**U.S. Department of Commerce**
**Technology Administration**
National Institute of Standards and Technology

**Office of Applied Economics**
**Building and Fire Research Laboratory**
Gaithersburg, Maryland 20899

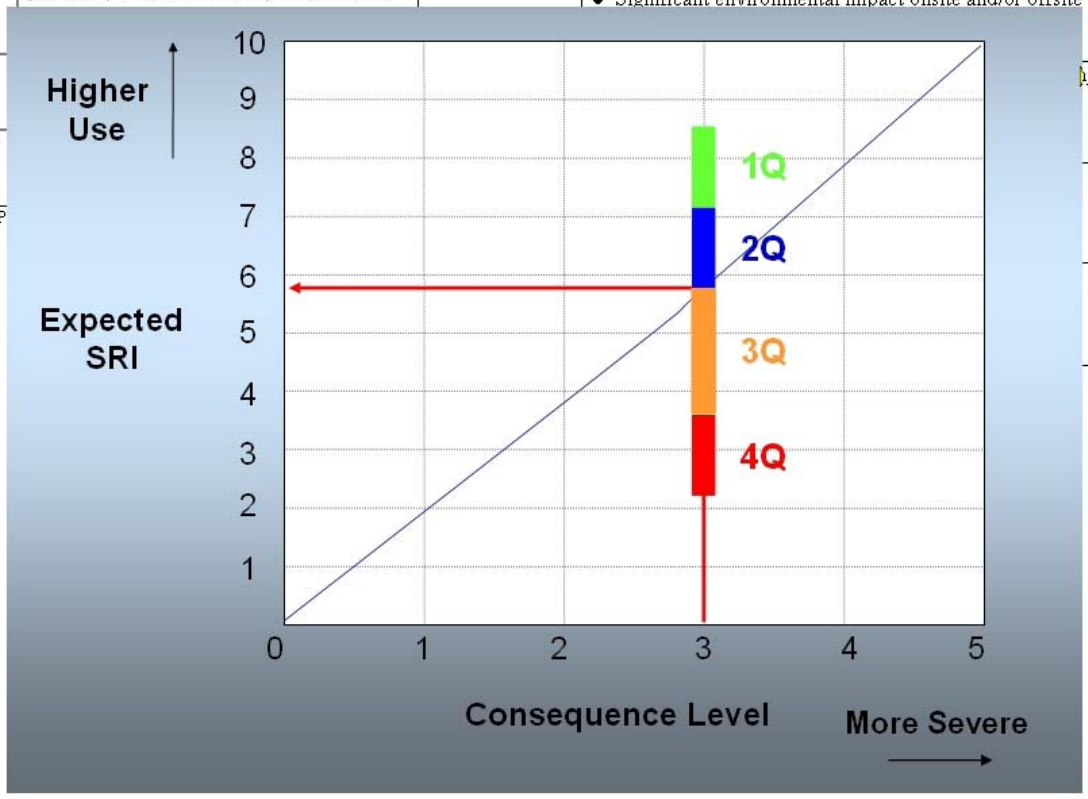
# Best Practices for Project Security

Stephen R. Thomas, Jonathan R. Sylvie, Candace L. Macken

| Threat Rating | Description |
|---|---|
| 5 - Very High | Indicates that a ***definite*** threat exists against the asset and that the adversary has both the capability and i attack or commit a criminal act, and that th assets are targeted on a frequently recurrin |
| 4 - High | Indicates that a ***credible*** threat exists again knowledge of the adversary's capability ar commit a criminal act against the asset, ba incidents having taken place at similar asse situations. |
| 3 - Medium | Indicates that there is a ***possible*** threat to th adversary's desire to compromise similar a possibility that the adversary could obtain |
| 2 - Low | |
| 1 - Very Low | |

Adapted from AP

| Consequence Category | Description |
|---|---|
| 5 – Very Severe | • Possibility of any offsite fatalities; possibility for multiple onsite fatalities<br>• Extensive environmental impact onsite and/or offsite<br>• Extensive property damage<br>• Very long term business interruption/expense |
| 4 – Severe | • Possibility of any offsite injuries; possibility for onsite fatalities<br>• Significant environmental impact onsite and/or offsite |



NIST GCR 04-865

**U.S. Department of Commerce**
**Technology Administration**
National Institute of Standards and Technology

**Office of Applied Economics**
**Building and Fire Research Laboratory**
Gaithersburg, Maryland 20899-8603

# Best Practices for Project Security

Stephen R. Thomas, Jonathan R. Sylvie, Candace L. Macken
Construction Industry Institute
3925 West Braker Lane
Austin, TX 78759-5316

Prepared For:
Robert E. Chapman
Office of Applied Economics
Building and Fire Research Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8603

Under Contract SB1341-02-W-1481

**July 2004**


**U.S. DEPARTMENT OF COMMERCE**
Donald L. Evans, Secretary

**TECHNOLOGY ADMINISTRATION**
Philip J. Bond, Under Secretary for Technology

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
Arden L. Bement, Jr., Director

## *Foreword*

The National Institute of Standards and Technology (NIST) develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life. In the aftermath of the attacks of September 11, 2001, NIST has taken a key role in enhancing the nation's homeland security. Through projects spanning a wide range of research areas, NIST is helping millions of individuals in law enforcement, the military, emergency services, information technology, the construction industry, and other areas protect the American public from terrorist threats.

NIST's Building and Fire Research Laboratory (BFRL) has as its mission to meet the measurement and standards needs of the building and fire safety communities. A key element of that mission is BFRL's commitment to homeland security. Specifically, the goal of BFRL's homeland security effort is to develop and implement the standards, technology, and practices needed for cost-effective improvements to the safety and security of buildings and building occupants, including evacuation, emergency response procedures, and threat mitigation. The strategy to meet this goal is supported by BFRL's:

- research and development (R&D) program to provide a technical foundation that supports improvements to building and fire codes, standards, and practices that reduce the impact of extreme threats to the safety of buildings, their occupants and emergency responders; and

- dissemination and technical assistance program (DTAP) to engage leaders of the construction and building community in implementing proposed changes to practices, standards, and codes. DTAP will also provide practical guidance and tools to better prepare facility owners, contractors, architects, engineers, emergency responders, and regulatory authorities to respond to future disasters.

This report, prepared for NIST by the Construction Industry Institute (CII), was funded by DTAP. It provides guidance for implementing security-related practices during the delivery process of chemical manufacturing and energy production and distribution projects. By focusing on the project delivery process—planning through start-up—this research increases the likelihood that cost-effective protective measures will be implemented. Furthermore, CII's research indicates that the security-related practices described in this report, if implemented, will enhance facility security throughout its life cycle. Finally, the report develops a Security Rating Index (SRI). The SRI provides a quantitative means for determining the level of use of security-related practices and for assessing their impacts on key project outcomes—cost, schedule, and safety. Understanding these impacts should lead to a management philosophy which fully integrates security into the project delivery process.

The material presented in this report complements research being conducted by the Office of Applied Economics (OAE) under BFRL's homeland security R&D program. OAE's research focuses on developing economic tools to aid facility owners and managers in the selection of cost-effective strategies that respond to natural and man-

made hazards. OAE's research has produced a three-step protocol for developing a risk mitigation plan for optimizing protection of constructed facilities. This protocol helps decision makers assess the risk of their facility to damages from natural and man-made hazards; identify engineering, management, and financial strategies for abating the risk of damages; and use standardized economic evaluation methods to select the most cost-effective combination of risk mitigation strategies to protect their facility. This report covers key components of the first two steps of the three-step protocol.

Robert E. Chapman
Office of Applied Economics
Building and Fire Research Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8603

## *Abstract*

This research, sponsored by the National Institute of Standards and Technology (NIST), was a first step in establishing security-related best practices with respect to the delivery of capital facility projects for the heavy industrial sector. Capitalizing on the expertise and knowledge base of the Construction Industry Institute (CII), its purpose was to develop security best practices for implementation during the project phases of planning through start-up to enhance facility security throughout its life cycle.

Two teams of industry experts were assembled; a Steering Team to guide the effort and a Practice Develop Team to develop the best practices. To better ensure a comprehensive solution, CII's library of best practices for project delivery was evaluated by the Practice Development Team to determine which practices were most appropriate for security enhancements. The evaluation and use of proven practices for project delivery offered a structured approach for examining the project delivery process and identifying specific security requirements. Six of the 26 practices, pre-project planning, alignment, constructability, design effectiveness, materials management, and planning for startup, were determined to be applicable. After identifying the essential security practices, these practices were categorized by security elements, physical, personnel, and information security for organization and analysis. The practices were further grouped by project phase to assist with scoring of their use.

The final step involved the development of the Security Rating Index (SRI). The SRI provides a quantitative means for determining the level of use of the practices and for assessing impacts on cost, schedule, and safety. Two key constructs underpinning use of the SRI are consequence ratings, which quantify potential results of a security breach over the facility life cycle and threat ratings, which quantify the intention and capability of an adversary to undertake detrimental actions.

**Keywords**

Best practices; chemical manufacturing; construction; energy production and distribution; facility security; homeland security; industrial facilities; security rating index.

## *Acknowledgements*

The authors wish to thank our industry partners whose valuable contributions made this research possible.

Stretch Dunn, BE&K, Inc.
Jim Porter, E. I. DuPont de Nemours & Co., Inc.
David Syphard, Jacobs Facilities, Inc.
Chuck McGinnis, U.S. Army Corps of Engineers (Retired); Fru-Con, Corp. (Retired);CII (Retired)
Charles Poer, Zachry Construction Company
Michael Spight, Black & Veatch/TRC Companies
John Brady, ConocoPhilips
Michael Hewitt, E. I. DuPont de Nemours & Co., Inc.
Gary Staton, E. I. DuPont de Nemours & Co., Inc.
Jay Toadvine, Fluor Corporation
Walter Lisiewski, Jr., Jacobs Facilities, Inc.

# *Table of Contents*

Disclaimer:

Certain trade names and company products are mentioned in the text in order to adequately specify the technical procedures used. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

## *List of Tables*

## *List of Figures*

# *1. INTRODUCTION*

The impetus for this study, funded by the Demonstration and Technical Assistance Program of the Building and Fire Research Laboratory (BFRL) at the National Institute of Standards and Technology (NIST), was the recognized need to secure national assets and infrastructure in the wake of the events of September 11, 2001. Since that time, steps have been taken by the Executive Office of Homeland Security and the Department of Homeland Security to ensure that an event of similar magnitude is unlikely to occur on domestic soil again. However, to the extent that national assets and infrastructure remain as plausible targets, continued efforts must be expended to integrate security into the basic operations of every economic endeavor in the country. This entails a top-down as well as a bottom-up perspective of security.

## 1.1 Security from a National Perspective

The events of September 11, 2001 underscored the need for integrating security into every sector of the national economy. From guarding borders, ports and airports, to protecting critical infrastructure and defending against terror and sabotage, security requires a partnership between the public and private sectors to evaluate and develop systems that will reduce vulnerability to attack. Even though the federal sector has a critical role in spearheading the initiative for enhanced security and decreased vulnerability, it is also driven by the desire to allow the private sector considerable latitude in managing its own endeavors. The goal of ensuring security for the nation as a whole can only be accomplished through this public-private partnership.

The *National Strategy for Homeland Security* (Office of Homeland Security, 2002) lists three strategic objectives necessary to meet the nation's goal of security. These are: prevent terrorist attacks in the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The first falls largely under the provenance of the federal government. One of the traditional roles of government in a market-driven society is to provide goods and services that benefit the public good, like defense, communications, or transportation infrastructure. Such goods and services cannot be provided easily through the market forces of supply and demand because it is difficult to quantify and market the units of goods or services to individual consumers. The second and third objectives, however, cannot be fully achieved without the active participation of the private sector. Among the eight mission critical areas identified in the *National Strategy* is the protection of critical infrastructure and key assets. Some of the private (or quasi-private) sector industries included in this area are water treatment, energy (i.e., oil production and refining, natural gas processing and distribution, and power generation and distribution), chemical manufacturing, and transportation infrastructure. Reducing vulnerability and minimizing damage can be accomplished by private sector initiatives to evaluate and enhance physical, personnel, and information security during project delivery, thus improving project security through the project life cycle. The aim of physical security is to deter, detect, and delay malicious acts through systems and architectural features. Personnel security includes practices and

procedures for screening, hiring, terminating, or addressing workplace issues. Information security is the protection of information systems, including hardware, software, and data, from loss or damage (Center for Chemical Process Safety, 2002).

## 1.2 Security from a Business Perspective

According to the American Academy of Actuaries, the events of September 11 caused the largest insured property/causality (P/C) loss ever recorded, estimated to be in the range of $30-$70 billion, pre-tax (American Academy of Actuaries, 2002). While trend analyses showed that P/C rates had been steadily increasing from around fall 1998 to fall 2001, the events of September 11 prompted most major reinsurers to exclude or substantially decrease terrorism coverage in commercial insurance policies resulting in a shifting of the exposure to risk from reinsurers and direct insurers to companies themselves as out-of-pocket costs. Faced with increased risk exposure and costs, companies have begun to change business and financial policies to ones that limit expansion or new development, possibly impacting the economy as a whole. At particular risk are the construction and real estate industries.

Apart from macro-level, national security interests, attention to security throughout the capital facility life cycle has a bottom line financial impact as well. As the risk of coverage for terrorist attacks is shifted from insurers to companies due to changes in the insurance industry, it behooves companies to keep a security focus in the front-end stages of project execution. A security focus during planning, design, and even construction may yield tangible benefits in eliminating or mitigating the effects of terror or sabotage during the later operation phases of facilities. An eye towards security during the project life cycle can provide a valuable indicator of the need for security enhancements as threats or consequences of terror or sabotage change.

## 1.3 Purpose and Scope

The primary purpose of this study was to identify the best approaches for integrating security into the project delivery process to improve the security of the facility throughout its life cycle. A secondary, though no less important, purpose was to provide a method to assess the impacts of these approaches on key business outcomes like project cost, schedule, and safety performance.

Capitalizing on the expertise and knowledge base of the Construction Industry Institute (CII) with respect to best practices within the construction industry, NIST contracted with CII to develop security best practices and a quantifiable measure of security integration in the capital facilities delivery process, which became known as the Security Rating Index (SRI). To this end, CII convened a series of workshops with industry stakeholders to develop security best practices, and to provide assessment feedback through the creation of the SRI. This report documents the process through which security best practices were identified, the development of the SRI, and suggests how the SRI can be used to assess implementation of security best practices during project planning and execution.

The material presented in this report complements research being conducted by the Office of Applied Economics (OAE) under BFRL's homeland security research and development program. OAE's research focuses on developing economic tools to aid facility owners and mangers in the selection of cost effective strategies that respond to natural and man-made hazards. OAE's research has produced a three-step protocol for developing a risk mitigation plan for optimizing protection of constructed facilities (Chapman and Leng, 2004). This protocol helps decision makers assess the risk of their facility to damages from natural and man-made hazards; identify engineering, management, and financial strategies for abating the risk of damages; and use standardized economic evaluation methods to select the most cost- effective combination of risk mitigation strategies to protect their facility. This report covers key components of the first two steps of the three-step protocol.

Project scope was defined using two of the mission critical areas identified in the *National Strategy:* energy and chemical manufacturing. In the CII database, these are classified as heavy industrial projects. Recognizing that security-related enhancements are less costly and more effective when integrated early in the project life cycle, the scope was further refined to include the following project phases: front end planning, detailed design, procurement, construction, and startup.

