact threats to NPPs under construction, which

probably would not involve radiological materials, might place them outside of the NRC's regulatory purview.

C.6 Summary of Workshop Discussions about Protective Measure Needs and Options

Protective measures vary depending on whether the focus is on protecting/controlling people (personnel security), the site, nuclear materials (material protection, control, and accounting), construction materials and components, or information. Supply chain and management issues cross-cut these other security domains. The workshop discussions focused on only a subset of potential protective measures. The afternoon whole-group session of the workshop started out with a general discussion of the various types of protective measures that would be pertinent to construction security. It included brief presentations/discussions of design security (pre-construction phase of the life cycle), supply chain security, cyber security, information security, physical security, personnel security, and inspection and detection security and the interactions among them. The presentations and discussions were intended to stimulate an exchange of experts' views pertaining to these security areas, including both typical and emergent strategies, best practices, and on-going challenges. They were also designed to inform the afternoon breakout session discussions. Although the afternoon whole-group session included a presentation on physical security measures, neither physical security nor engineering or structural features designed to provide security were addressed in any detail in this workshop.

Graded Approach to Protective Measures

During the whole group presentations, participants discussed the complexity of determining what, when, where, and to whom protective measures would be applied during construction, given the dramatic changes occurring in the people present on the site, the activities being conducted, and the in-place assets over the course of the construction process. They also discussed the trade-offs involved in deciding how much to tailor security measures. Participants with experience managing security programs during large scale construction projects observed that although simple, consistent security measures might affect some people who did not pose a significant threat, highly tailored and therefore variable measures might end up being more costly and less effective. Some participants argued that programs that imposed simpler, consistent requirements (a) were more effective in conveying a clear management commitment to security; (b) reduced administrative complexity at a time when complexity was difficult to manage; and (c) tended to reduce worker resistance/dissatisfaction/ complaints and increase compliance.

The workshop participants agreed that the differences in vulnerabilities and potential threat opportunities over the course of the construction process warranted consideration of a "graded strategy" in which protective measures were tailored and implemented progressively. They agreed that identification of the factors influencing the specifics of this graded approach should be part of the discussions of protective measures. They recommended that the additional administrative complexity of the graded approach be weighed against the reduced scope of the program when assessing the benefit-cost balance of a graded versus uniform approach.

Following this general discussion, the participants again divided into breakout sessions that focused on the following security areas for NPPs and conventional power plants or other CIs during construction:

- Personnel security;
- Information security;
- Supply chain security; and
- Management issues pertaining to security.

The afternoon breakout sessions focused on examining protective needs and options in these areas to address the security concerns identified in the morning breakout sessions.

Need to Consider Jurisdictional Authority

The discussion of CI construction protective strategies, particularly NPPs, led to a discussion about whether the government had greater latitude to impose security measures on its own construction projects than regulators, including the NRC, had to impose requirements on private sector entities. Participants who had worked on government-sponsored projects described a "cradle to grave" security perspective for many of them in which rigorous and closely monitored security programs were in force from project initiation to completion of the construction phase. Participants from the NRC pointed out that the Commission, as the regulator of privately owned entities with a specific, and circumscribed regulatory mandate, is not authorized to require security measures to protect, for example, those entities' investments in a plant or maintenance of their function within the U.S. critical infrastructure (e.g., electricity supply). As participants discussed their experience with different projects, they examined the hypothesis that public versus private ownership influenced the propensity to adopt protection measures. Participants generally observed that those responsible for building publicly owned CI facilities may be more inclined to adopt stringent security measures than owners of private sector facilities. Some participants attributed this difference to a different orientation toward risk, and observed that this might originate from differences in the roles, responsibilities, and liabilities of the entities involved in the construction process.[64]

In the course of this discussion, workshop participants emphasized that regulators have to be very attentive to the scope of their authority, and that some types of threats and some types of protection, though necessary and useful from an analytical perspective, may be outside the regulatory authority of a particular regulator. One participant pointed out that some private sector entities with high security needs or regulatory requirements, for example casinos and banks, might impose similarly rigorous security measures and that it would be worthwhile to examine practices in these sectors, even though casinos

[64] Although not represented at the workshop, the project team's subsequent consultation with persons knowledgeable about other public sector CIs, and review of the literature indicate that the observed commitment to security discussed at the workshop may not be representative of other public sector CIs. The project team speculates that the workshop topic and efforts to invite experts on security resulted in a participant group biased toward agencies and facilities with a particular need for and focus on security. Examples of publicly owned CI sectors that did not have an evident commitment to strong security measures for their facilities under construction include water treatment facilities, dams, roads, and bridges.

are not part of the critical infrastructure.[65] In preparing to apply the systems-based life-cycle approach several workshop participants emphasized that it is important to identify the regulatory authorities and requirements that have or could have security-related consequences at each phase of the life cycle of the new facilities. They suggested that mapping the authorities and requirements onto the systems and life-cycle phases to which they apply could provide a helpful basis for building the cross-organizational information exchange needed to implement a systems-based, life-cycle analysis.

For illustration, a few examples of existing regulatory requirements in each phase of the NPP life cycle were discussed, including:

- Reactor Design:
  - Design certification. The NRC has revised its design certification process to certify new reactor designs.
  - Design Basis Threat (DBT) Rule (10 CFR 73.1). The NRC issued Orders and amended the design basis threat (DBT) rule (final in 2007) to address the twelve factors identified in the Energy Policy Act of 2005[66]. Aspects of this amendment affect new reactor designs and evaluation parameters.
- Plant Siting:

[65] The project team followed up on this recommendation and found that casinos do impose a graded personnel security program on their construction process and impose access controls from project initiation. The individuals interviewed about casinos attributed the rigor of the personnel security measures employed during casino construction in part to regulatory requirements imposed by the gaming commission to prevent money laundering, control organized crime involvement, and prevent theft and fraud. They indicated that it was common for casinos under construction to conduct background checks (which, in the case the project team examined, included true identity, criminal history, credit, and character checks) on workers involved with construction of gaming rooms, power supplies, data centers, and security systems. They also reported using sophisticated access control measures that included smart badges and smart doors (able to determine if someone approached), and a strategy of imposing progressively more rigorous restrictions on worker access to specific areas (i.e., personnel with access to one area cannot also have access to another) and records of entry and exit as construction was completed. Persons interviewed regarding bank construction reported that more rigorous personnel security controls were imposed on the workers constructing data centers than on those constructing bank buildings, whose security relied more heavily on location and design and on physical components such as vaults. They reported that banks often hired specialized companies to install security systems, and that those companies' policies, rather than requirements imposed by the bank, were responsible for ensuring the trustworthiness, reliability, and fitness of their workers.

[66] The EPAct of 2005 states that "When conducting its rulemaking, the Commission shall consider the following, but not be limited to—

(1) the events of September 11, 2001;

(2) an assessment of physical, cyber, biochemical, and other terrorist threats;

(3) the potential for attack on facilities by multiple coordinated teams of a large number of individuals;

(4) the potential for assistance in an attack from several persons employed at the facility;

(5) the potential for suicide attacks;

(6) the potential for water-based and air-based threats;

(7) the potential use of explosive devices of considerable size and other modern weaponry;

(8) the potential for attacks by persons with a sophisticated knowledge of facility operations;

(9) the potential for fires, especially fires of long duration;

(10) the potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals;

(11) the adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility; and

(12) the potential for theft and diversion of nuclear materials from such facilities.''

- ✧ Early Site Permits (ESP) Program and Limited Work Authorizations (LWA). The NRC established the ESP program and the LWA process as part of a revision to the licensing process that includes combined construction and operating licenses (COL). NRC's siting process for NPPs has traditionally taken security into account, but it revised the ESP to update and strengthen the security approach based on the new threat environment and new thinking about how to promote security through siting. The NRC also included consideration of site characteristics, such as proximity to waterways and other access routes, in developing the modified DBT.