# *2. METHODOLOGY*

## 2.1 Establishment of the Steering Team

The Steering Team was formed to frame the methodological approach to developing a security best practice. The Steering Team was composed of industry representatives in policy-making positions within their organizations, the study sponsor, and the principal investigator. Industry representatives were selected to ensure a broad-based industrial perspective from owner and contractor organizations engaged in the engineering, construction, and operation of electrical, oil and gas processing and delivery; and chemical and petrochemical manufacturing. The positions and company affiliations of the Steering Team are shown in Table 1.

Initially, the methodological approach was to convene a series of regional workshops and site visits to learn what steps were being taken within the industry to address security following the events of September 11, 2001 with the intention of developing a standalone security best practice. At the first Steering Team meeting, however, discussion led the team members to conclude that security should be a part of all project best practices rather than a standalone best practice. Furthermore, the Steering Team recognized the opportunity to leverage CII's extensive library of best practices as a foundation upon which security practices could be integrated. This approach would be likely to provide a more comprehensive solution and assist in making the business case to corporate leaders, which would be of key importance in the acceptance and use of security practices. With this in mind, the Steering Team recommended the establishment of a Practice Development Team, staffed by particular practice and subject matter experts who would be responsible for reviewing CII's existing best practices and proposed best practices with the goal of integrating security into them. The Steering Team remained active throughout the study by providing continued guidance to the Practice Development Team and by reviewing the latter team's outputs.

**Table 1. Steering Team Composition**

| NAME | POSITION | COMPANY/ORGANIZATION |
|---|---|---|
| Stretch Dunn | Director of Federal Programs | BE&K, Inc. |
| Steve Thomas | Associate Director | CII |
| Jim Porter | Vice President, Engineering and Operations | E. I. DuPont de Nemours & Co., Inc. |
| David Syphard | Vice President | Jacobs Facilities, Inc. |
| Robert Chapman | Economist | National Institute for Standards and Technology |
| Chuck McGinnis | Director of Civil Works (Retired);<br>Executive Vice President/Chief Operating Officer (Retired);<br>Research Director (Retired) | U.S. Army Corps of Engineers;<br>Fru-Con, Corp.;<br>CII |
| Charles Poer | Business Unit Manager | Zachry Construction Company |

A significant output of the Steering Team was the consensus definition of security that it developed. This definition served to frame the concept of security in the context of this study and to guide the efforts of the Practice Development Team. The definition evolved as the study progressed in response to issues raised by the latter team. In its final form security was defined as:

> *All measures taken to guard against malevolent, intentional acts, both internal and external (e.g., sabotage, crime, and attack), that result in adverse impacts such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and off-site effects (consequences).*

The concern for making a business case for the acceptance of the security best practices is evident in the broad-based definition.

## 2.2 Establishment of the Practice Development Team

The Practice Development Team was charged with reviewing all of CII's existing and proposed best practices, selecting those appropriate for security integration, prioritizing the selected practices, and integrating security. The primary reference document for the review process was the *CII Best Practices Guide for Improving Project Performance* (Construction Industry Institute, 2002). This document provides descriptions of each best practice, a listing of the essential elements, a summary of the benefits of using the best practice, and a checklist for evaluating the degree of implementation. For the review of the proposed best practices the team relied upon the implementation documentation produced by the CII research team that conducted the original research.

Composition of the Practice Development Team was dynamic. A reasonable amount of time was spent on deciding what functional positions should be on the team. Business processes, not security, drove selection of the positions so that the practices that were developed would be more likely to be implemented. The team included security representatives from both owner and contractor organizations due to differing perspectives. Core team members from CII member organizations were selected for their functional expertise managing programs, corporate security, business units, plant operations, and risk. Once the core team selected the practices, subject matter experts were identified. The subject matter experts would meet with the core team as necessary to review their practices. The role of the subject matter experts, academics who were responsible for researching and developing the practice, was to provide a thorough review of the selected practice, to answer any questions that the industry representatives might have had about it, and to help identify security deficiencies. The functions and the company affiliations of the Practice Development Team are listed in Table 2.

**Table 2. Practice Development Team Composition**

| NAME | FUNCTION | COMPANY/ORGANIZATION |
|---|---|---|
| ***CORE TEAM*** | | |
| Michael Spight | Corporate Security Manager | Black & Veatch/TRC Companies |
| Shawn Lee | Analyst | CII |
| John Brady | Corporate Security Manager | ConocoPhilips |
| Michael Hewitt | Plant Operation Manager | E. I. DuPont de Nemours & Co., Inc. |
| Gary Staton | Risk Management Specialist | E. I. DuPont de Nemours & Co., Inc. |
| Jay Toadvine | Program Manager | Fluor Corporation |
| Walter Lisiewski, Jr. | Business Unit Manager | Jacobs Facilities, Inc. |
| Chuck McGinnis | Director of Civil Works (Retired);<br>Executive Vice President/Chief Operating Officer (Retired);<br>Research director (Retired) | U.S. Army Corps of Engineers;<br>Fru-Con, Corp.;<br>CII |
| ***EX-OFFICIO*** | | |
| Steve Thomas | Ex-Officio/Principal Investigator | CII |
| Robert Chapman | Ex-Officio | National Institute for Standards and Technology |
| Ben Matthews | Ex-Officio/ Graduate Research Assistant | U.S. Air Force |
| Jon Sylvie | Ex-Officio/Graduate Research Assistant | U.S. Army |
| Roger Snyder | Ex-Officio/CII Education Committee | U.S. Department of Energy |
| ***SUBJECT MATTER EXPERTS*** | | |
| Lansford Bell | Materials Management | Clemson University |
| Edd Gibson | Pre-Project Planning/Alignment | University of Texas |
| Richard Tucker | Design Effectiveness | University of Texas |
| James O'Connor | Planning for Startup/Constructability | University of Texas |

## 2.3 Review and Selection of the Practices

Twenty-six practices, 11 validated and 15 proposed, were reviewed and discussed to arrive at consensus on the potential impact and applicability that each might have for security. Validated practices have been shown through CII research to provide quantifiable benefits when implemented. Proposed best practices have been thoroughly researched, however, they have not completed the validation process. Impact was framed by a consequence concept: "If security were omitted from this practice, could its omission result in adverse consequences if the facility were attacked?" Applicability was determined after reviewing each of the practice elements included in the *Best Practices* guide and discussing whether the consideration of security was appropriate to the practice. Each practice was rated separately for high or low impact, and high or low applicability.

The practices measuring high on both impact and applicability were selected for a detailed review to determine how security should be integrated into them. Figures 1 and 2 show the results of the selection and prioritization process. Five validated best practices, pre-project planning, alignment, constructability, design effectiveness and materials management, and one proposed best practice, planning for startup, were determined to be high both in impact and applicability.

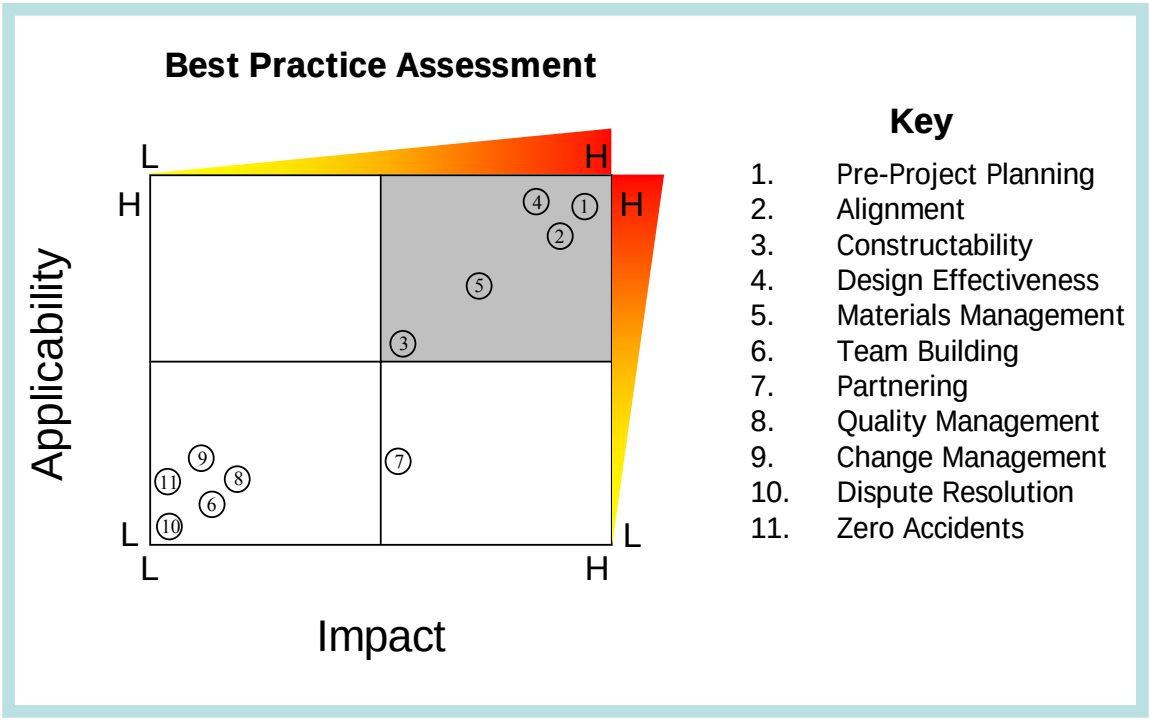



**Figure 1. Selection and Prioritization of Existing Best Practices**

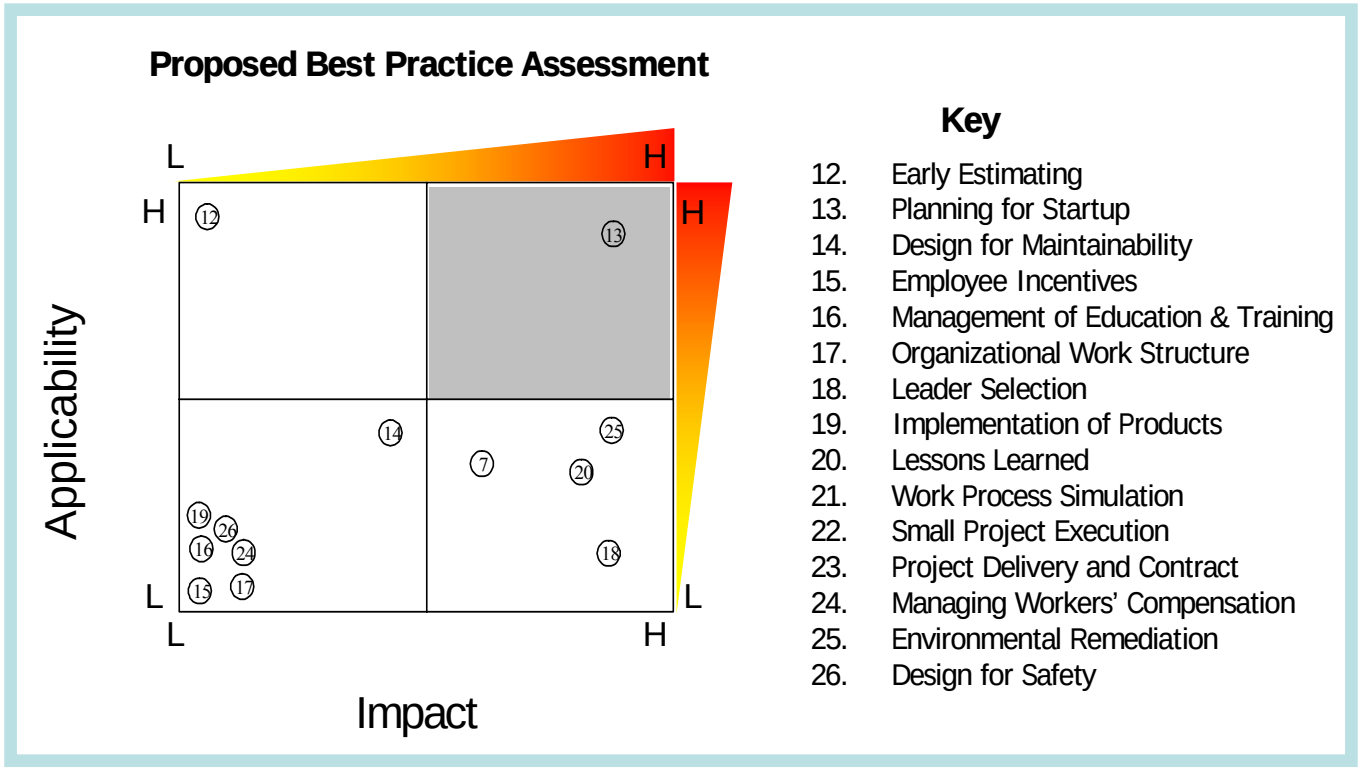



**Figure 2. Selection and Prioritization of Proposed Best Practices**

## 2.4 In-depth Review of the Practices

Once the practices were identified, the Practice Development Team held two meetings per practice. At the first meeting, subject matter experts presented the practice and facilitated discussion to identify in-depth, security-specific additions. The subject matter experts, representatives of the academic community, were members of the research teams that initially researched and documented the practice for CII. During this daylong meeting, a page-by-page walk-through of the documentation was conducted to discuss tools and flow processes. Together the subject matter expert and the Practice Development Team identified additional activities or processes that were needed to integrate security into a given practice. The first half of the second meeting was devoted to a review of all changes from the previous meeting in order to close any gaps and to achieve consensus. During the second half of the meeting subject matter experts presented the next practice for review.

# *3. INTEGRATION OF SECURITY INTO THE PRACTICES*

This chapter provides an overview of the six practices, discusses why security is important in each of the six practices, and provides brief examples of how security was integrated into each of them.

## 3.1 Pre-Project Planning

Pre-project planning, also known as front end loading, front end planning, or early project planning, is essential in developing sufficient information to address risk and to commit resources to maximize the potential for a successful project. Pre-project planning is an owner-driven process that is closely tied to business goals. As such, the integration of security into pre-project planning is essential if security is to be addressed in a cost effective manner.

Pre-project planning is divided into four primary sub-processes. These include:

- Organize for pre-project planning
- Select project alternatives
- Develop a project definition package
- Decide whether to proceed with the project

### 3.1.1 Organize for Pre-Project Planning

Since pre-project planning is a team effort, team makeup is critical to planning and project success. As stakeholders are identified for the project team, a project vulnerability assessment should be used to identify those who are responsible for security-related issues so that they will not be overlooked. The project vulnerability assessment can also provide guidance for the screening of the team for the appropriate level of clearance, as well.

Team members may also form sub-teams that will focus on specifically defined tasks. Among these tasks are risk assessments of environmental, legal, political, technological and security elements in the project; technology assessments; site assessment; and estimated market assessments.

Whether organized as a single project team or sub-teams, the required skill and staffing requirements of teams must be evaluated by the team leader to ensure appropriate staffing. Some of the staffing skills/requirements include business and market evaluation, engineering and construction, environmental, legal, and financial. In addition to these skills, the skills of a security manager or specialist should be added to ensure integration of security and fidelity to the project vulnerability assessment throughout the pre-project planning effort.

Once the team has been organized, a team charter should be drafted. The charter defines the team's mission, responsibilities, accountability, and authority to transform the project concept into a valid approach to project completion. The charter focuses the team on the task at hand, facilitates alignment, and is the basis for communication throughout the pre-project planning process. The charter should address key elements such as, the mission statement, the quality of deliverables, organization charts, reporting requirements, and security requirements.