- ➢ Plant Design:
  - ✧ Design Acceptance Criteria (DAC) for reviewing the acceptability of plant design to meet the certification process are described in 10 CFR 52.47, including the use of instrumentation and control (I&C) and digital displays (U.S. NRC February 15, 1991 (SECY-90-377)). Whitehead, et al.'s 2007 *Nuclear Power Plant Security Assessment Technical Manual* revises NUREG/CR-1345, providing conceptual and specific technical guidance for NPP design certification and addressing the layout of the facility, the physical protection systems to be used, and the effectiveness of the physical protection system against the DBT.
  - ✧ The NRC has participated in workgroups to examine security issues that could be addressed during plant design. There has been growing interest and attention to security during the facility design phase as a means of mitigating security vulnerabilities. Assuring information control is also an issue.
- ➢ Plant Construction:
  - ✧ The NRC is still examining the need for new or revised regulatory requirements for NPP construction security. The NRC addressed, with participation from the public, the issue of fitness-for-duty during construction in the revised Part 26 rule, published in the *Federal Register* on March 31, 2008 (73 FR 16965). It continues to address, with stakeholder participation, the issues of physical security and access authorization requirements and other issues pertaining to personnel security during construction (see NRC's policy paper on access authorization and personnel security during construction (NRC 2007b (SECY 07-0211)). The NRC may decide to address additional issues. This project is part of the NRC's effort to develop a more robust understanding of the security considerations during construction and their implications for personnel security.
- ➢ Plant Operations:
  - ✧ In the aftermath of 9/11, the NRC issued a series of five orders addressing security for operating NPPs, including orders pertaining to the Design Basis Threat, Access and Personnel Security, Physical Security, Cyber Security, and Information Security. [67] As noted above, the NRC has also promulgated

[67] These orders include: (1) EA-02-026 Interim Safeguards and Security Compensatory Measures (February 25, 2002); (2) EA-02-261 Compensatory Measures Related to Access Authorization (January 7,2003); (3) EA-03-038 Compensatory Measures related to Fitness-for-Duty Enhancements Applicable to Nuclear Facility Security Force Personnel (April 29, 2003; (4) EA-03-039 Compensatory Measures related to Training Enhancements on Tactical and Firearms Proficiency and Physical Fitness Applicable to Armed

the revised Fitness for Duty rule. Revised physical security (10 CFR 73.55) and personnel access authorization (10 CFR 73.56) rules are nearing finalization.

- ✧ The NRC's Insider Mitigation Program (IMP) is in the process of developing performance metrics.

There was also widespread agreement among the participants that it was important to consider implementation issues, indirect effects, and cost effectiveness when attempting to determine best protection strategies.

Personnel Security Measures

The breakout session participants approached the discussion of personnel security options and strategies from a good practices and cost-effectiveness perspective. According to the workshop participants, relatively little attention has been given to personnel security during the construction phase of U.S. CI, most of which focused on on-site personnel. A substantial portion of the overall effort has been on attempting to determine whether, when, and for whom protective measures should be applied. The NRC participants in the workshop described their regulatory philosophy of tailoring requirements to risk significance.

In response to the post 2001 changes in the security environment and the heightened emphasis on potential insider threats, workshop participants indicated that particular attention had been focused on understanding the nature and seriousness of intentional security threats and threats caused by insiders and how to prevent, deter, and detect them. Consistent with the points they had made earlier in the workshop, some participants recommended broadening the focus to consider not only intentional and unintentional threats, but also personnel security issues involving the extended construction-related workforce, including supply chain contractors and suppliers. The workshop participants adopted this broader perspective, although the principal focus continued to be on activities occurring proximate to the construction site. The participants agreed that personnel security measures should address both intentional and unintentional threats. They also agreed that this meant focusing on measures to assure that workers were fit-for-duty as well as trustworthy and reliable. The breakout session discussions focused on laying out the issues involved with personnel security and identifying areas for further investigation, recognizing that the limited time available precluded a thorough exploration of these issues. The NPP breakout session discussion then focused on pre-employment screening, access authorization, and fitness-for-duty measures and other program options, strategies, and issues.

The breakout session participants discussed the following measures/requirements as security program options, noting that time constraints prevented thorough consideration of all potentially useful options:

Pre-employment Screening

- ➢ Verification of identity

Nuclear Power Plant Security Force Personnel (April 29, 2003); (5) EA-03-086 Requiring Compliance with Revised Design Basis Threat for Operating Power Reactors (April 29, 2003).

- Through document review
- Through fingerprinting or other biometric measures

- Citizenship requirement
- Terrorist Screening Center (TSC) review
- Criminal history check
- Additional background checks
  - Credit check
  - Employment and personal history verification
  - Character and reputation check
- Pre-employment or pre-access drug testing
- Pre-employment psychological testing, including polygraph and other trustworthiness and reliability screening techniques

On-Site Access Authorization Controls

- Perimeter and interior access controls
  - Entry/exit access controls
  - Personnel and vehicle checks/searches/surveillance
- Smart badges/proximity cards
- Biometric controls
- Escort requirements
- 2-person rules/peer checking

Fitness-for-Duty

- Drug and alcohol testing
  - For-cause
  - Post-accident
  - Random
- Behavioral observation programs (BOP) for indications of impairment
- Fitness monitoring programs
- Periodic psychological testing or life stress surveys
- Employee Assistance Programs
- Fatigue management programs
- Medication reporting and evaluation
- Legal action reporting and evaluation

Other Personnel Security Programs

- Behavioral observation programs (BOP) and personnel monitoring
  - Supervisor/worker requirements
  - Escort/visitor requirements

- 2-person rules/peer checking [duplicate]
- Surveillance cameras
- Information system monitoring

- Security culture
  - Awareness/training programs
  - Responsibility assignment ("security is everyone's job")
- Insider threat mitigation programs
- Reporting/self-reporting
  - Suspicious behavior
  - Arrests/legal actions
  - Medications
  - Fatigue
- Personnel security program testing/quality assurance
  - Rotating "Devious Dan" agents (personnel assigned to perform prohibited actions to test and reinforce detection/deterrence measures)
  - Spot checks
  - Red teams (challenge teams)[68]

Pre-Employment Screening Options, Strategies, and Issues during NPP Construction

Throughout this discussion, breakout session participants discussed the pros and cons of grouping workers into categories that reflected their responsibilities and ability to pose either delayed or immediate impact threats. All agreed that to be useful, these groupings could not be too complicated or short-lived/transient. Participants were interested in both the effectiveness and administrative efficiency of the options. Participants made the following points during this discussion:

- Information sharing across sites – Construction workers on NPPs are likely to move from one site to another. The NRC participants reported that during its recent rulemaking, industry had indicated that they were interested in reducing their administrative costs and the burdens on workers by sharing information about workers with access to protected areas at operating facilities. The breakout session participants discussed whether an information-sharing strategy might be appropriate for the construction phase as well, if worker screening was employed for construction workers.
- Verification of identity – Participants agreed that all construction personnel – indeed all personnel accessing the site – should be subject to some form of verification of identity, or at least verification of affiliation with an employer. However, they expressed differing viewpoints about how stringent the identity verification needed to be and whether/under what circumstances it should involve true identity verification via fingerprinting (or some other biometric) as opposed to

[68] Red teams are a group of individuals engaged to take on the role of an adversary and to critique, identify weaknesses, and challenge the strategies or defenses of an organization, proposal, or system in order to identify vulnerabilities and ways to improve those strategies or defenses.

an identification process that relied on documents such as a driver's license or employee picture badge. Participants pointed out that the choice of measures needed to consider legal issues (for example, whether it was legal to require fingerprints), administrative issues (how much of a paperwork and data management burden and cost the measure would entail), privacy issues, and worker acceptability issues. This was particularly true for fingerprinting.[69] Participants raised the question of how other Department of Homeland Security initiatives, such as the REAL-ID (authenticated drivers licenses) and the Transportation Worker Identification Credential (TWIC) will affect the ease of determining an individual's true identity by the time construction is underway for new NPPs. A workshop participant noted that some ethnic or cultural groups, including, for example, some Japanese, object to being fingerprinted, and that a requirement for fingerprinting could raise issues of whether exceptions would be permitted based on personal beliefs, values, or sense of privacy. A number of breakout session participants who were familiar with construction projects that required workers to have security clearances asked whether applicants for on-site NPP construction work were likely to include non-U.S. citizens, whether there would be a U.S. citizenship requirement for any workers, and how that would affect the measures used to assure identity. Questions raised during the discussion included:

- How important is it to know a worker's true identity? What means of identification are appropriate for workers who are only temporarily on site or who are escorted while on site?
- Would a fingerprinting requirement be likely to result in more administrative and privacy costs than it would provide security benefits?
- Does fingerprinting afford an effective means of verifying true identify for non U.S. citizens?
- Would a fingerprinting requirement create issues with workers and their representatives that would affect employee relations?
- Is it possible that using fingerprint biometric access controls (see access authorization below) could reduce arguments against fingerprinting being used in pre-employment screening (both true identity verification and criminal history checks as discussed further down in this list)?
- When thinking about a regulation, might it be useful to require fingerprints for identity and criminal history checks with the expectation that fingerprints may become more useful nationally and internationally in the future (also taking into account that modifying regulations in the future would be difficult and costly)?