The next organizational activity is to prepare the pre-project planning plan, which is a formalization and documentation of the methods and resources an owner company can use to operationalize the pre-project planning process. The plan is comprehensive and includes the statement of business need, an outline of known alternatives, a defined schedule and budget for pre-project planning, a contract strategy, and a definition of the tasks necessary for minimizing risk. The risk minimization tasks are also comprehensive and cover areas such as, research, technology, health and safety, and project assessment and security requirements. The pre-project planning plan sets the stage for successful project performance and, ultimately, a more secure facility.

### 3.1.2 Select Project Alternatives

This activity comprises four major functions: analyze technology, evaluate sites, prepare conceptual scopes and estimates, and evaluate alternatives. The selection of alternatives drives many security concerns. Technology and site selection directly affect consequences of security breaches and can make the facility a more attractive target. While many factors must be considered when selecting alternatives, risk analyses and security concerns can be critical and must be criteria for selection. The site vulnerability assessment is an integral part of the analysis when alternatives are selected.

The issues surrounding site objectives and characteristics are lengthy and far too numerous to adequately address here. From a security standpoint, though, analysis of the overall security climate is critical. Some of the major issues to be considered may include background checks as part of the labor analysis.

### 3.1.3 Develop a Project Definition Package

After the decision maker has established the pre-project planning team, evaluated and selected alternatives, the next step is to develop the project definition package. There are five major activities necessary to the development of the project definition package: analyze project risks, document project scope and design, define project execution approach, establish project control guidelines, and compile the project definition package.

The most important part of a risk assessment program may be the risk identification phase. Risk identification relies heavily on the experience and insight of the project team, hence identifying stakeholders for the team is critical. The business risks that require thorough assessment may include market conditions, technology uncertainty,

regulations, and cost, among others. With respect to security, costs must be analyzed on a life cycle cost basis and must address the cost of security throughout the facility life cycle. Such costs can be minimized when they are identified early in pre-project planning.

In documenting project scope and design, the key technical and physical attributes of the project, including general quality requirements and budget, and commercial or security issues that would affect design planning or decision making are described. Although the details of a project definition package are too numerous to discuss in this document, suffice it to say that the package must include a detailed scope of work, document controls, environmental impact statements, a written site vulnerability assessment, and a project procedures manual that includes a project security plan.

A formal execution approach, or project execution plan, is required to ensure that all tasks are identified and carried out in a timely manner. The plan provides overall direction for the project team and serves as a road map to guide the numerous decisions required during the course of a project. It should address every key element that affects how the project will be executed, as well as the procedures and resources that will be required to accomplish project execution.

Establishing project control guidelines is the next activity in developing a project definition package. The purpose of project control is to enable project participants to evaluate project performance against a pre-defined plan and to take corrective action when necessary. The plan serves as a baseline to monitor physical progress and costs, and as background for forecasting future performance based on current trends.

Compiling the project definition package includes assembling the information into both a project definition package and a project authorization package. The project definition package serves as baseline and guidepost to be used during the execution phase of engineering, procurement, and construction. Essential elements of the project definition package include: project objectives and priorities (e.g., purpose for the project, financial objectives, quality requirements, and operability, technology, security, and safety requirements), cost estimate, economic and risk analyses, project alternatives, and future obligations. The project authorization package is an executive summary containing all information necessary for the decision maker to evaluate the viability of the project and to make a go/no go decision on funding. In addition to introducing the proposed project to decision makers, it contains information on background and objectives, alternative solutions, labor requirements, and identification of major risks including health, safety, security and environmental considerations.

### 3.1.4 Project Definition Rating Index (PDRI)

The Project Definition Rating Index (PDRI) (Construction Industry Institute, 1996) is a simple but powerful tool that measures project scope definition for completeness. It consists of three sections that cover the basis of project decision, front end definition, and execution approach.

The Practice Development Team reviewed the 70 elements of the PDRI for industrial projects to identify the elements in which security should be added. Security considerations were deemed to be important in considering the information necessary for understanding project objectives, the process and technical information that should be evaluated to understand project scope, and the elements that should be evaluated to understand the requirements of the execution strategy.

The team proposed 37 updates to the 70 elements. Figure 3 provides a sample of the updates under manufacturing objectives criteria. Security affects reliability philosophy by building in system redundancy, which allows for keeping the system operational should acts of sabotage impair operations. As one of the business objectives, planning that includes security considerations affects the feasibility and affordability of the project by ensuring that operations may continue during periods of elevated threat. Security considerations also affect the complexity of the project, and the attendant trade-offs among cost, schedule, and security must be weighed among the mix of manufacturing objectives. Sample recommended updates are underlined in the figure below.

From Appendix C, Section I, *Project Definition Rating Index (PDRI), Industrial Projects*

**A. MANUFACTURING OBJECTIVES CRITERIA**

**A1. Reliability Philosophy**

A list of the general design principles to be considered to achieve dependable operating performance from the unit. Evaluation criteria should include:

- ❑ Justification of spare equipment
- ❑ Control, alarm, security and safety systems redundancy
- ❑ Extent of providing surge and intermediate storage capacity to permit independent shutdown of portions of the plant
- ❑ Assessment of extra capacity requirement if an area is sabotaged
- ❑ Mechanical / structural integrity of components (metallurgy, seals, types of couplings, bearing selection, etc.)

From Appendix C, Section I

**B. BUSINESS OBJECTIVES**

**B4. Affordability / Feasibility**

Have items that may improve the affordability of the project been considered? These should include incremental cost criteria such as:

- ❑ Consideration of feedstock availability and transport to the job site, especially during periods of elevated threat
- ❑ Performing an analysis of capital and operating cost versus sales and profitability

Results of these studies should be communicated to the project team.

**Figure 3. Sample PDRI Security Updates**

## 3.2 Alignment

In the context of capital projects alignment is defined as the condition where appropriate project participants are working within acceptable tolerances to develop and meet a uniformly defined and understood set of project objectives. These project objectives must meet business or mission requirements, including security, and be consistent with the overall organization's strategy. Alignment is crucial during pre-project planning, but it must also be present throughout the project life cycle. Aligning the team involves developing clearly understood objectives and gaining the commitment to work towards these goals.

The business environment under which projects are planned and executed is increasingly more integrated. Projects are developed using a wide range of relationships including joint ventures, partnerships with government, formal contracts, and associations of companies within the same industry. Mixed in with the formal relationships are the concerns of informal stakeholders such as government regulatory agencies and the public. Increasing attention to the requirements of effective security add to project complexity. As a result, a relatively simple project may have a large number of stakeholders. Obviously those different stakeholders will frequently have conflicting objectives for the same project. Proper alignment involves the communication, negotiation, and compromise required to gain stakeholder commitment to overall project objectives.

### 3.2.1 Critical Alignment Issues

CII literature identifies 10 critical alignment issues that have the greatest effect on team alignment (Construction Industry Institute, 1997). After reviewing these issues, the Practice Development Team proposed security updates to 4 of the issues. The 10 issues are listed below and those with security updates integrated are marked with an asterisk (*).

- Stakeholders are appropriately represented on the project team.*
- Project leadership is defined, effective, and accountable.
- Relative priorities among cost, schedule, safety and required project features are clear.*
- Communication within the team and with stakeholders is open and effective.
- Team meetings are timely and productive.
- Team culture fosters trust, honesty, and shared values.
- Pre-project planning process includes sufficient funding, schedule and scope to meet the project objectives.*
- Reward and recognition system promotes meeting or exceeding project objectives.
- Teamwork and team building programs are effective.
- Planning tools are effectively utilized.*

Stakeholder identification can be critical to security; therefore, the vulnerability assessment should be a factor in the selection of stakeholders for the project team. Alignment on project objectives is essential. The team must be aligned concerning the importance of security issues identified in the project objectives. Priorities among cost, schedule, and required project features must be based on the vulnerability assessment. Planning tools can be most effective for identifying, prioritizing, communicating, reinforcing, and controlling project objectives. The CII Agreement Matrix is such a tool; it quantifies agreement between various project participants and can be used to ensure that team members are in agreement on the importance of security. (Construction Industry Institute, 2003)

## 3.3 Design Effectiveness

Design effectiveness is an all-encompassing term to measure the results of the design effort against the specified expectations of the owner. These expectations include cost, schedule, safety, quality, and other expectations in the project objectives. Security is an essential consideration when the priorities among these expectations are established. Design effectiveness then, is a method by which the design, not the designer, is evaluated (Construction Industry Institute, 2002).

A design cannot be considered to be effective in a post 9/11 environment if it does not adequately address security. Security throughout the project life cycle is directly linked to the activities of the design effort. An effective design must be based on the vulnerability assessment and will thus help decrease security risks.

### 3.3.1 Security as a Design Evaluation Criterion

Even before the increased sensitivity to security, owners and contractors had to consider from the start of conceptual design how capital facilities would be protected from intruders who enter a facility to steal property, obtain secret information, or to commit sabotage (Weiss, 1996). Rather than a single line of defense, a security system should be thought of as protection in-depth, which means consideration of other measures in addition to security guards. Planning and layout of the building and surroundings, perimeter fencing, alarm handling, safeguarding equipment, and key and lock control are also features of a security system that should be considered.

Harrington-Lynn and Pascoe (1995) outlined a risk-based strategy to assess the effectiveness of security measures in the design phase. Such a strategy requires an understanding of:

- the probability of the event occurring
- the effects on the health and safety of the target audience of the crime
- the financial losses occurring due to the event
- the rewards the perpetrators expect from undertaking the crime
- the risks the perpetrators are willing to take in carrying out the crime

- the likely cost and effectiveness of the individual countermeasures

Though at the time the authors considered the risk of high security breaches, i.e., the probability of a terrorist attack, to be small, they asserted that given the type of facility targeted, the risk to health and safety and the financial cost would be catastrophic. In such cases security measures would be worthwhile at any cost.

A useful tool for evaluating whether security is an essential element of the project is the security vulnerability assessment (SVA). The SVA is a process of determining the likelihood of a successful exploitation of vulnerability by an adversary, and evaluating the countermeasures necessary to ensure the security of the project. According to the American Petroleum Institute/National Petrochemical and Refiners Association (2003), an SVA should include the following activities:

- Understanding what critical assets need to be secured
- Identifying threats against assets, evaluating assets in terms of attractiveness, and evaluating consequences if assets are damaged or stolen
- Identifying potential security vulnerabilities
- Determining the likelihood of a successful event and the consequences of an event if it were to occur
- Ranking the risk of the event occurring
- Identifying and evaluating risk mitigation options

Using this process, the results of the SVA can be used to determine whether security should be added as a criterion for measuring design effectiveness.

### 3.3.2 Input Variables and Outcome Parameters

Design is a complex process involving the reconciliation of competing objectives and constraints. Design decisions that are made during the early phases of a project have the greatest influence on the project and the most cost-effective influence on security. These decisions and other constraints form input variables to the design. CII research has identified the 10 input variables having the greatest impact on design effectiveness (Construction Industry Institute, 1987). These include: scope definition, owner profile and participation, project objectives and priorities, pre-project planning, basic design data, designer qualifications and data, designer qualification studies, project manager qualifications, construction input, type of contract, and equipment source. Security should be a consideration to some degree for each of these inputs.

Design effectiveness can be measured by design outcome parameters. Eight parameters identified by CII research include: final project schedule, constructability, quality of design, final project cost, plant start-up, performance, safety, and security. CII has correlated the first 7 of these parameters with the 10 input variables above, and the last parameter was added by the Practice Development Team during the process presented in Chapter 2.

### 3.3.3 Assessing Design Effectiveness

The Practice Development Team recognized that the Project Objectives Matrix offered a suitable means for assessing the effectiveness of the design and that by integrating security into the matrix it could be used as an additional criterion for assessment. The Project Objective Matrix is a multi-criteria decision matrix developed for assessing design effectiveness (Construction Industry Institute, 1986). Although specific criteria used for evaluation may vary from project to project, Figure 4 provides a typical example matrix. The criteria should include only those elements that directly impact attainment of project objectives. The criteria included in Figure 4 are defined below:

- Accuracy of Design Documents - Because specifications and drawings are the most readily identifiable products of a design, they are of major importance in a measure of design effectiveness. This criterion addresses design effectiveness by measuring the frequency and impact of changes in the drawings and specifications.

- Usability of Design Documents - This criterion determines the ease of use of the design documents by construction forces, and relates to the completeness and clarity of the drawings and specifications.

- Cost of Design - The cost of the design can be quantified by the cost effectiveness of the design activities compared to original (plus approved changes) budgeted amounts and overall project costs.

- Constructability - Constructability is the optimum use of construction knowledge and experience in planning, engineering, procurement, and field operations to achieve overall project objectives. Implementation of a planned constructability program helps to optimize project costs by successfully integrating construction knowledge into design engineering.

- Economy of Design - The economy of design criterion relates to overdesign or inefficient design. A poor physical layout of the facility can be an indication of inefficient design. This criterion is extremely complex; nonetheless, the criterion should be included in any evaluation of design effectiveness.

- Performance Against Schedule - The proper scheduling of design documents and designer specified/procured materials significantly affect a project. The performance against schedule criterion reflects the timeliness of design document and materials delivery.

- Ease of Start-Up - Ease of start-up is a partial indication of the accuracy and efficiency of the design. A measure of the efficiency is obtained by comparing budgeted to actual start-up time.

- Security - Security throughout the project life cycle is directly linked to the effectiveness of the design effort. A quality design considers this element

throughout the project. The amount of effort given to security considerations must depend on the vulnerability assessment. An effective design will help decrease security vulnerabilities in a project.

From Chapter 5, The Objectives Matrix

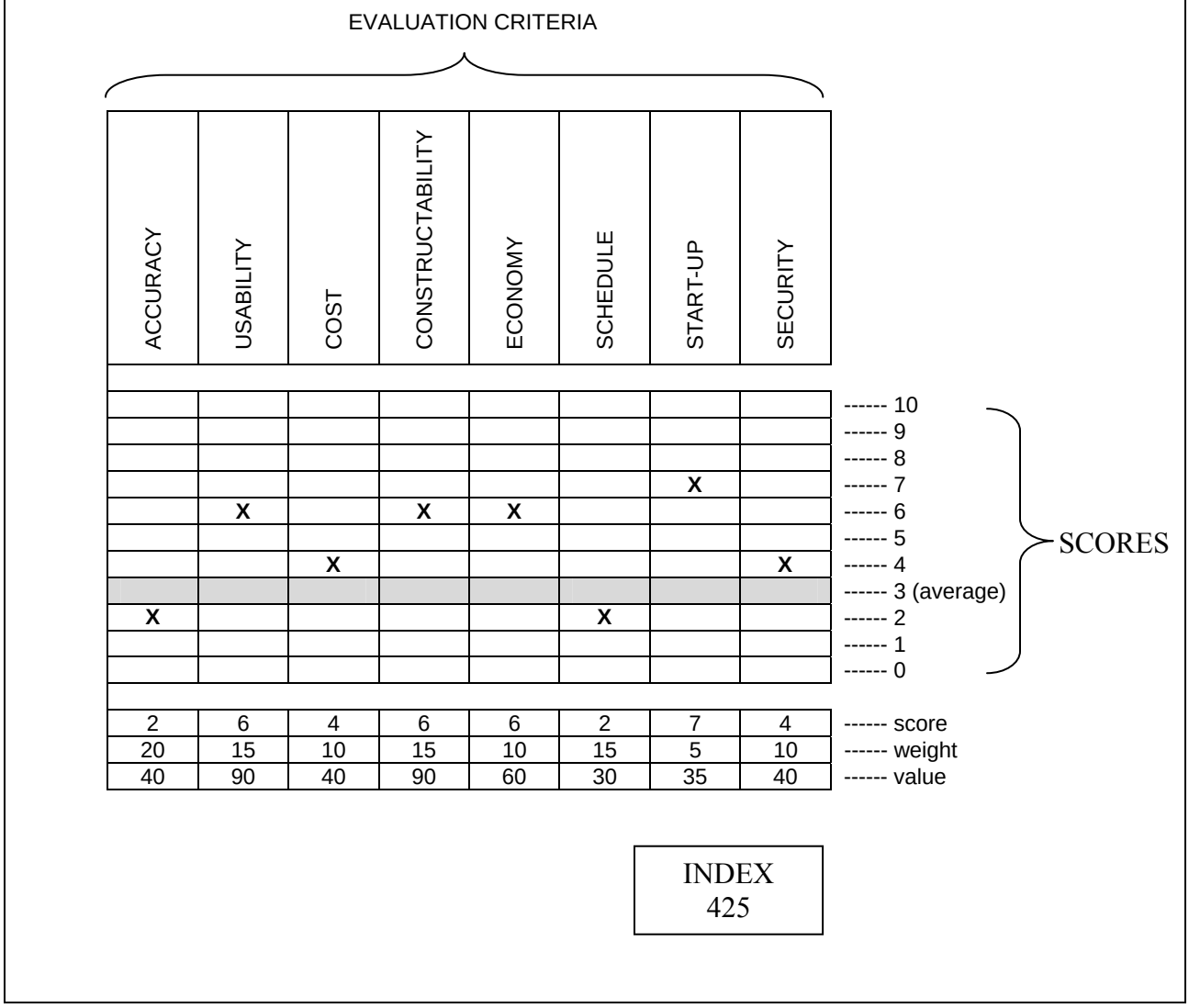



**Figure 4. Sample Project Objectives Matrix**

The objectives matrix consists of four main components: the criteria, the weights, the performance scale, and the performance index. The criteria define what is to be measured. The weights determine the relative importance of the criteria to each other and to the overall objective of the measurement. The performance scale compares the measured value of the criterion to a standard or selected benchmark value and permits scoring of the individual criterion. Using these three components, the fourth component, the performance index, is calculated and the result used to indicate performance.

As previously noted the criteria may vary from project to project and the weights may vary according to circumstances. The weightings shown in Figure 4 are for illustrative purposes; they should actually be establish by the project team at the beginning of the project and can be most valuable for aligning team objectives.

## 3.4 Constructability

Constructability refers to the effective and timely integration of construction knowledge into the conceptual planning, design, construction and field operations to achieve overall project objectives in the most timely, accurately and cost-effective fashion. Constructability can support all project objectives including reduced cost, shortened schedules, improved quality, security, and safety, and enhanced management of risk (Construction Industry Institute, 2002).

### 3.4.1 Constructability Concepts

CII literature identifies 17 constructability concepts that capture the essential elements of constructability (Construction Industry Institute, 1993). Eight of the concepts deal with conceptual planning; another eight cover design and procurement; and the last concept covers field operations. The Practice Development Team reviewed these concepts and determined that 12 failed to adequately address security issues. The 12 concepts deemed lacking in security application were updated by the team. Figure 5 lists all 17 concepts and those with security updates integrated are marked with an asterisk (*).

From Part IV, Page 109: Summary of Constructability Concepts

## Constructability Concepts

| Concept Index | Concept Name |
|---|---|
| I-1* | Constructability program is an integral part of project execution plan |
| I-2* | Project planning involves construction knowledge and experience |
| I-3 | Early construction involvement is considered in development of contracting strategy |
| I-4* | Project schedules are construction-sensitive |
| I-5* | Basic design approaches consider major construction methods |
| I-6* | Site layouts promote efficient construction |
| I-7* | Project team participants responsible for constructability are identified early |
| I-8* | Advanced information technologies are applied throughout project. |
| II-1 | Design and procurement schedules are construction sensitive |
| II-2* | Designs are configured to enable efficient construction |
| II-3 | Design elements are standardized |
| II-4* | Construction efficiency is considered in specification development |
| II-5* | Module/preassembly designs are prepared to facilitate fabrication, transport, and installation |
| II-6* | Designs promote construction accessibility of personnel, material, and equipment |
| II-7* | Designs facilitate construction under adverse weather conditions |
| II-8 | Design and construction sequencing should facilitate system turnover and start-up |
| III-1 | Constructability is enhanced when innovative construction methods are utilized |

**Figure 5. Constructability Concepts**

Among the planning concepts, security considerations ranked high in early project planning, basic design approaches, and site layouts. Security can be enhanced during early project planning by alignment of priorities, screening of team members to include preferred suppliers, and basing site selection and design criteria development on a vulnerability assessment. Design approaches must consider security implications of major construction methods. For example, designs with increased modularization can reduce the size of the on-site labor force and decrease the visibility of efforts during construction, thereby increasing on-site security. Modularization, however, introduces a whole new set of security issues at the off-site preassembly location. Site layout decisions can promote facility security in all types of projects and the issues can differ significantly for retrofit compared to greenfield projects.

Among the design and procurement concepts, designs promoting accessibility of personnel, materiel, and equipment were found to be of high importance to security. Security considerations were highly important because of their inverse relation to accessibility. Control of design and procurement documents becomes most important for security during design and procurement. A distribution matrix for document control can be an effective tool to enhance security during these activities.

### 3.4.2 Constructability Security Updates

While numerous changes were proposed to the CII *Constructability* Implementation Guide, many appear to be rather minor. However, when considered in total, they promote an awareness of security throughout the constructability process. Other changes, particularly to the constructability concepts noted above are substantial. Figure 6 below summarizes changes proposed for 3 of the concepts; the changes are underlined.

From Part IV, Page 109: Summary of Constructability Concepts

Constructability Concepts

| Concept Index | Concept Name |
|---|---|
| I-2 | Project planning involves construction knowledge.<br>Planning aspect requires security input.<br>Security factors affect construction<br>Site selection<br>Establishment of priorities<br>Preferred suppliers |
| I-5 | Basic design approaches.<br>Implications of major construction methods on security<br>Modularization can increase security<br>Reduce on-site labor force<br>Decrease visibility of efforts |
| I-6 | Site layouts promote efficient construction.<br>Site layout decisions can affect security<br>Adherence to security standards<br>Efficient access control procedures<br>Retrofit vs. greenfield |

**Figure 6. Sample Constructability Security Updates**

## 3.5 Materials Management

Materials management is an integrated process for planning and controlling all efforts to ensure that the quality and quantity of materials and equipment are appropriately specified in a timely manner, obtained at a reasonable cost, and available when needed. Materials management systems integrate takeoff, vendor evaluation, purchasing,

expediting, warehousing, distribution, and disposal of materials (Construction Industry Institute, 2002).

### 3.5.1 Security Considerations for Material Management

The materials management activities begin early in the planning phase and continue throughout design, construction, and start-up. Issues arise for each of the security elements of physical, personnel, and information security. Physical security can be critical during transportation, warehousing and distribution of materials to prevent theft or acts of sabotage. During start-up, the introduction of feedstock can greatly affect the consequences of a security breach. Personnel security becomes important for vendor screening and qualification. Much of the procurement process is accomplished via electronic means, which makes information security more critical than ever before. With the internet outgrowth, information security has become a major issue for procurement requiring continual reassessment. Each of these security elements must be addressed using the security vulnerability assessment.

Methods of construction will affect the procurement process and ultimately security considerations. Prefabrication of plant equipment and materials including preassembly and modules can have a significant positive impact on the field labor requirements, project cost, procurement plans, and security. While preassembly can improve jobsite security, it can increase the requirements for vendor/supplier screening and actually increase inspection and acceptance costs.

An approved supplier list (ASL) approved by the owner and contractor is an important part of the project procurement plan. Security factors must be considered during the preparation and approval of this list.

The main security concerns of site material control are protection of tools, equipment, and materials from theft; admittance and direction of delivery vehicles to receiving areas; and procedure for removal of materials, tools, and equipment from the site (gate pass procedure). Materials personnel should be involved in the development and review of security procedures to make certain their concerns are adequately addressed. An effective communications system between security, material control, and construction personnel is essential for efficient direction of incoming deliveries, unloading crews and equipment, and routine communication between the crafts and the warehouse.

When managing materials on international construction projects, the contractor frequently has less control than with a typical domestic project. This is the case in particular, for projects in underdeveloped and developing (UD/D) countries. Theft and pilferage are potentially significant problems in some such countries. Continuous or periodic physical inventory checks and security procedures are therefore among the most important warehousing activities on remote projects. Because of the time required for replacement of imported items, losses from inventories can cause schedule crises as well as impact cost performance. Such losses may be the result physical deterioration, misappropriation of critical items for other uses, poor and inaccurate record keeping, as

well as theft and pilferage. Security challenges presented by international projects may be different from those experienced domestically and may require additional efforts and assets to successfully manage those threats. In all cases though, a security vulnerability assessment is critical for assessing risk to the materials management system.

### 3.5.2 Material Management Security Updates

The Practice Development Team's guided walk through of the CII documentation (Construction Industry Institute, 1999) yielded numerous updates to the materials management best practice. This document is extensive addressing virtually all aspects of materials management and it includes many checklists to assist with implementation. While many updates to the manual were identified and documented, two are presented here for illustration in Figure 7.

| |
|---|
| From Chapter 7, Section 4.0, Subcontractor Prequalification Form – New question:<br><br>Do you conduct background investigations on all of your employees assigned to your site? Yes ❑ No ❑ |
| From Chapter 14, Section 5.0, Materials Management Computer System Evaluation Questionnaire:<br><br>9. Describe the general system hardware and software platforms to include configurable permissions and data access controls. |

**Figure 7. Sample Materials Management Security Updates**

## 3.6 Planning for Startup

Plant startup is defined as the transitional phase between plant construction completion and commercial operations, including all of the activities that bridge these two phases. Critical steps within the startup phase include system turnover, check-out of systems, commissioning of systems, introduction of feedstock, and performance testing (Construction Industry Institute, 1998).

### 3.6.1 Planning for Startup Model

The planning for startup model is a sequence of 45 planning activities organized according to project phases. These phases include pre-project planning, detailed design,

procurement, construction, and startup/initial operations. The research team that developed CII's Planning for Start-up best practice actually identified 8 project phases; however, 3 of those phases are combined here to present the practice consistent with the 5 project phases identified throughout this report. After combining the first 3 phases, the pre-project planning phase includes the activities of pre-project planning requirements definition, technology transfer, conceptual development and feasibility, and front-end engineering. The start-up phase includes checkout and commissioning and initial operations.

### 3.6.2 Planning for Startup Security Updates

In addition to recommending the necessary updates to the 45 startup planning activities, the Practice Development Team identified 3 new activities: Plan for Startup Security, Update Startup Security Plan, and Finalize Startup Security Plan. These activities were integrated into the Planning for Startup Model adding the interrelationships as appropriate. Complete definition of these activities included development of key concepts, deliverables, motive/rationale, responsibility, quality gates/sequencing constraints, basic steps for implementation, tools needed/provided, and challenges to successful implementation. An example of the definition sheet for Plan for Startup Security is provided in Figure 8.

Updates to the existing startup activities varied from modifications to activity inputs to redefining key concepts and basic implementation steps. For the requirements definition and technology transfer parts of the pre-project planning phase, the security vulnerability assessment was added to the business plan as an input to the first model activity, Ensure Senior Management Commitment. In the checkout and commissioning part of the startup phase, implement startup security plan was added as part of the Finalize Operations/Maintenance Organization & Management System activity.

The Planning for Startup best practice also includes 26 tools to complement the 45 planning activities. These tools are intended to facilitate implementation of the startup planning activities. The Practice Development Team updated these tools as appropriate. The updates in some cases were as simple as the addition of responsibilities for security, or updates to basic steps for accomplishment of activities in a security aware environment. Other tool updates were more comprehensive such as the identification and documentation of "security assurance" as a startup objective.

From Chapter 4, Establish Startup Objectives

**Plan for Startup Security**

**A. Phase:** Front-end engineering

**B. Key Concepts:** Startup security risks must be assessed early on in order to minimize their impacts. Documented security lessons learned can be very helpful in this effort.

**C. Deliverables:** A listing of potential risks to successful startup security and associated estimates of impact. Updated SVA and updated security plan.

**D. Motive/Rationale:** Overlooked security risks can severely impact startup schedule, cost performance, and other measures of success. Early detection efforts are needed in order to reduce or contain these loss potentials.

**E. Responsibility:** Startup Manager
**Accountability:** Manufacturing Operations Representative, Owner Project Manager
**Consult:** Contractor Project Manager, Planner/Scheduler, Security Manager
**Inform:** Plant Manager

**F. Quality Gate/Sequencing Constraints:** This activity is not a quality gate but should occur before approval of appropriate request.

**G. Basic Steps:**

1. Consult the Startup Execution Plan, Security Vulnerability security plan, and lessons learned to date
2. Identify risks associated with security concerns

**H. Tools Needed:** Security Vulnerability Assessment, Process Hazards Analysis

**I. Challenges to Successful Implementation:**

- Obtaining accurate threat information with which to update SVA
- Budget limitations
- Understanding of operational environment (cultural, economic, social)
- Lack of security awareness
- Limitations of in-house expertise

**Figure 8. Plan for Startup Security Activity Definition**

# *4. OTHER METHODOLOGICAL ISSUES*

## 4.1 Security Elements

Security elements were conceived of as the major security subdivisions to be addressed while reviewing the practices. Three security elements were identified: physical, personnel, and information. Physical security considerations include equipment, building and grounds design, and security practices designed to prevent physical attacks on facilities, persons, property, or information. Personnel security includes practices and procedures for hiring, terminating, and addressing workplace issues; screening or background checks of employees. Information security refers to practices and procedures for protection of documents, data, networks, computer facilities, and telephonic or other verbal communication (Center for Chemical Process Safety, 2002).

## 4.2 Practice Mapping

After all of the CII best practices had been reviewed and security integrated, the Practice Development Team began practice mapping. The intent was to organize the practices incorporating security components in a logical manner, facilitating the development of the security questionnaire.

In order to map the practices, the team members reviewed each of the security practices by project phase. Since phases within the project execution process typically overlap, organizing by phase assisted the team in identifying those practices to be addressed in multiple phases.

Five phases were used to organize the practices: front-end planning, detailed design, procurement, construction, and startup. As practices were mapped to phases, the team also assessed whether the practices were applicable to physical, personnel, or information security elements. It was found that practices could address multiple elements, with some being applicable to all three.

Mapping practices by project phase and security element permitted the team to chronologically walk through the project execution process and perform gap analysis. Following the first gap analysis (Section 4.3), the team identified and addressed the lack of security practices documented during the construction phase.

Note that the number of practices mapped in a phase does not indicate whether one phase contributes to security more than another phase or that one security element is more influential to project security than another. The practice mapping enabled the team to develop the security questionnaire; the weighting process (Section 5.2) following the questionnaire development (Section 4.4) was used to develop relative importance of the respective practices and elements.

Appendix A provides the results of the practice mapping exercise.