[69] The NRC was authorized by Section 149 of the Atomic Energy Act of 1954 to require licensees of utilization facilities licensed under sections 103 or 104b of the AEA to obtain fingerprints of certain individuals. This authority was limited to individuals who were permitted unescorted access to the facility or access to safeguards information under section 147 of the AEA. The Energy Policy Act of 2005 amended Section 149 to extend the fingerprinting and criminal history check requirement to cover individuals who are permitted unescorted access to radioactive material or other property that is subject to NRC regulation and that the Commission determines "to be of such significance as to warrant fingerprinting and background checks." The ability to require fingerprints for non-criminal justice purposes is limited by Department of Justice regulations. Without a valid requirement from a federal agency, licensees are not authorized to require fingerprinting.

- Citizenship requirements – Given the changing nature of the construction workforce, workshop participants questioned whether it was necessary, feasible, and/or desirable to impose a U.S. citizenship requirement on all workers, or on highly specialized critical categories of workers. Some pointed out that experienced NPP construction workers are now in short supply and demand is likely to increase, making measures that further restrict the pool of qualified workers problematic. Workshop participants did not know whether a citizenship requirement was being considered for any or all construction work at NPPs. Questions raised included:
  - Could this requirement result in greater costs than benefits by restricting the pool of experienced NPP construction workers to draw upon and possibly degrading the quality of the construction workforce?
- Terrorist Screening Checks – Department of Defense – Defense Threat Reduction Agency workshop participants confirmed that checks through the federal Terrorist Screening Center (TSC) are worthwhile. They reported that it has helped DOD screen out persons with suspicious connections. In addition, they observed that if an event did occur during NPP construction and an after-the-fact investigation revealed workers who were on the TSC suspects list, it would certainly raise questions about NPP security. The disadvantage of TSC screening is that it can result in false positives. Based on this discussion, the participants agreed that TSC screening checks should be considered the minimum character check required for on-site construction workers. Questions raised included:
  - What are the costs associated with false positives and do they outweigh the benefits of the screening check; and
  - If the TSC incorporates fingerprinting in the near future, how much will it reduce false positives?
- Criminal history checks – Some participants argued that a national criminal history check, also referred to as a criminal records check done by the Federal Bureau of Investigation (FBI), using fingerprints is more effective and cost-effective than conducting local criminal history checks based on the job applicant's residences, particularly for construction workers who are likely to have lived in multiple locations. Others argued that the FBI database is incomplete and out of date, missing data from many lower level law enforcement agencies. In their view, checking local records at all places of residence over the appropriate time period gives more valid results. They all agreed that the jurisdictional issues with fingerprinting need further investigation (as discussed above), give the lack of clarity about how the authority to require fingerprinting and criminal record applies during the construction phase. Questions raised include:
  - How effective are fingerprints for conducting criminal history checks if workers are not required to have U.S. citizenship or if the person has lived and worked abroad for extended periods?
  - Do local criminal checks produce information worth the cost of the effort, especially if records from multiple localities need to be checked?
  - Would it be wise to require fingerprints for identity and criminal history checks, given that system improvements and data expansion are expected to

make fingerprinting more useful and regulations are so difficult and slow to modify once they are established?

- Additional background checks – Participants generally considered credit checks a useful, inexpensive, and acceptable way to check on an individual's trustworthiness and reliability and their financial susceptibility to coercion or pressure that was applicable to individuals from many countries. There was general consensus that credit checks would be appropriate for workers with access to information or systems that could make the plant more vulnerable and less safe. Employment, character, and reputation checks and life history checks require more time and effort than credit checks, but participants thought they provided important information about both qualifications and trustworthiness and that they would not be difficult to apply to selected categories of workers, particularly those conducting security- and safety-significant functions. No questions were raised for further investigation. Recommendations included:
  - Conduct credit, employment, character/reputation, and life history checks for workers performing security- and safety-significant functions.
- Pre-employment drug and alcohol testing – There was general consensus that unescorted construction personnel should be subject to pre-employment and for-cause drug and alcohol testing. The only debate was about random drug testing of employees (discussed under fitness for duty below).
- Pre-employment and/or pre-assignment psychological testing – Breakout session participants noted that pre-employment and pre-assignment (post-hiring but before assignment to a particular project or job duty) psychological testing is typically conducted only for a small subset of security- and safety-relevant construction positions. An even smaller group, typically those involving classified or intelligence information or materials, is typically required to pass a polygraph test. The project team members participating in the workshop reported their findings from earlier work that most federal agencies continued to use the Minnesota Multiple-Phase Personality Inventory MMPI-2 for psychological testing, when psychological testing was required. Experts consulted prior to the workshop thought this instrument was more effective in assessing psychological disturbances or tendencies that could affect a person's reliability and judgment than in evaluating honesty and trustworthiness. One expert had indicated that efforts were underway by psychologists working in security-sensitive organizations to modify the tests to improve their utility for workers in security-sensitive positions and their ability to assess honesty and trustworthiness (Kennedy, 2006).

  One workshop participant described scientific content analysis (SCAN) techniques that analyze individuals' statements as an approach that is being developed to serve this purpose (see Driscoll 1994 and Kapardis 2003 for a description of this technique). Participants thought it possible that techniques more effective in assessing trustworthiness than the current psychological tests would be available by the time NPP construction begins and that it was possible that SCAN techniques could become preferable to the polygraph tests some

agencies now use to assess trustworthiness.[70] Questions posed by the workshop participants included:

- ✧ What is the best way to craft a requirement for security-relevant psychological testing given that this is an evolving area?[71]
- ✧ Would it be desirable for any regulatory requirements imposed on CI facilities to allow flexibility to adopt screening techniques that may become available in the future?
- ✧ How likely is it that validated tests for trustworthiness and reliability will be available whose results can be interpreted by a trained security assessor rather than requiring evaluation by appropriately trained licensed psychologists?

The NPP breakout session participants agreed that the pre-employment screening measures applied to either on-site or off-site workers during the construction phase should probably be different for different groups of workers and at different phases of the construction process. The workshop participants termed this a "graded approach."[72] The breakout session participants from the NRC described NRC's use of "safety- and security-relevant structures, systems, and components (SSR-SSCs)" as a way to categorize aspects of an NPP that reflects their potential to affect safety and security. As a starting point for considering whether and which pre-employment screening measures would be appropriate, the breakout session participants suggested the following on-site groupings of workers:

1. General laborers and crafts-workers
2. Specialized technicians not working on or having access to SSR-SSCs
3. Supervisors of workers who do not have access to or perform activities that involve safety- or security-related structures, systems, and components (SSR-SSCs)
4. Workers working on or with access to SSR-SSCs
5. Supervisors for SSR-SSC-related activities/workers; QA/QC personnel (those conducting inspections, tests, analyses, and acceptance criteria (ITAAC) programs); security guards; and access authorization(AA) and fitness for duty (FFD) program personnel (including off-site contractors/suppliers)

They recommended that the groupings should be as few and simple as was consistent with achieving the appropriate level of security. Several participants emphasized that it was important to remember that pre-employment screening and personnel security requirements overall were only one of the set of protective measures that could be used to achieve security goals. Participants suggested that pre-employment screening for off-

[70] See Shearer (1999) for a discussion of this type of technique.

[71] It was noted that the NRC's regulatory process for fitness for duty precludes requiring the licensee to demonstrate that they employ best practices, thus making it challenging to determine how evolving technologies and standards can best be taken into account.

[72] In this discussion, a graded approach meant an approach in which protective measures are added or removed, applied to or removed from individuals, areas, or tasks, or made more or less stringent to address different threat levels. Grading can be temporal, spatial, and/or task-based.

site construction workers might therefore also apply a graded approach. It could focus on contractors/suppliers and workers involved in or with access to SSR-SSC-related jobs, supplemented with consideration of other aspects of the off-site work that might affect potential threat levels or vulnerabilities, for example, the nature of the transportation routes or the security-reputation of those along the supply chain.