## 4.3 Gap Analysis, Part 1: Best Practices Review

Practice mapping served to organize and consolidate security practices, but it also permitted the team to perform gap analysis and identify phases and security elements that had not been well addressed. It became clear from this analysis that construction site security had been inadequately addressed in the security practices identified thus far. To correct this oversight a team consisting of 2 security specialists, one representing an owner and one representing a contractor, the principal investigator, and a research assistant was formed. The team convened a special workshop and construction site security guidelines were drafted. The guidelines were reviewed and approved by the Practice Development Team and later expanded based on current security management publications.

The construction site security guidelines are intended as a checklist to help owner and contractor organizations incorporate security measures based on assessments of risk. Depending on the type of project and the potential risks that might be faced, certain of the elements may be more important than others. The guidelines are not an all-inclusive list of security measures, and owner and contractor organizations may find it necessary to consider other measures as appropriate to the project. The guidelines are included in Appendix B.

## 4.4 Questionnaire Development

Two important steps necessary to the development of a security assessment tool were completed: 1) identification of specific security practices and 2) mapping of these security practices by project phase and security elements. The next step undertaken was the further consolidation of practices and the construction of a questionnaire for assessing the level of integration of security into project processes.

In an effort to minimize respondent burden while still maximizing information gathering capability, the team further consolidated practices. The first step was to collapse them into logical groupings. Practices that were related or that were components of a process were combined. An example of this is the grouping of Civil/Structural Requirements, Architectural Requirements, Water Treatment Requirements, and Loading/Unloading/Storage Facilities Requirements from Front-end Planning phase into the Preparation of Specifications and Requirements group.

Collapsing the practices was an iterative process. The team reviewed every practice on the Practice Map for logical groupings. Once the first iteration was complete, the team reviewed the logical groupings to determine whether some of the groups could be consolidated into another group. After numerous rounds of collapsing security practices into logical groupings, the team was able to formulate questions that addressed multiple security requirements with only 33 questions. Because of the consolidation process, it is possible to categorize the 33 questions by project phase, security element, relevant CII

publication, and a logical category. These categories, included: objectives, planning, requirements and specifications, personnel, information, site information, and site security.

The 33 questions were then formatted as shown in Figure 9. The stem for each of the questions was, "Security was a consideration in …" followed by an activity appropriate for security integration. The response option was a Likert-type, 5-point scale response category, ranging from strongly disagree to strongly agree. Based on experience from CII's ongoing benchmarking program, the Practice Development Team felt that by structuring the questions as shown in Figure 9, respondent burden would be kept to a minimum and quality of the data could be maximized. Appendix C contains the complete security questionnaire.

An examination of Appendix C, Security Questionnaire and Appendix A, Results of Practice Mapping reveals the degree of consolidation required to keep the questionnaire manageable and also illustrates the linkage between the CII best practices and the final questions. For example the first question in Appendix C, "Security was a consideration in establishing project objectives, (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion, etc.)," incorporates elements from the CII best practices of Pre-Project Planning (PDRI) IR113-2, Alignment During Pre-Project Planning IR113-3, Constructability Publication 34-1, and Materials Management IR 7-3. The phase & source key included with the practice mapping results in Appendix A can be used to trace linkages for all of the questions in Appendix C.

| Security was a consideration in | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree | NA/Unknown |
|---|---|---|---|---|---|---|
| establishing project objectives (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion, etc.). | | | | | | |
| preparation of the specifications and requirements (e.g., civil/structural, architectural, water treatment, loading/unloading/storage facilities, substation/power sources, instrument & electrical, etc.). | | | | | | |
| developing and evaluating design criteria (based on vulnerability assessment). | | | | | | |

**Figure 9. Security Questionnaire Example**

## 4.5 Gap Analysis, Part 2: Applying Risk Profiles

Following the consolidation of security practices into the 33 questions and questionnaire formatting, the Practice Development Team decided to perform another gap analysis to reexamine the coverage of security issues for each project phase and security element. While discussing approaches for the gap analysis, it became apparent that the team members' responses to the questions and perceptions of gaps were strongly influenced by their views of risk. The team, therefore, decided to develop a consensus risk profile, which would be used in the second gap analysis. Each team member was asked to consider two types of projects, new construction (green field or grassroots) and renovation (retrofit, additions and modernizations), and to list in priority order the major risks confronting heavy industrial projects during each phase of the project. Team member risk profiles were then consolidated for the consensus risk profile in rank order, from highest risk to lowest risk. The risks identified varied considerably by team members, thus the consolidated profile was useful when reviewing the questionnaire for completeness. The consolidated risk profiles are shown in Appendix D.

It is worth noting that the team felt that information disclosure/compromise was a risk in all phases of construction. This perspective was significant during the question weighting process (Section 5.2).

Following the development of the consolidated risk profile, the team analyzed the 33 questionnaire items to determine whether all of the risks identified were addressed in the questionnaire. With minor additions to some of the 33 questions, the team concluded that the risks were adequately covered by the questions.

# 5. DEVELOPMENT OF THE SECURITY RATING INDEX

An objective of this research was to develop a means of quantitatively assessing the level of implementation of security practices for a project. The Security Rating Index (SRI) provides this means. The SRI score, in conjunction with Threat and Consequence ratings (Section 6.1), enables comparison among projects with similar conditions.

## 5.1 Scoring Algorithm

A scoring algorithm was developed for the SRI to assess use of the security best practices on a scale of 0 to 10, with 0 indicating no use of the practices and 10 indicating full use. The SRI score is computed with two algorithms. The first algorithm calculates SRI scores for each of the five project phases; the second algorithm calculates the Project SRI based upon the Phase SRI scores. In order to calculate the Project SRI score, a minimum of 3 phase scores are required for owners and a minimum of 2 phase scores are required for contractors.

The Phase SRI algorithm is:

$$P = \left[ \frac{\sum_{i=1}^{n} (w_i)(v_i)}{\sum_{i=1}^{n} w_i} \right] \times 10$$

Where P is the project's Phase SRI score;
n is the total number of questions within a phase;
$w_i$ is the phase question weight ( see Section 5.2)
$v_i$ is the value of the response on a 0 to 1 scale (0 = strongly disagree, 0.25 = disagree, 0.5 = neutral, 0.75 = agree and 1 = strongly agree); questions answered NA/UNK are omitted from the calculation

The Project SRI algorithm is:

$$S = \frac{\sum_{i=1}^{n} (W_i)(P_i)}{\sum_{i=1}^{n} W_i}$$

Where S is the project's SRI score;
n is the total number of phases within a project;
$W_i$ is the sum of the phase weights
$P_i$ is the Phase SRI score; phases not submitted are omitted from the calculation

## 5.2 Establishing Weights

Upon completion of the questionnaire, the Practice Development Team discussed the issue of weighting the questions. The team concluded that while all questions were important for assessing project security, not all questions contributed equally to this assessment. Since security features that are incorporated early in the project delivery process often have more impact, and are more cost effective, than those incorporated later, the Practice Development Team felt that it was appropriate to weight the project phases. The team also felt that the importance of the security elements varied by phases, as did the individual questions within each element. Weights were therefore developed for security elements within each project phase and for individual questions within each element. For example, to illustrate the importance of practices by project phase, developing a system startup plan was less important to the longer term security of the facility than preparation of specifications and requirements during front-end planning.

Weights were established using the analytical hierarchy process (AHP) (ASTM International, 2002) and Expert Choice© software (Expert Choice, Inc., 2003). AHP is a decision analysis method that considers nonmonetary attributes, both qualitative and quantitative, when evaluating project alternatives. It uses pairwise comparisons to rate the relative importance of alternative elements in a hierarchy. AHP relies upon expert opinions to establish relative importance, and the Practice Development Team served as the experts.

Three pairwise comparison matrices were developed. First, weights were established for each project phase from front end planning through startup using the verbal scale shown in Table 3. Experience led the team to conclude that in most cases security implementation performed earlier in the project was far more likely to favorably impact outcomes, including security, than if performed later in the project delivery cycle. This resulted in higher phase weights assigned to earlier project phases. Next the team weighted the security elements comparing physical, personnel, and information security. The team decided that the relative importance of the elements was phase dependent; therefore, the weighting process for elements was conducted for each project phase. As a final step the team weighted each of the questionnaire items within each phase. This was an onerous process; however, the Expert Choice© software provided the means to effectively accomplish this. The software also provided an assessment of consistency throughout the decision making process. Appendix E shows the results of the weighting exercise. Note that the sum of the weights assigned to each phase is 1.0, and the sum of the weights for the security elements within each phase also sums to 1.0.

**Table 3. Verbal Scale for the AHP**

| Verbal Scale | Numerical Scale |
|---|---|
| Equal importance of one item to the other | 1 |
| Moderate importance of one item over the other | 3 |
| Strong importance of one item over the other | 5 |
| Very strong importance of one item over the other | 7 |
| Extremely strong importance of one item over the other | 9 |

The output, an aggregate of each of the weighting exercises, yielded some surprising results. Once the initial weighting was complete, some questionnaire items, like identifying stakeholders for the project team, were not as relatively important as the Practice Development Team first hypothesized.

Further analysis showed that the framework for weighting physical, personnel, and information security elements incorporated the typical security bias towards physical security, at the expense of information and personnel security elements. Physical security was originally rated as having more importance during the front-end planning phase, but the major risks are more likely to be personnel and information security during this phase since no actual facility exists, at least for greenfield projects. This viewpoint is supported by the consolidated risk profile discussed in Section 4.5.

While the physical security elements of the proposed facility are being addressed during the early phases, the *risks* to the project are mostly due to inadequate team selection or compromise of sensitive information; this can severely impact security later in the project life cycle. Information is considered an economic resource on par with human resources, equipment, materials, and capital (Fay, 2002). Because of the security element weights were not representative of the aforementioned considerations, the team reweighted the three security elements to better address risk during the phases, yielding the final weights. The final output showed a relative distribution of importance that was more congruent with team member expectations. Even though the number of questions related to physical security is greater than the number containing information and personnel security, the highest weighted questions contain information and personnel security elements. This is consistent with the team members' expectations as well as current security management principles. Appendix F shows the final AHP output.

# 6. INTERPRETATION AND USE OF THE SECURITY RATING INDEX

An SRI may be obtained for a project by simply completing the security questionnaire. Nevertheless, this is not sufficient to interpret the SRI. Depending on factors such as site location, industrial processes, or environmental effects, some projects may require higher levels of security integration than other, similar projects. As an example, a chemical processing facility located in an area where there is no surrounding residential development and minor potential for adverse environmental impacts may require less security integration than one sited close to a densely populated area. In order to interpret the SRI correctly, it must be viewed in the context of threats and consequences of potential security breaches.

## 6.1 Threats and Consequences

The Practice Development Team used the Security Vulnerability Assessment (SVA) methodology, developed by the American Petroleum Institute/National Petrochemical & Refiners Association (API/NPRA) (2003), to approach the issue of threats and consequences. An "SVA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact on an asset" (Center for Chemical Process Safety, 2002, p. 8). Rather than a quantitative analysis, an SVA is a qualitative risk analysis similar to the qualitative risk analysis used in assessing the risk of accidental damage and injury exposure at a facility.

An SVA also employs the concepts of *threats* and *consequences* to assess security vulnerability. A threat is defined as any indication, circumstance, or event with the potential to cause loss of, or damage to, an asset (Center for Chemical Process Safety, 2002). It also includes the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Adversaries might include: terrorists, either domestic or international; activist or pressure groups; criminals (e.g., white-collar, cyber hackers, organized, opportunists). Sources of threats may include: insider, external, and insiders working as colluders with external sources.

Implicit in the threat concept is likelihood of the event occurring. As the threat increases, the likelihood of the security incident increases, as well. Threat ratings range from 1, very low, to 5, very high. Very high indicates that a definite risk exists and that the adversary has both the intent and capability to breach security possibly resulting in the consequences listed in Table 5. It also indicates that the facility, or similar assets, is targeted on a recurring basis. Very low, on the other hand, suggests no credible evidence of intent or capability, and no history of actual or planned threats against a facility or similar assets.

Using the API/NPRA guidelines as a model, the Practice Development Team developed the threat and consequence rating criteria shown in Tables 4 and 5. The team expanded upon the API/NPRA ratings to apply to all industrial projects, rather than petrochemical-

related projects, and to all phases of the project delivery cycle, rather than the operational phase.

Threat is not static throughout the project delivery cycle and is linked to consequences of a security breach. As the external environment or indicators (e.g., Homeland Security Advisory System level) change, the threat to the project may change as well.

**Table 4. Threat Rating Criteria**

| Threat Rating | Description |
|---|---|
| 5 - Very High | Indicates that a ***definite*** threat exists against the asset and that the adversary has both the capability and intent to launch an attack or commit a criminal act, and that the subject or similar assets are targeted on a frequently recurring basis. |
| 4 - High | Indicates that a ***credible*** threat exists against the asset based on knowledge of the adversary's capability and intent to attack or commit a criminal act against the asset, based on related incidents having taken place at similar assets or in similar situations. |
| 3 - Medium | Indicates that there is a ***possible*** threat to the asset based on the adversary's desire to compromise similar assets and/or the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents. |
| 2 - Low | Indicates that there is a ***low*** threat against the asset or similar assets and that few known adversaries would pose a threat to the asset |
| 1 - Very Low | Indicates ***no credible*** evidence of capability or intent and no history of actual or planned threats against the asset or similar assets |

Adapted from API/NPRA

In addition to threats, the worst-case consequences of security breaches must be evaluated. Consequences are defined as the amount or damage that may be expected from a successful attack against an asset (Center for Chemical Process Safety, 2002). Examples of consequences include: injuries to the public or to workers; environmental damage; direct and indirect financial losses to the company, to suppliers, and/or associated businesses; disruption to the national, regional, or local operations or economy; loss of reputation or business viability; evacuation of people living or working near the facility; excessive media exposure and related public hysteria affecting people that may be far removed from the actual event location.

Similar to threat, consequence is scored on a 1 to 5 scale with 1 indicating very minor consequences and 5 indicating very severe consequences. Specific criteria for assessment of each level of consequence are provided in Table 5.

Note that consequence is defined as the worst-case result of a security breach *over the facility life cycle*. The reason for this distinction is that it is neither practical nor economical to redesign a facility to ameliorate consequences as they change over the life cycle. For instance, during the construction phase of an oil refinery, no feedstock is on site, so the potential for offsite injuries as a result of a breach is low. Once the facility is commissioned, however, feedstock and highly combustible products are onsite, greatly increasing the potential for offsite injuries, fatalities, or environmental damage. The consequence changes significantly, but this is not an unexpected event, since it is known in the front-end planning phase. The project team certainly would not change the design because the consequence escalates throughout the life cycle; the design would address the operational consequence before the facility is constructed. Exceptions to consequence remaining the same would be for unforecasted reasons, for example, if the product or process changes or if the potential for offsite effects changes, perhaps due to demographic change.

**Table 5. Consequence Rating Criteria**

| Consequence Category | Description |
|---|---|
| 5 – Very Severe | ● Possibility of any offsite fatalities; possibility for multiple onsite fatalities<br>● Extensive environmental impact onsite and/or offsite<br>● Extensive property damage<br>● Very long term business interruption/expense |
| 4 – Severe | ● Possibility of any offsite injuries; possibility for onsite fatalities<br>● Significant environmental impact onsite and/or offsite<br>● Significant property damage<br>● Long term business interruption/expense |
| 3 – Moderate | ● No offsite injuries; possibility for widespread onsite injuries<br>● Moderate environmental impact onsite and/or offsite<br>● Moderate property damage<br>● Medium term business interruption/expense |
| 2 – Minor | ● Possibility for onsite injuries<br>● Minor environmental impact only<br>● Minor property damage<br>● Short term business interruption/expense |
| 1 – Very Minor | ● Possibility for minor onsite injuries<br>● No environmental impact<br>● Little to no property damage<br>● Little to no business interruption/expense |

Adapted from API/NPRA

## 6.2 Internal Company Use

The SRI has a number of important uses. First, it can be used as a checklist to influence security in the early phases of project planning so that essential security considerations can be integrated. Second, it focuses efforts on project security during project definition. Eventually, it should enable analysis of how changes in threat and consequence levels may impact cost and schedule. Finally, it should provide a means to manage risk by estimating the marginal costs of increasing the value of the SRI in terms of project cost and schedule.

## 6.3 Among Different Companies

Once sufficient data are available, the SRI will provide a means by which companies can gauge the level of security integration of their own projects against similar projects within the industry. Norms can be established for projects with similar threat and consequence levels across all industrial projects.

Figure 10 shows an example of a conceptual model that relates consequence, threat, and an expected SRI. Note that this is not based on actual data since not enough data has been collected for the SRI at this time. Consequence levels, described in Table 5 and plotted along the horizontal axis, may range from 1 to 5. Threat levels are conceptualized as a family of curves, each curve representing a threat level from 1 to 5 as described in Table 4. Shown for illustration is the consequence and expected SRI relationship for all projects for given a threat level 3. A similar curve would be produced for each level of threat. The expected SRI is the average of all the reported SRIs for a given threat and consequence level.

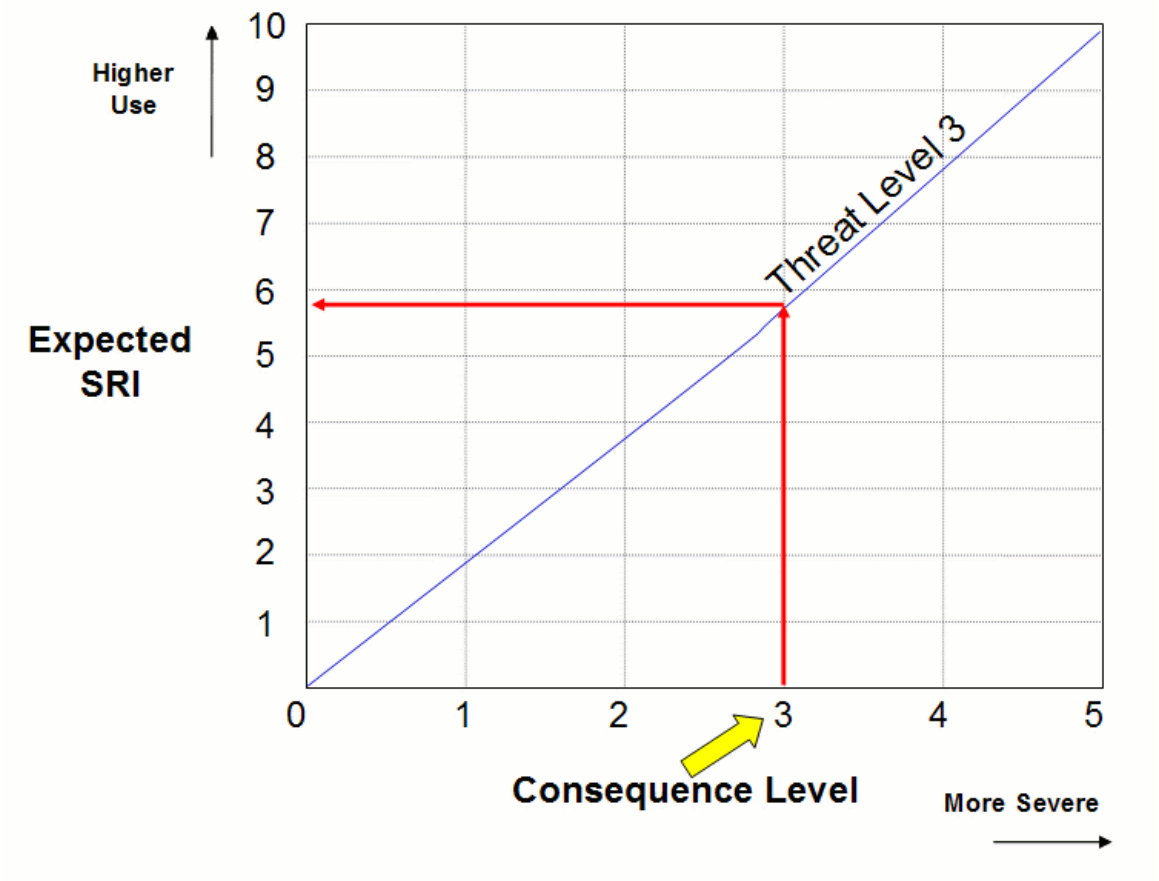



**Figure 10. Conceptual Model of an SRI**

This example shows that the expected SRI for projects with a threat level of 3 and a consequence level of 3 is slightly less than 6. Based on this example, should any single project with the same threat and consequence level receive the same score, then it is likely that security has been integrated into the project at a level similar to the mean of like projects given similar consequences and threats. Scores below that may indicate a lower level of security integration, while scores above that may indicate a higher level of security integration.

Figure 11 provides another example of how the data can be used. As the database is populated, quartiles of security integration can be developed enabling better comparisons of an individual project's SRI to similar projects in the database. Quartiles are a means to describe some of the characteristics of a distribution, in this case a distribution of projects. The 1st quartile is the point below which 75% of all other projects fall. The 2nd quartile represents the point below which 50% of all other projects fall, etc.

Figure 11 illustrates that a project with an SRI of slightly less than 6 is in the middle of the distribution for all projects at the same consequence and threat level. That is, 50% of all similar projects have a higher level of security integration, and 50% have a lower level of security integration.

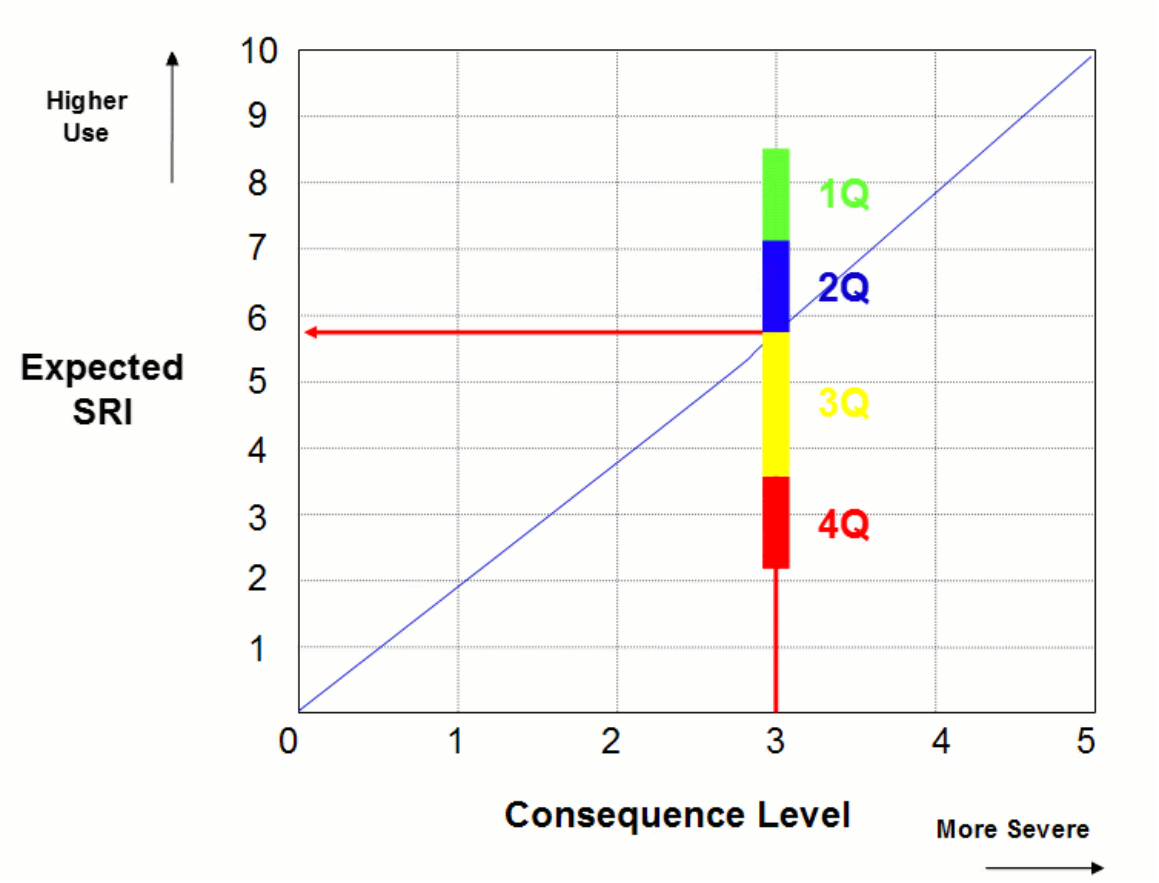



**Figure 11. Conceptual Model of Quartiles of SRI Use**

Corporate management can use this model to determine the level of security implementation they feel is appropriate for their project. For example, one company may feel that the median SRI, or industry "norm" for the same threat and consequence is sufficient for its project. Any SRI score in the second quartile or above would be acceptable. Another company might prioritize security as the most important characteristic of its project. In that case, the company may undertake additional measures to improve the SRI score so that it lies within the first quartile.

# 7. *SUMMARY AND RECOMMENDATIONS FOR FUTURE RESEARCH*

Figure 12 graphically displays the number of questions used to produce the SRI by project phase. Note that the total number of unique questions is 33, but because some are applicable to more than one phase, they are repeated in the appropriate phase. Including repeated questions nearly 32% of the questions address front end planning, and slightly over 25% address design. More than 60% of the activities relating to security (considering procurement, as well) occur before construction begins. This was an observation apparent to the Practice Development Team, although security activities were not front loaded intentionally.

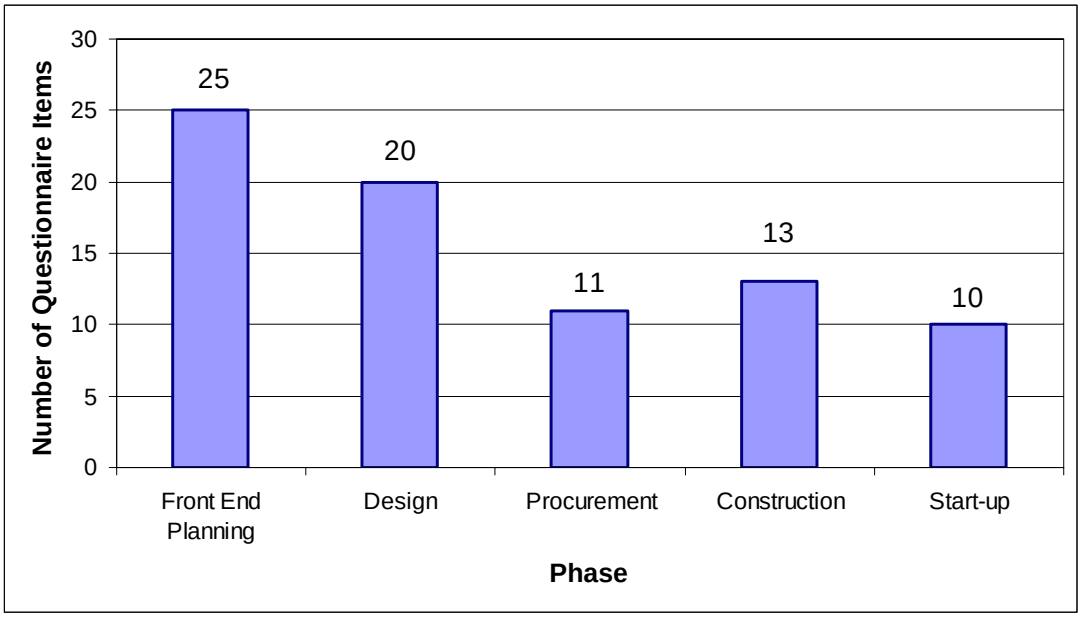



**Figure 12. Security-Related Questions by Project Phase**

Since the weights assigned to security activities in the front end planning and design phases were greater (Section 5.2 and Appendix E) than those assigned to activities in later phases, the relative importance of the activities is even greater than would be indicated by Figure 12 when project cost is considered. CII has long postulated a relationship between the ability to influence project cost as the project proceeds from planning through execution. This relationship, known within CII as the cost influence curve, suggests that the ability to influence project cost decreases rapidly when the execution phases of procurement and construction commence (Construction Industry Institute, 1995). Similarly, there exists an SRI-influence relationship as shown in Figure 13. The ability to influence security curve is fitted to the weights of the questions occurring in each phase of the project from front end planning through start-up.

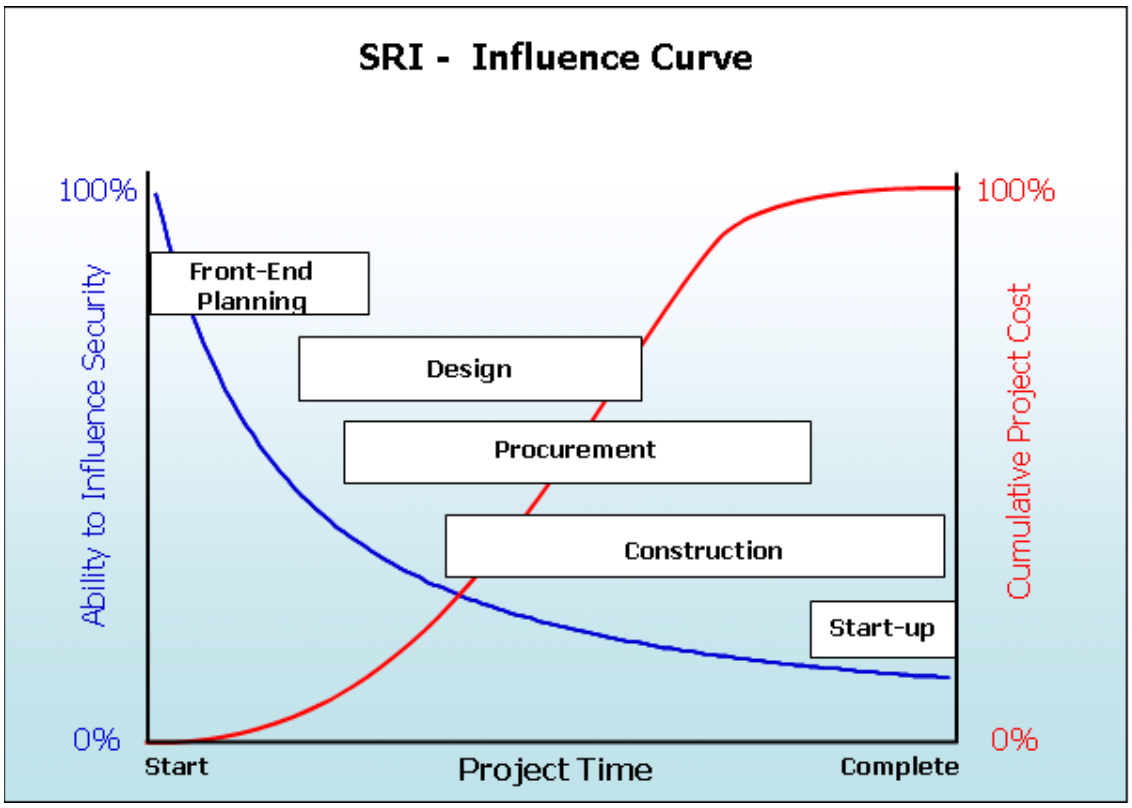



**Figure 13. SRI-Influence Curve**

Facility security, like many other facility attributes, can be enhanced most cost effectively when addressed early in the planning and design phases of a project. While this assertion may seem obvious, this study went far beyond confirming this contention and identified specific activities during project delivery that can be used to improve facility security and provide a quantitative assessment of the integration of security into established processes. Using a consensus building process, a Steering Team and a Practice Development Team composed of representatives of industry and academia, working with security experts, developed a tool to provide this quantitative assessment. The next step for this effort will be to validate the tool through collection of actual project data by CII. The validation process will serve several purposes: 1) to evaluate whether this tool will be an effective means of assessing security, 2) to quantify the impact of security best practices on cost, schedule, and safety, and 3) to establish longer term trends in security integration. To this end, the security questionnaire is expected be incorporated into the CII Benchmarking program.