Access Authorization Options, Strategies, and Issues during NPP Construction

The NRC staff at the TISP workshop indicated that the NRC has also been working with its stakeholders to develop access authorization requirements for NPPs during construction and that, consistent with its overall regulatory strategy, it was considering whether a graded approach was appropriate. The breakout session discussion focused on consideration of:

- Perimeter and internal (within the site) access controls – Breakout session participants reported that perimeter access controls for NPPs tend to be covered in physical security plans and physical protection programs as part of the defense-in-depth strategy. However, these security programs are typically not required to be in place until the construction phase is nearly complete. Workshop participants generally agreed that perimeter controls should apply to all workers at shared sites and should be applied to all individuals and vehicles entering and leaving separate/greenfield sites.[73]

  The workshop discussions focused on perimeter and internal access controls for separate/greenfield sites. The NRC participants reported that a key stakeholder, the Nuclear Energy Institute (NEI) that represents the nuclear industry in many policy-related activities, is proposing to create internal "controlled areas" within the construction site once activities involving SSR-SSCs commence at NPPs under construction. These controlled areas would enclose the SSR-SSCs and would be subject to separate access controls. The workers within these areas would be subject to greater surveillance and oversight, and perhaps pre-access authorization screening. Also, there was general consensus in the discussion that access to activities involving SSR-SSCs during the NPP construction phase by off-site contractor or supplier personnel should be controlled. During the discussion, participants raised the issue of cyber-security as an important security consideration. The NRC staff at the workshop reported that the NRC and its stakeholders were devoting considerable attention to cyber-security and remote access. Participants also noted that behavioral observation, peer-checking, and supervisory oversight were important elements in assuring that workers with access to the site were not engaging in problematic behaviors. Time constraints prevented detailed discussion of these options.

  - The questions posed during this discussion included:
  - Is the strategy of establishing controlled areas to set off areas within the construction site in which SSR-SSC work is being done sufficient to adequately reduce delayed impact threats? Would the restrictions apply to all

[73] A shared site is a construction site at which an operating facility is already present and the facility under construction is being built proximate to or interspersed within the operating facility (which applies access controls). A separate/greenfield site is a construction site on which the facility under construction is the only, or first facility, i.e., without an existing operating facility of the same type.

workers accessing these areas, or only to those actually engaged in SSR-SSC tasks?

- ✧ Is it possible for on-site construction workers who are not authorized to access the controlled areas to obtain information that creates a security threat and, if so, could information security controls during the construction phase mitigate this vulnerability?
- ✧ Should access to off-site locations where safety- and security-related SSCs are being developed/built be examined as a potential security concern?
- ✧ Should exit as well as entry controls be considered for controlled areas?
- ✧ Are entry/exit guards needed?
- ✧ Is there a need to have more secure verification of access authorization, such as smart cards or biometric controls?
- ✧ Is it possible that using fingerprint biometric access controls could reduce arguments against fingerprinting being used in pre-employment screening (both for true identity verification and criminal history checks, as discussed earlier)?

Fitness-For-Duty Options, Strategies, and Issues during NPP Construction

In the discussions of fitness-for-duty options as potential protective measures for security during the construction phase of NPPs and other CI facilities, a number of the workshop participants commented that, in their experience, security programs tended to focus on preventing intentional threats. Consequently, they noted that fitness-for-duty programs and measures designed to prevent or reduce unintentional threats, such as those caused by worker impairment from drug or alcohol abuse or fatigue, were often categorized as components of safety or management programs rather than as aspects of a comprehensive security program. Consequently many security experts would not consider themselves experts on fitness for duty measures except in considering workers' vulnerabilities to coercion or bribery as a consequence of drug or alcohol use/abuse. However, when considering the role that inattention or errors could have on security, the workshop participants generally agreed that measures to assure workers' fitness for duty would play an important role in assuring security and therefore warranted consideration as protective security measures. The breakout session discussions about fitness-for-duty options and strategies focused primarily on the following issues.

- ➢ Drug and alcohol testing – The NRC staff in the breakout session on NPPs reported that the NRC had been working with its stakeholders for a number of years to amend its fitness-for-duty rule and that it was preparing to publish its amended rule in 2008. The amended rule will implement a graded approach to fitness-for-duty (FFD) programs and include a requirement for licensees to address FFD issues during NPP construction.[74]

  The workshop participants agreed that for-cause and post-accident drug and alcohol testing would be useful for workers at construction sites. As with pre-employment testing, workshop participants expressed varied opinions about the administrative feasibility and cost-effectiveness of random testing of the entire construction work force. Some cited the short duration and rapid turnover of

[74] The revised Fitness for Duty Rule (10 CFR Part 26) was published in March, 2008 (see 73 *FR* 16965).

workers at construction sites as barriers to effective random testing. The workshop participants from the NRC explained that Subpart K of the amended FFD rule allows licensees constructing a new NPP to either adopt a drug and alcohol testing program for covered workers that includes random testing or to implement a fitness monitoring program rather than random testing.

The project team participants at the workshop summarized findings from interviews with experts from other CI sectors and review of the literature concerning construction workers' persistently high rates of drug and alcohol use compared to other workers and the growing incidence of drug testing of construction workers in other sectors. They reported that key craft unions have publicly supported drug and alcohol testing of construction workers as a way to reduce workforce injuries.

Questions raised by the breakout session participants included:

- ✧ Would difficulties in implementing random testing at NPP construction sites cause the costs to outweigh the benefits of random testing?
- ✧ How do the effectiveness, costs, and benefits of random testing and fitness monitoring programs compare?

- ➢ Periodic psychological testing/life stress surveys – The NPP breakout session participants generally reiterated their observations about pre-employment psychological testing when considering periodic psychological testing and life stress surveys for workers during construction. They agreed that psychological testing or life stress surveys would typically be applied only to a subset of workers (generally those dealing with classified or other sensitive security information or materials). There was general agreement that few workers during the construction phase of either NPPs or other CI facilities would warrant periodic psychological testing, the potential exceptions being those authorized to use weapons, and those responsible for security, QA/QC, access authorization, or fitness-for-duty programs or systems. However, participants emphasized the importance of effective behavioral observation and supervisory interaction on construction sites to detect and intervene with workers who exhibit erratic behaviors, aggressiveness, or belligerence. A question resulting from this discussion was:
  - ✧ Would life stress surveys be cost-effective for key safety and security - relevant personnel during NPP construction? [Note life stress surveys are not common even for operating NPPs.]
- ➢ Fatigue management –The NRC participants indicated that the NRC is not imposing fatigue management requirements on NPPs during construction in its amended rule. The workshop participants from other sectors indicated that, in their experience, formal fatigue management programs were uncommon for construction projects, but pointed out that managing fatigue among workers is part of overall management responsibility and that cost and schedule pressures during construction can result in long shifts and 7-day work weeks that make fatigue management a genuine management concern.

Other Personnel Security Programs during NPP Construction

Breakout session participants briefly discussed several additional aspects of personnel security, including:

- Fitness Monitoring Programs (FMPs) – The NRC staff explained that Subpart K of the amended FFD rule will allow licensees and other entities to implement a fitness monitoring program rather than conducting random drug and alcohol testing for covered individuals. Breakout session participants were interested in this alternative and discussed whether evidence was available to compare the costs, effectiveness, and benefits of fitness monitoring and random testing. They were also interested in the characteristics of FMPs compared to the behavioral observation programs required by the NRC fitness-for-duty and access authorization rules. Several breakout session participants thought that a FMP might provide greater security benefits than a random drug and alcohol testing program by enabling workers to be better and more aware observers of site activities and by encouraging a security culture. A question posed during this discussion included:
  - Would having a security, as well as safety, oriented FMP be a good practice for all or some additional categories of construction workers (other than security, QA/QC, and FFD/AA personnel who are required to be part of the regular FFD behavioral observation program)?

Information Security Measures

Several of the workshop participants were experts in information security. They emphasized that all sectors of the U.S. economy were finding it necessary to pay more attention to information security as a consequence of the changing use of information technologies and the increased volume and sophistication of threats to information security. In their view, attention to information security during the construction phase of all CI projects, including NPPs, is warranted. They stressed that information security needs to be addressed from the very earliest phases of the life cycle. The reactor design and plant design phases are critical because so many individuals may have access to design information that could be used later to attack or compromise the operating NPP.[75]

Because construction sites tend to be so open, several workshop participants expressed the view that careful consideration should be given to control of electronic or hard-copy documents, such as design specifications and blueprints that could be obtained or viewed by walking around the site. They also recommended that an examination be made of what information and documentation was accessible to whom. In terms of the construction phase, questions raised in the discussion included:

- Would creating interior controlled areas when critical SSC activities begin eliminate the need for information controls prior to that time or for the rest of the site at that time?

[75] Large design/build firms typically do not do routine design in house. Therefore, contractors to the general construction contractor may also be of concern in examining information security issues and needs.

- What information security controls are needed for electronic and hardcopy information?
- What information controls are necessary to prevent individuals from obtaining information by just being free to move about the site?
- What level of specificity is needed in documenting changes and waivers so that a record is available to understand the differences between the plant as designed and as built?
- What information controls need to be applied to which off-site contractors/suppliers?
- To what extent would security be enhanced by parceling work out to different individuals/companies (to limit access to information); what would be the down sides of parceling out work on this basis?

Several of the workshop experts also noted that information management is extremely important to construction projects, including functions such as tracking contract and design changes, waivers, and changes between the design and as-built facility (referred to as "deltas"). They pointed out that the tools used to track and manage this information might need to be subject to access and modification controls. The group decided that these were more safety than security issues and therefore did not discuss them further.

Supply Chain Security Measures

Several workshop participants emphasized again that the supply chain represents a threat pathway that warrants systematic examination. They pointed out that many companies are forming distinct groups to focus on supply chain security and are developing guidance and best practices focused on the supply chain. For most CI facilities, they expressed the opinion that this threat pathway was probably most salient during the construction phase, when so many different goods and materials, as well as persons, are coming onto and exiting the site.

Workshop participants noted that the Department of Homeland Security (DHS) has been encouraging both the public and private sectors to focus greater attention on the supply chain to enhance resilience and thwart potential terrorist attacks. They described a key program in this area, the Custom-Trade Partnership Against Terrorism (C-TPAT),[76] which, like TISP, is a joint government-business initiative to build cooperative relationships that strengthen the U.S. homeland security posture. C-TPAT's focus is overall supply chain and border security. C-TPAT recognizes that U.S. Customs officials can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain – importers, carriers, brokers, warehouse operators and manufacturers. C-TPAT is designed to encourage businesses to ensure the integrity of

[76] See Appendix B, and http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml for a description of C-TPAT. Other related federal initiatives include:

- Technology Asset Protection Association (TAPA) standards;
- New Transportation Security Administration (TSA) requirements establishing a timeline for screening 100% of containers on passenger planes (50% within 18 months; 100% within 3 years);
- Certified Shipper Security Standards.

their security practices and communicate their security guidelines to their business partners within the supply chain. It is a voluntary program that takes a "trust but verify" approach.

Workshop participants familiar with the C-TPAT program described it as emphasizing a risk-based, cost-conscious approach that encourages companies to prioritize their risks and design a supply-chain security program that applies security measures in a graded way. Workshop participants from the aerospace industry indicated that this program has led companies in their sector to make many changes, including dramatically reducing the number of different freight carriers used (from 114 to 14 at one company), and that their evaluation of the programs has concluded that they succeeded in both reducing the company's security risks and generating cost savings. The workshop participants who had been focusing on supply chain security emphasized the potential to identify many cost effective opportunities to improve the security of the supply chain. They emphasized the importance of measures to encourage suppliers to apply adequate security measures at their facilities. Because of the vulnerabilities along the supply chain, they recommended taking possession of parts at the supplier's facility whenever possible in order to verify and control what is put into the containers and ensure that secure shipping containers and transport systems are used. They emphasized that supply chain security is a large, complex problem, particularly for projects such as NPPs, which will be receiving components from many different suppliers located in many different locations. They warned that cost and competitive pressures within the organization will make obtaining the necessary management attention and financial support to implement effective supply chain security programs a constant challenge. Questions posed during this discussion included:

- Could the nuclear industry have gaps in the area of supply chain security during construction?
- Would the industry and the NRC benefit from a systematic examination of security concerns involving the NPP supply chain?

Management Issues and Good Management Measures

Throughout the workshop, the participants with experience planning and implementing security programs emphasized that management commitment and support is essential to effective security programs: Security managers cannot establish effective programs without it, particularly during the construction phase when issues of roles, responsibilities, and timely decision making pose particular challenges. Descriptions of the security programs employed at different facilities led to a discussion of differences between publicly- and privately-owned CIs during construction and the observation by some participants that security managers for public-sector facilities seemed to be more successful than their private-sector counterparts in establishing programs that implemented security best practices.

Several workshop participants emphasized the importance of understanding the roles and responsibilities of the different players in the construction process, particularly the facility owners, the construction manager, contractors, and subcontractors, especially with regard to liability. Several workshop participants pointed out that the owner largely determined the security measures employed during the construction process. However, others noted that under some design-build contracts, the general construction contractor actually owns the site and the facility until the final phase of the construction process

(finish work and punch list), and therefore takes responsibility for risks occurring during construction. In these instances, the general contractors are much more likely to be aware of and concerned with security during construction. However, they would probably pay more attention to immediate impact threats than delayed impact threats, which would be manifest after the facility was operational and therefore difficult to attribute to the contractor. The supply chain experts in the workshop pointed out once again the importance of attention to security regarding subcontractors and off-site suppliers, particularly as modular construction practices increase their role in the construction process.

Several security program managers emphasized that unless security measures are shown to be cost-effective in the very near term, it is difficult to obtain the resources to implement them. They recommended preparing a risk assessment that informed and supported the recommendations concerning security measures, and clearly distinguishing between risk avoidance "must dos" and "best practices" when presenting proposed security plans to management and other stakeholders.

Several workshop participants who were expert in construction management tools and practices discussed the management challenges of large-scale construction projects such as power plants, particularly NPPs. There is widespread agreement in industry and academia that better management tools and practices are needed and that greater attention to "designing for constructability"[77] (i.e., the ability to implement a design as specified) during the early life-cycle phases would reduce problems experienced during construction. Security considerations need to be better incorporated into this design process.

Workshop participants also noted that it was particularly difficult to construct "first-of-a-kind projects," both because of constructability problems and because the construction managers and workers were likely to be inexperienced in at least some of the requirements. The workshop participants identified the following strategies and tools that could improve construction management:

- Design for constructability – construction project manageability begins in the design phase;
- Tools for coordinating and integrating construction processes – a key is ensure that security is addressed as these systems are set up:
  - Web-based project management tools that can be used to manage construction are becoming more reliable and widely used (a well-known example is Buzzsaw);[78]
  - Modular simulation software tools such as Enterprise Resource Planning (ERP) systems (participants noted that, unfortunately, not many of these tools are geared toward construction, though they should be);
  - Information system management and change management tracking tools, such as new technologies for tracking and documenting changes made during construction (deltas);

[77] See for example, Jergeas and Van der Put (2001)

[78] For a sample description of one version of Buzzsaw, see http://www.rand.com/imaginit/1/pdfs/technology/software/Buzzsaw_2pg_ConstMgmt_Final.pdf.

- ✧ Locks, tags, and tracking systems for supply chain components and shipments.

One security expert at the workshop, with experience in the construction of U.S. embassies overseas, emphasized the importance of identifying and managing the key priorities for the specific type of facility being constructed. He noted that some CI facilities, such as embassies, have higher security and lower technical/engineering priorities during than NPPs do. He postulated that this shaped the overall character of the construction project. He observed that, for example, foreign embassy construction is essentially a security project with a construction component, while NPPs are construction projects with very significant engineering and security components.

- ➢ In the next breakout session discussion, workshop participants emphasized that an exchange of information among individuals with different specialties and knowledge is essential to the development of a comprehensive and effective security strategy, but that it is often difficult to achieve this exchange. They recommended forums to raise awareness, discuss issues, and share information about best practices that bring together representatives from:
- ➢ The construction industry as a whole;
- ➢ Those involved in CI construction; and
- ➢ Those involved in NPP construction, specifically.

C.7 Workshop Results: Closing Points

During the closing session, the TISP sponsors emphasized that they had hosted the workshop to promote a better understanding of CI construction security issues in general, and that they were pleased with the effectiveness of using security during NPP construction as a particular case in point to focus the discussion. During the closing full-group discussion, workshop participants made the following closing points:

The Challenges of Developing an Optimal Security Strategy

The workshop participants reiterated that there were many benefits of looking across the life cycle of a facility at the beginning of the planning process to identify security needs and potential strategies for each of the life-cycle phases. They noted that a life-cycle perspective enhanced the ability to evaluate which security measures would be most cost-effective and when in the facility's life cycle they would best be implemented. However, they also noted that implementing this approach thoroughly would require pre-planning, a range of expertise, resources, and clarification of the criteria to be applied. They cautioned that experience has shown that it is difficult to marshal these assets. Nevertheless, workshop participants generally expressed agreement that a systems-based, life-cycle, cost-benefit- informed framework was useful, even if applied only at a conceptual level, because of its value in structuring both analysis and dialogue.