Security best practices were developed during this study using experts and practices for industrial projects. A recommendation for future work is to adapt the security best practices to building and infrastructure projects.

It is also recommended that the use of the security best practices be expanded to an audience broader than CII member organizations for the purpose of gaining industry-wide acceptance. Organizations are currently being identified for this purpose.

## *Appendix A. Results of Practice Mapping*

| Phase | Physical | Personnel | Information |
|---|---|---|---|
| **FRONT END PLANNING** | Security Stakeholders on P3 Team (AI #1)[2] | | |
| | | Social Issues (B8)[1] | |
| | | | CADD/Model Requirements (M1)[1] |
| | Operating Philosophy (A3)[1] | | |
| | | Training Requirements for Operational Facility (P6)[1] | |
| | | | Document Control Systems (M3)[1] |
| | Reliability Philosophy (A1)[1] | | |
| | Affordability/Feasibility (B4)[1] | | |
| | Affordability/Feasibility (7-3)[5] | | |
| | Future Expansion Considerations (B6)[1] | | |
| | Technology (C1)[1] | | |
| | Processes (C2)[1] | | |
| | Project Objectives Statement (D1)[1] | | |
| | Objectives with Security Delineated (AI #8)[2] | | |
| | Effective Communication (AI #4)[2] | | |
| | Clear Priorities (AI #3)[2] | | |
| | Project Design Criteria (D2)[1] | | |
| | Project Design Criteria (7-3)[5] | | |
| | Site Characteristics (D3)[1] | | |
| | Lead/Discipline Scope of Work (D5)[1] | | |
| | Process Simplification (E1)[1] | | |
| | Design/Material Alternates Considered (E2)[1] | | |
| | Design/Material Alternates Considered (7-3)[5] | | |

PHASE & SOURCE KEY:
[1] PDRI, IR 113-2
[2] Alignment, IR 113-3
[3] Design Effectiveness, RS 8-1
[4] Constructability, Pub 34-1
[5] Materials Management, IR 7-3
[6] Construction Site Security Plan
[7] Planning for Startup, IR 121-2

| Phase | Physical | Personnel | Information |
|---|---|---|---|
| **FRONT END PLANNING** | Site Location (F1)[1] | | |
| | Site Location (7-3) [5] | | |
| | Permit Requirements (F4)[1] | | |
| | Fire Protection & Safety Considerations (F6)[1] | | |
| | Plot Plan (G8)[1] | | |
| | Plot Plan (7-3) [5] | | |
| | Equipment Status (H1)[1] | | |
| | Civil/Structural Requirements (I1)[1] | | |
| | Architectural Requirements (I2)[1] | | |
| | Water Treatment Requirements (J1)[1] | | |
| | Loading/Unloading/Storage Facilities Requirements (J2)[1] | | |
| | Substation Requirements Power Sources Ident. (K4)[1] | | |
| | Instrument & Electrical Specifications (K6)[1] | | |
| | Procurement Procedures and Plans (L2)[1] | | |
| | Engineering/Construction Plan & Approach (P2)[1] | | |
| | Engineering/Construction Plan & Approach (7-3)[5] | | |
| | Pre-Commissioning. Turnover Sequence Requirements (P4)[1] | | |
| | Startup Requirements (P5)[1] | | |
| | PEP incorporates security (I-1) [4] | | |
| | PEP incorporates security (7-3)[5] | | |
| | Security input into planning (I-2) [4] | | |

PHASE & SOURCE KEY:
[1] PDRI, IR 113-2
[2] Alignment, IR 113-3
[3] Design Effectiveness, RS 8-1
[4] Constructability, Pub 34-1
[5] Materials Management, IR 7-3
[6] Construction Site Security Plan
[7] Planning for Startup, IR 121-2

| Phase | Physical | Personnel | Information |
|---|---|---|---|
| **FRONT END PLANNING** | | Design Effectiveness Criteria (RS8-1)[3] | |
| | Procurement/Logistics Procedures and Plans/Strategies (7-3)[5] | Procurement/Logistics Procedures and Plans/Strategies (7-3)[5] | Procurement/Logistics Procedures and Plans/Strategies (7-3)[5] |
| | Security input into planning (7-3)[5] | Security input into planning (7-3)[5] | Security input into planning (7-3)[5] |
| | Estimate Startup Security Costs (2-B)[7] | Estimate Startup Security Costs (2-B)[7] | Estimate Startup Security Costs (2-B)[7] |
| | Identify Startup Security Objectives (3-A)[7] | Identify Startup Security Objectives (3-A)[7] | Identify Startup Security Objectives (3-A)[7] |
| | Assign Startup Security Stakeholders (3-C)[7] | Assign Startup Security Stakeholders (3-C)[7] | Assign Startup Security Stakeholders (3-C)[7] |
| | Reconcile Startup Logic with Security Plan (3-D)[7] | Reconcile Startup Logic with Security Plan (3-D)[7] | Reconcile Startup Logic with Security Plan (3-D)[7] |
| | Acquire O&M Input for Security Systems (3-E)[7] | Acquire O&M Input for Security Systems (3-E)[7] | Acquire O&M Input for Security Systems (3-E)[7] |
| | Identify Startup Security Risks (3-F)[7] | Identify Startup Security Risks (3-F)[7] | Identify Startup Security Risks (3-F)[7] |
| | Identify Startup Security Procurement Requirements (3-H)[7] | Identify Startup Security Procurement Requirements (3-H)[7] | Identify Startup Security Procurement Requirements (3-H)[7] |
| | Refine Startup Security Costs (3-I)[7] | Refine Startup Security Costs (3-I)[7] | Refine Startup Security Costs (3-I)[7] |
| | Develop Startup Security Plan (3-X)[7] | Develop Startup Security Plan (3-X)[7] | Develop Startup Security Plan (3-X)[7] |
| | Develop Construction Site Security Plan (CSS)[6] | Develop Construction Site Security Plan (CSS)[6] | Develop Construction Site Security Plan (CSS)[6] |

PHASE & SOURCE KEY:
[1] PDRI, IR 113-2
[2] Alignment, IR 113-3
[3] Design Effectiveness, RS 8-1
[4] Constructability, Pub 34-1
[5] Materials Management, IR 7-3
[6] Construction Site Security Plan
[7] Planning for Startup, IR 121-2

| Phase | Physical | Personnel | Information |
|---|---|---|---|
| **DESIGN** | Design approaches and/or alternatives consider security (I-5); (II-2); (II-5)[4] | | |
| | Site layout considers security (I-6) [4] | | |
| | Consider security aspects of construction accessibility for retrofit (II-6)[4] | | |
| | Update Startup Security Risks (4-I)[7] | Update Startup Security Risks (4-I)[7] | Update Startup Security Risks (4-I)[7] |
| | Ensure Security Addressed in O&M Training Plan (4-J)[7] | Ensure Security Addressed in O&M Training Plan (4-J)[7] | Ensure Security Addressed in O&M Training Plan (4-J)[7] |
| | Refine Startup Security Costs (4-N)[7] | Refine Startup Security Costs (4-N)[7] | Refine Startup Security Costs (4-N)[7] |
| | Update Startup Security Plan (4-X)[7] | Update Startup Security Plan (4-X)[7] | Update Startup Security Plan (4-X)[7] |
| | Refine Construction Site Security Plan (CSS)[6] | Refine Construction Site Security Plan (CSS)[6] | Refine Construction Site Security Plan (CSS)[6] |
| **PROCUREMENT** | | Materials Management Personnel Security Procedures Training (7-3)[5] | |
| | | Background Investigations/Personnel Screening for Site Personnel (7-3)[5] | |

PHASE & SOURCE KEY:
[1] PDRI, IR 113-2
[2] Alignment, IR 113-3
[3] Design Effectiveness, RS 8-1
[4] Constructability, Pub 34-1
[5] Materials Management, IR 7-3
[6] Construction Site Security Plan
[7] Planning for Startup, IR 121-2

| Phase | Physical | Personnel | Information |
|---|---|---|---|
| **CONSTRUCTION** | Assess & Communicate Startup Security Effects from Changes (4-B)[7] | Assess & Communicate Startup Security Effects from Changes (4-B)[7] | Assess & Communicate Startup Security Effects from Changes (4-B)[7] |
| | Finalize Startup Security Risks (6-F) [7] | Finalize Startup Security Risks (6-F) [7] | Finalize Startup Security Risks (6-F)[7] |
| | Finalize Startup Security Plan (6-X)[7] | Finalize Startup Security Plan (6-X)[7] | Finalize Startup Security Plan (6-X)[7] |
| | Implement Construction Site Security Plan (7-3)[5] | Implement Construction Site Security Plan (7-3)[5] | Implement Construction Site Security Plan (7-3)[5] |
| | Implement Construction Site Security Plan (CSS)[6] | Implement Construction Site Security Plan (CSS)[6] | Implement Construction Site Security Plan (CSS)[6] |
| **START-UP** | Implement Startup Security Plan (7-A)[7] | Implement Startup Security Plan (7-A)[7] | Implement Startup Security Plan (7-A)[7] |
| | Implement Construction Site Security Plan (CSS)[6] | Implement Construction Site Security Plan (CSS)[6] | Implement Construction Site Security Plan (CSS)[6] |

PHASE & SOURCE KEY:
[1] PDRI, IR 113-2
[2] Alignment, IR 113-3
[3] Design Effectiveness, RS 8-1
[4] Constructability, Pub 34-1
[5] Materials Management, IR 7-3
[6] Construction Site Security Plan
[7] Planning for Startup, IR 121-2

## *Appendix B. Construction Site Security Guidelines*

**Note: The Construction Site Security Guidelines were developed by a subcommittee of the Process Development Team. The version that appears below is an expanded version based upon current security management publications.**

The owner is ultimately responsible for determining the measures that need to be implemented; this is especially true in renovation or addition projects, where the project occurs in or adjacent to an active facility.

Security considerations on "Greenfield" projects will typically be more contractor-driven. "Greenfield" projects may have a lessened likelihood of sabotage and attack than projects in existing facilities, but still have many opportunities for crime

The success of construction site security will be strongly contingent on the role management takes in the project (Broder, 2000).

I. Policy and Program
   a. Has a security policy been established?
   b. Has the policy been published?
      i. A crucial aspect of construction site security is establishing a written security policy. The security policy defines objectives and priorities, ensuring alignment between owner and contractor.
   b. Has the policy been agreed to between the owner and contractor?
      i. While the project owner must approve the security policy, the contractor must concur with all elements, since he will be responsible for much of the daily oversight and enforcement while the construction site is active.
      ii. Any exceptions to the policy must be resolved between the owner and contractor. This is crucial in cases where the construction site security plan will result in schedule or budget impact.
   c. Is the contractor's security supervisor accessible to the owner's security manager?
      i. These individuals will be responsible for ensuring compliance with their employers' objectives. They should have regular contact during the course of the construction project.
   d. What are the consequences of non-compliance?
      i. If the owner's security manager determines that the construction security plan is being violated, there should be clearly identified consequences.
         1. Disciplinary procedures should be specified in writing, preferably in the construction contract.
         2. Enforcement measures can range from written notices for minor infractions to monetary penalties for repeated offenses.

3. Non-compliance with the construction security plan is at least as serious as non-compliance with material specifications or other contract specifications.

II. Organization
   a. Has the contractor appointed a full-time security supervisor?
      i. It is crucial to have a security supervisor on site at all times. If the contractor does not have an employee on site whose sole responsibility is security, he should appoint a person who will be on site for the majority of the project as security supervisor. An example would be the construction superintendent or a foreman.
      ii. What is the security chain of command?
         1. The designated security supervisor must have access to owner's security manager, regardless of whom he reports to for non-security related issues.
   b. Are there security shifts?
      i. When the construction site is not operational, who assumes security responsibilities? Security is a full-time responsibility.
         1. On renovation/addition projects, the owner's full-time security personnel may assume responsibility after hours. If this is the case, have written procedures for handoff of security responsibilities.
         2. On Greenfield projects, this may not be possible. Have a written contract for professional security personnel or have other trained contractor personnel secure the site.
   c. Have security personnel received security training?
      i. Security training and certification is available from organizations such as the American Society for Industrial Security (ASIS) - http://www.asisonline.org/, which sponsors classes and conferences, as well as on-line coursework
   d. Are written reports made for incidents?
   e. Has there been a background investigation performed for security personnel?
   f. Are there periodic inspections of the construction site security by owner personnel?
   g. Does the security supervisor maintain contact with local law enforcement agencies to keep abreast of criminal activities and potential disorder in the community (Broder, 2000)?

III. Access Control
   a. Is 100% identification required of all persons entering the construction site?
      i. Are identification badges issued?
         1. Photo identification badges are preferred. They can also incorporate the following security measures:
            a. Proximity Card
            b. Magnetic Strip

c. Radio Frequency Identification Tag (RFID)
d. Smart Card
e. Biometric information

ii. Wearing enforcement?
iii. A written issue/return process is necessary
1. Badge recipients must sign an acknowledgment that they will report any lost badges

b. Is the personnel and vehicle search policy clearly posted at all entrances?
c. Who is responsible for controlling access to the site?
d. What is the visitor registration procedure?
i. Are visitors escorted at all times while on the construction site?
e. How is access between the construction site and the operational facility controlled?
f. How are vehicles admitted to construction site?
i. There should be a written policy stating vehicle access procedures and who is the approving authority
1. An approved vehicle access roster should be kept by the gate guard(s)
a. Approved vehicles that need to access the site for more than a day should be registered and provided a tag
2. Worker vehicles should have a designated parking area outside the construction site.
3. Policies and procedures should include
a. Employees
b. Visitors
c. Deliveries
d. Material and equipment removal

IV. Barriers
a. Is there a continuous fence around the entire construction site?
i. Permanent vs. non-permanent
ii. Eight feet high, two-inch square mesh, 11-guage or heavier wire (Broder, 2000)
b. Gates (Broder, 2000)
i. In good repair
ii. Gates same height and construction as fence?
iii. Open only when required for operations?
iv. Locked other times?
v. Equipped with alarm (how many?)
vi. Guarded when open?
vii. Under surveillance when open? How?
viii. Alternate access gates should be installed, but are not required to be active at all times
1. For emergency egress
2. Organized labor considerations, i.e., if main gate is blocked by striking workers or protestors

V. Lighting
   a. Is the entire perimeter of the construction site lighted?
      i. Both sides of the fence must be lighted so that an intruder may be detected at 100 meters (Broder, 2000)
      ii. Any access gates must be illuminated
   b. Lights must be checked daily, prior to darkness, so that deficiencies may be corrected prior to their use.
   c. The power supply for perimeter lighting must be inaccessible or tamper-proof. For example, if using light tower/generator set trailers, they must be secured in place and the control doors locked.
   d. Switches and controls (Broder, 2000)
      i. Protected?
      ii. Weatherproof and tamper resistant?
      iii. Accessible to security personnel?
      iv. Inaccessible from outside the perimeter barrier?
   e. Materials and equipment in receiving, shipping, and storage areas adequately lighted (Broder, 2000)?
      i. If laydown areas are geographically separate from the construction site, they must have the same security measures as the construction site.