Tailoring the Grading of Construction Site and Supply Chain Security Measures/Programs

The workshop participants voiced agreement with the goal of tailoring protective measures to match variations in threats across workers and over the course of the

construction process, but warned that trade-offs between targeting, implementability, and clarity needed to be carefully considered. Some workshop participants, particularly those with direct experience designing and managing construction-phase security programs emphasized the value of programs and policies that were as uniform and consistent as possible, that reflected the importance of maintaining an acceptable level of security throughout the construction project, and of conveying a clear, strong management commitment to security "from day one." All participants agreed that it was important to consider how workers would perceive the strategy. In addition, they agreed that it was important to avoid imposing unnecessary burdens on workers or costs on owners, but that it was most important to ensure adequate security for the site, the facility, and the workers. They also agreed that the specifics of any project's security strategy would depend on the specific characteristics of the project, the site, and the threat environment. They acknowledged the organizational dynamics involved in deciding whether "best" or "acceptable" practices will be implemented in the construction security efforts.

Integrated Approach to Construction Security

Workshop participants reiterated the benefits an integrated approach that addresses all of the different domains of security (such as personnel security, information security, physical security) and ensures that security is integrated with safety and QA/QC. However, they also pointed out that both regulators, and agencies or companies who are making decisions about their own facilities, face organizational and regulatory challenges that make it difficult to achieve a fully integrated approach.

Performance-Based versus Process-Based Requirements

Workshop participants observed that regulators are being pushed to adopt an outcome- or performance-based approach to regulation but that it can be difficult (and perhaps not fully possible) for security- and safety-oriented regulations to define risk-based performance outcomes that would be compatible with performance based regulation. Therefore, they argued that process-based regulations may be most appropriate for achieving security and safety goals. Several participants pointed out that regulators often have multiple, competing objectives and are subject to many constraints. The NRC participants at the workshop observed that the objective of providing a stable regulatory environment is somewhat at odds with an objective of promoting the use of best practices or current standards.

Best Practices in Security Management

A workshop participant with many years of experience in construction and security management presented a summary of the key elements he had identified as representing best practices in security management. Table C.1 represents a slightly edited version of this presentation, based on the discussion his presentation prompted with workshop participants.

Table C.1 Summary of Security Management Best Practices

Best Practices in Security Management

1. Security risk and needs assessments are conducted to inform risk management and risk acceptance decisions.
2. The facility owner defines risk avoidance in terms of “must do” and “should do” (security driven requirements versus recommended best practices).
3. Allocation of responsibility and liability between the facility owner and the general contractor is clarified at the onset of the project and issues are resolved early.
4. Management commitment to security on the part of both the facility owner and the general contractor is clear and strong.
5. Adequate management skill and attention is focused on security. A CI construction project might need a Project Director (PD) and a Project Security Director (PSD) who reports directly to the PD. The PSD is a facility-owner employee who represents the facility owner and reports directly to an appropriate high-level person on the facility management team.
6. The PD and PSD work together to ensure that project milestones, success criteria, etc., in the project plan take security into account.
7. The PSD develops the security plan and integrates it into the overall project plan to ensure that the two plans mesh.
8. The PSD promotes integration of security into other related areas, such as QA/QC and safety, and ensures that QA/QC and safety programs take security issues into account.
9. Key stakeholders in security and the assets needed to implement the security plan are identified and involved.
10. The security plan clearly articulates and documents objectives, roles and responsibilities, milestones, critical paths, and incentives.
11. The security plan includes a Security Oversight Team (SOT) that includes top-level representation across all relevant domains (QA/QC, safety) as well as a high-level, appropriately-trained security representative from the owner’s security division or contracted by the facility owner.
12. Security is managed and tracked as a project.
13. Security project management assesses and addresses emergent security issues throughout the planning and construction period and implements change management controls.
14. Security management ensures employee security training and awareness and promotes a security culture.

C.8 TISP Workshop Agenda and Materials

INVITATION

THE INFRASTRUCTURE SECURITY PARTNERSHIP
(TISP)

Workshop on
Security during the Construction of Critical Infrastructure

February 7, 2008
8:00 AM – 5:00 PM

Navy League Building
2300 Wilson Blvd., Suite 400
Arlington, VA 22201

BY INVITATION ONLY

Detailed Agenda:

8:00-8:30 Welcome and Introductions

- TISP Introduction and Welcome (Perry Fowler)
- Participant Introductions

8:30-9:00 Workshop Rationale, Objectives and Framework

- Rationale
  - Basis of Concern
    - Post 9/11 Changes in Construction Security Concerns
    - Changes in Construction Security Concerns (from theft, vandalism, fraud to major sabotage and terrorist attacks)
  - Nature of Concern
    - When Threats to Private CI become a Public Concern
    - When Threats Constitute a Regulatory Concern
  - Types of CI having Potential Construction Security Concerns
    - Nuclear Power Plants (NPPs); Other Energy (Oil/Gas/Power Grid); Chemical Plants; Transportation Infrastructure (airports, seaports, roadways, bridges, tunnels); Telecommunications and other Critical Communication Infrastructure; Water Supply; Dams; Public Health; Emergency Response Infrastructure; Critical Software Systems; Key Government Buildings; Others?
- Objectives
  - Expert Opinion Regarding Credible Threats and Pathways (external, internal, collusions)
  - Expert Opinion Regarding Best Protection Strategies/Practices (degree of consensus/ disagreement)
  - Expert Identification of Potential Implementation Issues/Obstacles
  - Expert Opinion Regarding Areas that Need Further Examination
- Basic Framework
  - Life-Cycle Approach to Security
  - Systems-Based Approach
  - Cost/Benefit Approach
- Workshop Process
  - Characterizing the Construction Security Threat
  - Assessing Threats during the Construction Phase
  - Designing an Optimal Construction Security Solution
  - Identifying the Appropriate Set of Protection Measures

9:00-9:15 Break

9:15-10:00 Characterizing Security Threats and Vulnerabilities during Construction

- Expert Discussion to Identify Threats of Potential Concern—Are There Credible Security Threats and Vulnerabilities Associated with Construction?

- ✧ Expert Opinion regarding Best Threat Characterization Methodology
- ✧ Threat Characterization (Desirability/ Vulnerability)
  - ◆ Immediate versus Delayed Impact Threats
  - ◆ Types of Threats
    - o What
      - ▪ Compromised Safety Systems
      - ▪ Compromised Security Infrastructure (such as CCTV blind spots, cloned electronic access, compromised alarm systems)
      - ▪ Critical Information (information that could inform later attack)
      - ▪ Other Vulnerable or Critical Systems, Utilities, or Structures (HVAC, electrical, structural integrity, etc.)
    - o How
      - ▪ Cyber-Security Easter Eggs or Other Malware
      - ▪ Hidden Explosives
      - ▪ Compromising Construction Materials
      - ▪ Hidden Surveillance Devices
      - ▪ Hiding/Storing Other Types of Materials That May be of Use Later
      - ▪ Delayed Biocontamination (such as in HVAC)
  - ◆ Threat Pathways
    - o External Threats
      - ▪ Supply Chain Threats
      - ▪ Others
    - o Insider Threats
    - o Insider/Outsider Collusion
  - ◆ Threat Consequences/Impacts
    - o Economic
    - o Public Health and Safety
    - o National Security
    - o Social/Political (Public Confidence)

➢

10:00-11:00 Breakout Groups—Experts Apply Methodology to Identify Credible Threats and Threat Pathways for a Selected CI and for NPPs

➢

11:00-12:00 Working Lunch: Report Back from Breakout Groups and Discussion

➢

12:00-2:15 Designing Optimal Protection Strategy

- ➢ Expert Discussion to Identify What is Needed to Address these Threats, If Anything
  - ✧ Expert Discussion of Methodological Approaches
  - ✧ Do Typical Construction Practices Sufficiently Address the Threats?

- ✧ What May be Needed?
  - ◆ Overall Security Characterization
    - o Pre-Construction Design Security
    - o Supply Chain Security
    - o Cyber Security
    - o Physical Security
    - o Personnel Security
    - o Information Security
    - o Security Oversight/Inspections
    - o QA/QC and Safety Interfaces
    - o Others
  - ◆ Presentation and Discussion of Key Protection Strategies Impacting Construction Security (with breaks between presentations as time permits)
    - o Pre-construction Design Security (15 min) – Mike Garcia (DHS)
    - o Supply Chain Security (15 min) – Ken Konigsmark (Boeing, head of supply chain security
    - o Cyber Security (15 min) – Group discussion, led by DTRA participants
    - o Information Security (15 min) – Group discussion
    - o Physical Security (15 min) – Group discussion
    - o Personnel Security (20 min) – Kristi Branch (PNNL)
    - o Inspection and Detection Security Oversight – such as explosive detection (10 min) – Berne Indahl (ex State Department, Embassy Security)

➢

2:15-3:00 Breakout Groups—Experts Apply Methodology to Assess Effectiveness of Various Protection Measures and to Identify Optimal Protection Strategy for Selected CI and for NPPs

➢

3:00-3:45 Report Back from Breakout Groups

➢

3:45-5:00 Conclusions about Security during Construction of Critical Infrastructure

- ➢ Areas of Agreement (methodologies, threat reduction priorities, optimal set of security measures, importance of various security measures, best practices)
- ➢ Outstanding Issues/Unanswered Questions
- ➢ How NRC Can Ensure Adequate Protection (Berne Indahl leads discussion)
- ➢ Recommended Next Steps

TISP CI Construction Security Workshop Participants

➢

Host: Perry Fowler (TISP)

Invited Organizers:
Kate Baker (PNNL)
Kristi Branch (PNNL)
Niav Hughes (NRC)
Val Barnes (NRC)—not able to attend

Invited Participants (ordered by affiliation):
Marla Dalton (TISP)
Mike Burrell (NRC)—not able to attend
Julius Persensky (NRC)
Scott Morris (NRC)
Ralph Way (NRC)—not able to attend
Roberta Warren (NRC)
Amanda Nerret (NRC)
James Fisicaro (Nuclear Energy Institute)—not able to attend
William Dexter Beard (DOE, Y-12 facility)—not able to attend
Mchael Garcia (DHS—served as liaison to NRC)
Berne Indahl (Boeing, Dept of State)
Ken Konigsmark (Boeing, Head of supply chain security)
Vernon Rhodes (DISA, Antiterrorism Officer)
Kevin Skymes (KBR)
Marion Andrews (DTRA)
Thomas Bucklew (DTRA)
Ira Brown (DTRA)
Roland Ferrera (AMEC)
Ken Oscar (Fluor)—not able to attend
Diane Homes (Fluor)
Richard Captain (Bechtel)
Richard Graves (KBR)
Christopher Raddel (Parsons)
Roger Jordan (ACEC)
Miroslaw Skibniewski (University of Maryland)
Gerald Galloway (University of Maryland)
Ed Hecker (USACE)

Breakout Session Objectives

Bring experts together across key domains to:

- Systematically assess, prioritize, and address threats associated with CI construction.
- Discuss ways to promote effectiveness and efficiency in addressing the issue of CI construction security.
- Identify ways to prevent arbitrary decision-making and requirements that might be imposed without taking a systematic life-cycle, systems-based approach

Breakout Session 1: Focus on Threats and Threat Pathways

Breakout Session 2: Focus on Protection Measures and Strategies

Breakout Session 1: Threat Assessment

*Experts Apply Methodology to Identify and Assess Credible Threats and Threat Pathways during the **Construction Phase** for a Selected CI and for NPPs*

Methodology for Threat Analysis:

- Identify all the possible threats during the construction phase
- For each threat determine the possible threat pathways
- For each threat pathway assess risks and vulnerabilities (threat consequences X ease of perpetuating the threat)

Questions:

1. What are the possible threats during construction (immediate and delayed impact threats)?
   - Hidden explosives
   - Hidden surveillance devices
   - Hiding/storing other types of materials that may be of use later
   - Delayed biocontamination (such as in HVAC)
   - Compromised critical systems
   - Built-in weaknesses in security system
   - Compromised materials
   - Obtaining critical information
   - Sabotage
   - Fraud/Theft/Crime
   - Blundering & ineptitude
2. What are the potential impacts of each of these threats?
3. What are the possible threat pathways for each threat?
   - Who (insiders, outsiders, collusion)
   - Where (systems, components, materials, information on site or during supply chain)
   - When (when in supply chain or when during construction life cycle)
4. What are the key vulnerabilities for each pathway?
5. What are the threat reduction priorities (consequences x probability)
   - Threat consequences (worst case scenarios)
   - Ease of perpetrating the threat

Breakout Session 2: Protection Analysis

Experts Apply Methodology to Assess Effectiveness of Various Protection Measures and to Identify Optimal Protection Strategy to Address Threats ***during Construction*** *of Selected CI and NPPs*

Methodology for Protection Analysis:

- For each pathway determine optimal cost/benefit protection strategy based on life-cycle, system-based approach
- Identify protection measures that work across multiple pathways and eliminate any measures that become superfluous
- Reassess optimal protection strategy from life-cycle and systems-based approach

Questions:

6. What can be done to prevent/mitigate construction security threats (as prioritized in breakout 1) from a systems perspective?
   - Beyond Construction Practices:
     - Design
     - Siting
     - Supply Chain (ensuring materials, components, systems are not compromised before coming onto the site)
     - Workforce Pool (shared industry processes to select/screen workers before allowing construction site access)
   - Construction Practices
     - Entry/exit searches
     - On-site inspections/testing
     - On-site surveillance/oversight
7. For construction protection measures, when in the construction life cycle would these be introduced? (when, where, scope)?
8. What measures are most effective and efficient?
9. What are the priority measures and optimal protection strategies?

Issues to Consider:

- Are typical design, supply chain, workforce screening, and construction practices (security/safety/QA/QC) sufficient to address these threats?

- How much benefit is gained by screening, observing, and testing workers that come onto the construction site if supply chain workers are not similarly screened, observed, and tested?
- Can threat pathways associated with the supply chain be effectively addressed in ways that do not require these personnel security measures? (i.e., “trusted computing technologies” vs trustworthy persons)

Table C.1 provides a preliminary list of possible protective measures to use as a starting point for this discussion.

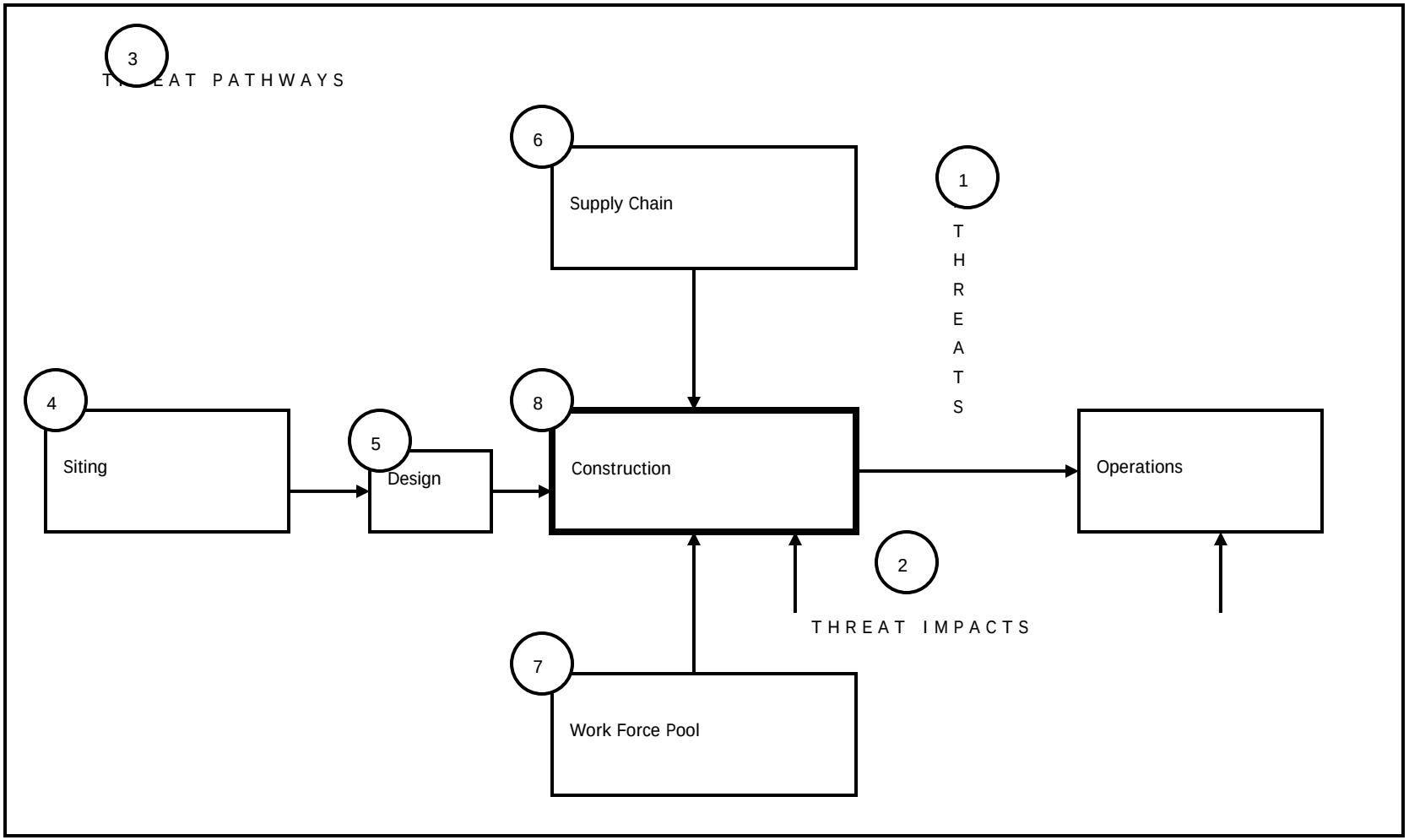


Figure C.5. Plant Construction Life cycle

Breakout Session 1: Address 1, 2, 3 ➔Prioritize threats and vulnerabilities that need to be addressed

Breakout Session 2: Address 4, 5, 6, 7, 8 ➔ID key protection measures and optimal protection strategies

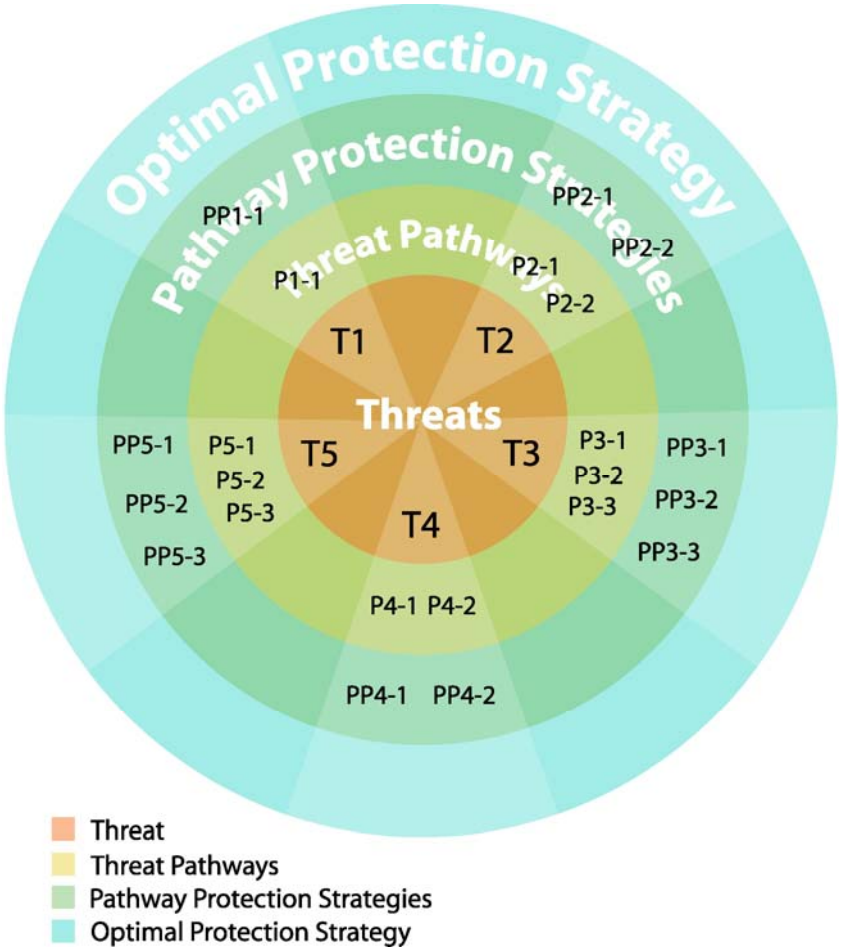


Figure C.6. Assessment Process

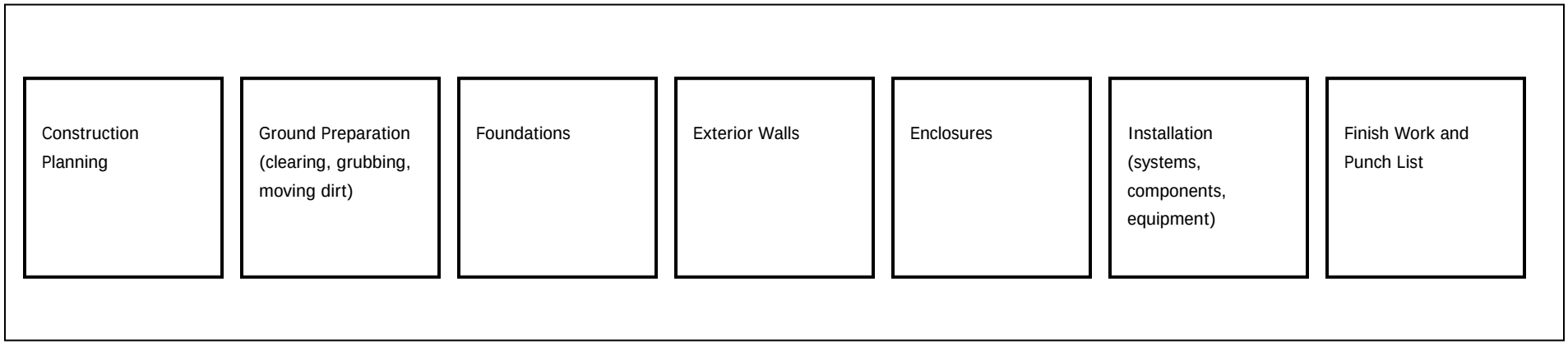


Figure C.7 Plant Construction Life Cycle

Table C.2 List of Possible Protection Measures

Table C.2 Possible Protection Measures
Possible Pre-construction Supply Chain Protection Measures (materials, components, software systems): ➢ Greater security-oriented specifications in vendor contracts ➢ Vendor background checks and assessments ➢ Personnel security requirements for key vendors & off-site contractors ➢ Spot checks of vendors ➢ Having owner oversight personnel located at vendor sites ➢ Built-in software protections & code alteration detection capabilities ➢ Certified and tracked chain of custody ➢ Tamper proof containers/packaging ➢ Others?
Possible Pre-construction Plant Design Protection Measures: ➢ Increase standoff ➢ Maximize physical protective barriers ➢ Increase structural integrity and resiliency (load issues, etc) ➢ Decrease collateral damage (types of materials, windows, etc. ➢ Enhance fire resistance ➢ Improve emergency egress and access ➢ Facilitate security response ➢ Enhance resiliency if a critical system fails ➢ Maximize the ability to isolate compromised/damaged components to minimize the downtime (and costs) of recovery ➢ Separate design drawing responsibilities across multiple subcontractors ➢ Others?
Possible Protection Measures to Address during Construction Planning and Issuing Contract Requirements: ➢ Additional security specifications in construction contracts with clear enforcement/incentive measures ➢ Security liability agreements ➢ Good risk management planning ➢ Life-cycle perspective ➢ Others?

Table C.2 Possible Protection Measures
Possible Protection Measures Pertaining to Management/Employee Involvement ➢ Have owner staff on construction management team ➢ Good labor/union relations ➢ Strong security culture & awareness/training programs ➢ Broad scope behavioral observation program that includes security ➢ Others?
Possible Physical Security Protection Measures ➢ Intrusion detection (alarms/security seals/tampering indicating devices) ➢ Cooperative agreements with local/federal law enforcement agencies ➢ Others?
Possible Personnel Security Protection Measures ➢ Biometric access controls ➢ Identity verification ➢ Background checks ➢ US citizen requirements ➢ Local crime checks ➢ Fingerprinting & national crime check ➢ Terrorist Screening (TSC) ➢ Pre-employment psychological testing ➢ Pre-employment drug testing ➢ For-cause drug testing ➢ Random drug testing ➢ Behavioral observation program that includes security ➢ Escort program ➢ Higher supervisor/worker ratios ➢ Others?

Table C.2 Possible Protection Measures
Possible Surveillance/Searches/Inspections Protection Measures ➢ Surveillance cameras ➢ Undercover security agents (also see “Devious Dan” program in Other) ➢ Roving security patrols ➢ Periodic searches for explosives, including use of dogs ➢ Perimeter entry/exit searches ➢ Security walk downs/spot checks ➢ Chain-of-custody requirements ➢ Security-informed QA/QC ➢ Security-oriented material/component inspection & testing of all key components ➢ X-raying, scanning, sniffing key components ➢ Red team security inspections ➢ Others?
Possible Information Security Protection Measures ➢ Divide and fragment work ➢ Control copying and distribution of documents ➢ Others?
Possible Cyber Security Protection Measures ➢ Supervisory control and data acquisition (SCADA) procedures ➢ 2 person rule for software administrators ➢ Others?