VI. Locks and Keys
   a. Is the contractor security supervisor responsible for control of locks and keys?
      i. The contractor security supervisor should have overall authority for the issue and replacement of all locks and keys for the construction site.
         1. If the construction site is within an existing facility, the contractor should control the site, even though he may not be able to access it without passing through the owner's security.
         2. Owner personnel should not be allowed to access the construction site without contractor security supervisor approval.
   b. The lock and key control procedures should be in writing
      i. All key recipients should sign a key control register
         1. Non-employees should not be allowed to sign for keys
         2. Key recipients must sign an acknowledgment that they will report any lost keys and that they may not duplicate any keys
      ii. Master keys should not be identifiable as such (Broder, 2000)
      iii. Spare locks and keys should be double locked (i.e. in a locked container in a locked room)
   c. Padlocks should be locked to a hasp or staple when door or gate is open to prevent substitution (Broder, 2000).

d. Locks on inactive doors or gates should be checked regularly for evidence of tampering (Broder, 2000).

VII. Alarms
- a. Intrusion Detection
  - i. What assets should be protected?
    1. Three general classes (POA, 2003)
       - a. Perimeter or point of entry
       - b. General Area
       - c. Object
- b. Fire
  - i. Does it comply with National Fire Protection Association (NFPA) Code 72, National Fire Alarm Code
  - ii. What sensor type(s) are appropriate for the construction site?
    1. Detecting a fire at an early stage is critical. Certain construction materials or locations may necessitate different sensors because of the nature of potential fires.
    2. Sensors (POA, 2003)
       - a. Thermal (heat)
       - b. Smoke (photoelectric)
       - c. Flame (ultraviolet)
       - d. combination
       - e. Fusable link
       - f. Water flow indicator
- c. How will the alarms be monitored?
  - i. Central monitoring
    1. What is the primary method of transmission?
       - a. Some alternatives available include: wire, RF, microwave, laser, cellular telephone, satellite (POA, 2003).
       - b. Is there an alternate method of communication if the primary method is disabled or inoperative?
  - ii. Local monitoring
    1. A consideration of local monitoring is that someone must be on-site 24/7. If the site is remote or located in a high-crime area, remote monitoring is recommended, even if the site is guarded.

VIII. Communications
- a. Are there separate communications for security and emergency use (Broder, 2000)?
  - i. Telephone
    1. Are telephones Caller ID capable?
  - ii. Radio
    1. If the radio is shared with other users, security should be able to override them in emergency situations

2. Some manufacturers offer handheld radios equipped with a button that sends an emergency duress signal, including unit identification, to a central monitoring station (Garcia 2001)

iii. Cellular

b. Is there a means of contacting guard on patrol immediately? How? (Broder, 2000)

c. What is the procedure for contacting local police and fire departments

i. Verify if 911 service or similar service is available in the location of the construction site

ii. Contact the local police and fire departments to determine if there a direct number to contact emergency dispatchers

1. Do emergency service responders have another preferred method of contact?

d. How will employees on site be alerted to an emergency?

i. Ensure that there are both visual and audible signals

1. Visual – strobe light, flashing lights on site

2. Audible – intercom/public address announcement, klaxon, siren

## IX. Property Control

a. Has a property control policy been established?

i. Is it published?

b. Who approves the issue of property?

i. Issue of equipment, material, and tools should require a signed authorization from a designated authority.

ii. When the designated authority is the intended recipient, a higher level authority must approve the issue.

iii. Property transactions should be audited by a third party, other than security (Broder, 2000)

c. How is access controlled to the construction site?

i. All gates should be guarded as per Section III – Access Control

ii. Workers' personal vehicles should not be allowed to access the construction site – a separate parking location should be designated

d. Vehicles departing the construction site should undergo inspection

1. Determine an frequency of inspection that balances security with job performance

2. Authorization for vehicles to depart with property (including salvage material) must be delivered to gate guards prior to vehicles arriving at gate

a. It is important that the designated property control authority approve each item departing the construction site

e. Tools and equipment

i. Employees must sign for tools and equipment issued

1. Issuing authority must specify the period of issue

a. Must not be open-ended, i.e., when "job is complete"
b. Follow up on items signed out past due-date

ii. Tools and pilferable items must be secured in locked cages or rooms
iii. Inventories must be conducted regularly and losses reported

f. Loss Reporting
i. All losses must be reported
ii. Property issuing authority must conduct an investigation and provide findings to management

X. Emergency Planning

a. Has an emergency response plan been developed?
i. Is it published?
1. Responses to:
a. Weather, i.e. flood, tornado, hurricane
b. Fire
c. Explosion
d. Chemical release
e. Bomb threat
f. Terrorist acts
2. Responsible individuals designated (Broder, 2000)
3. Responsibilities delineated

b. Are emergency response drills rehearsed?
i. Drills must me conducted for key leaders as well as all personnel on the construction site
1. Leader rehearsals can consist of walkthroughs or "what-if" scenarios
2. 100% personnel drills should involve a scenario and response, including evacuation of the construction site

c. Have critical features of plant and equipment been identified? (Broder, 2000)
i. Are they protected by barriers, access control, and lighting?

d. Has the emergency response plan been coordinated with:
i. Local emergency responders
1. Police
2. Fire
3. Medical
ii. Disaster Responders
1. FEMA

e. Has a disaster recovery plan been developed?
i. What resources are required?

XI. Personnel

a. Employment Application

i. All prospective employees should fill out a written application and sign it to certify that the information is correct
ii. Candidates for a position should be interviewed prior to receiving an employment offer

b. Background Investigation
    i. Does prospective employee have a criminal record?
    ii. Verify previous employment
        1. Employer
        2. Dates of employment
        3. Title and responsibilities
        4. Characterization of employment
        5. Reason for resignation/termination
    iii. Verify education and training
    iv. Examine medical record
        1. Does prospective employee have a history of drug abuse?
        2. Does applicant have previous work injuries or occupational illnesses?
    v. Additional screening for positions of increased responsibility
        1. Supervisory
        2. Purchasing
        3. Inventory Control
        4. Cleaning/Housekeeping Personnel
            a. They have access to most areas of the construction site

c. Are supervisors trained to look for indicators of drug and alcohol abuse?
    i. The indicators fall into three categories: performance, behavior, and general (Fay, 2002).
        1. Performance
            a. Frequent no-shows and lateness
            b. Unexplained absences from construction site (15-30 minutes every 4-5 hours)
            c. Frequent and long visits to the restroom
        2. Behavior
            a. Unexplained change in disposition in a short period
                i. A mood swing may be due to drug use. A change from a "down" mood to an "up" mood may be because the employee took a drug. A change in the opposite direction may be because the drug is wearing off.
            b. Weight loss and/or loss of appetite
            c. Nervousness
                i. Nervousness may manifest itself in a non-smoking employee starting to smoke or a smoker increasing the amount of smoking
            d. Reluctance to show the arms or legs.
                i. Most, if not all, employees on a construction site will be wearing long sleeves and long pants for protective purposes. In this case,

blood spots on pants legs and sleeves may indicate drug usage.

e. Withdrawal symptoms
    i. Common symptoms of a drug wearing off are runny nose, sniffling, bloodshot eyes, trembling, unsteady gait, and a general tiredness
f. Active symptoms
    i. The employee is under the influence of a drug on the construction site. Symptoms will differ for depressants and stimulants.
        1. Stimulants. Hyperactive, jumpy, energetic, fast moving, and talking in a rapid, nonstop manner.
        2. Depressants. Slow-moving, distracted, and talking in a slurred manner.

3. General
    a. Admission of drug use to seek help or to explain poor performance.
    b. Possession of drugs without a valid prescription or medical reason.
        i. Prescription drugs or illegally manufactured drugs can be abused by an employee.
        ii. Common forms of drugs include pills, tablets, capsules, powders, pastes, leafy materials, gum like substances, and liquids.
    c. Possession of alcohol-containing substances on the construction site.

## *Appendix C. Security Questionnaire*

| Security was a consideration in | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree | NA/Unknown |
|---|---|---|---|---|---|---|
| establishing project objectives (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion, etc.). | | | | | | |
| preparation of the specifications and requirements (e.g., civil/structural, architectural, water treatment, loading/unloading/storage facilities, substation/power sources, instrument & electrical, etc.). | | | | | | |
| developing and evaluating design criteria (based on vulnerability assessment). | | | | | | |
| developing project scope. | | | | | | |
| design and material selection. | | | | | | |
| developing the engineering/construction plan & approach. | | | | | | |
| developing the procurement/materials management procedures and plans (e.g. warehousing, inventory control, key & lock control, hazardous materials). | | | | | | |
| prequalification/selection of suppliers. | | | | | | |
| developing the pre-comm/turnover sequence/startup requirements/objectives. | | | | | | |
| technology and process selection. | | | | | | |
| determining required site characteristics and location. | | | | | | |
| preparing the permitting plan. | | | | | | |
| developing the plot plan (e.g., layout, accessibility, gate configuration, etc.) - retrofit & greenfield. | | | | | | |

| Security was a consideration in | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree | NA/Unknown |
|---|---|---|---|---|---|---|
| evaluation of various personnel issues (e.g., education/training, safety and health considerations). | | | | | | |
| development of a distribution matrix for document control (e.g., drawings, project correspondence, CAD, as-built documents). | | | | | | |
| alignment concerning the importance of security issues identified in the project objectives. | | | | | | |
| defining and purchasing security-related equipment with appropriate input (e.g., O&M, Security Manager, etc.). | | | | | | |
| identifying stakeholders for the project team (based on vulnerability assessment). | | | | | | |
| establishing priorities between cost, schedule, and required project features (based on vulnerability assessment). | | | | | | |
| identifying and resourcing startup requirements (e.g., procurement, personnel, training). | | | | | | |
| screening of the project team for appropriate level of clearance. | | | | | | |
| screening of contractor/subcontractor employees/delivery personnel for appropriate level of clearance. | | | | | | |
| identifying startup risks. | | | | | | |
| developing/implementing startup security plan. | | | | | | |
| developing system startup plan (reconciled with security plan). | | | | | | |
| developing training plans (e.g., job site, O&M, startup). | | | | | | |

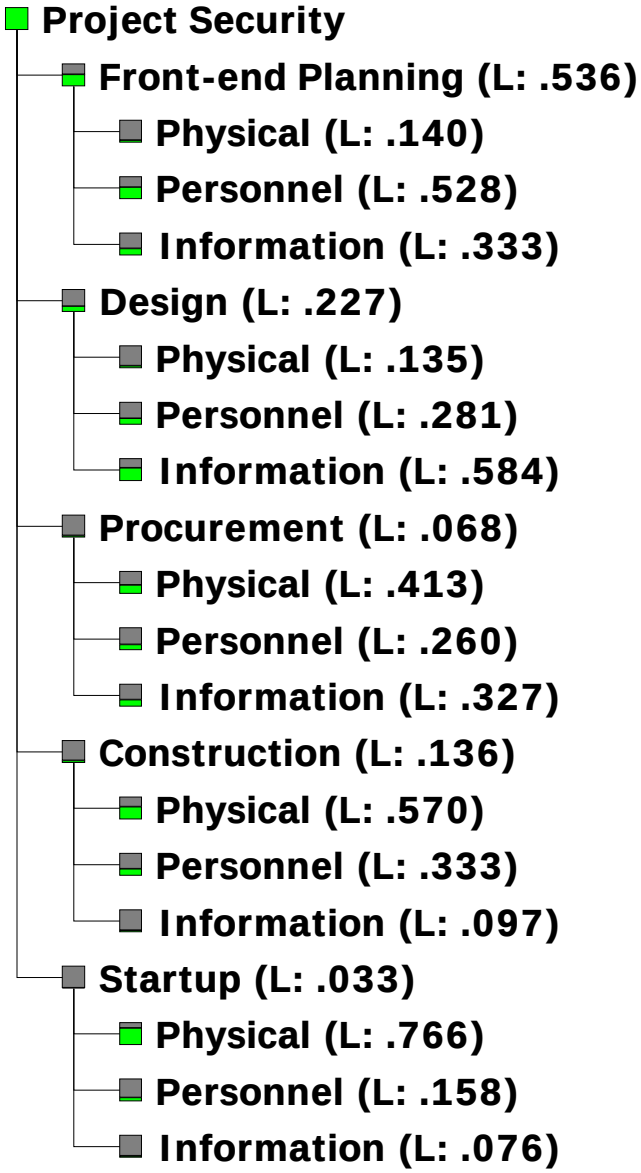
| Security was a consideration in | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree | NA/Unknown |
|---|---|---|---|---|---|---|
| assessing & communicating effects from change orders. | | | | | | |
| developing/implementing construction site security plan (e.g., fire protection and safety considerations, egress, emergency responder access, process shutdown) | | | | | | |
| The project had a designated site security coordinator. | | | | | | |
| developing business partnerships/alliances. | | | | | | |
| project information systems security plan (e.g. firewalls, wireless security, passwords, access controls). | | | | | | |
| Security breaches/incidents were routinely investigated. | | | | | | |
| developing emergency response plan in coordination with local authorities. | | | | | | |

## *Appendix D. Consolidated Risk Profiles*

| | New Construction, Green Field, Grassroots | Renovation, Retrofit, Add-on, Modernization |
|---|---|---|
| | **Risk Item** | **Risk Item** |
| **Front-end Planning** | 1. Premature Information Disclosure/Compromise<br>2. Document Theft<br>3. Cyber Attack<br>4. Activist and/or Local Opposition/Disruptions | 1. Activist and/or Local Opposition/Disruptions<br>2. Attack on facility<br>3. Sabotage of facility<br>4. Cyber attack<br>5. Premature Information Disclosure/Compromise |
| **Design** | 1. Information Disclosure/Compromise (incl. theft and sabotage)<br>2. Competitor Sabotage (e.g. hiring away employees, bribery, disloyal employees)<br>3. Cyber Attack | 1. Information Disclosure/Compromise (incl. theft and sabotage)<br>2. Competitor Sabotage (e.g. hiring away employees, bribery, disloyal employees)<br>3. Cyber Attack<br>4. Activist and/or Local Opposition/Disruptions |
| **Procurement** | 1. Material Pilferage/theft (onsite or during transportation)<br>2. Material Destruction (onsite or during transportation)<br>3. Activist and/or Local Opposition/Disruptions<br>4. Information Disclosure/Compromise<br>5. Competitor Sabotage (e.g. by talking to your vendors)<br>6. Cyber Attack<br>7. Employee disloyalty | 1. Material Pilferage/theft (onsite or during transportation)<br>2. Material Destruction (onsite or during transportation)<br>3. Information Disclosure/Compromise<br>4. Competitor Sabotage (e.g. by talking to your vendors)<br>5. Cyber Attack<br>6. Employee disloyalty<br>7. Activist and/or Local Opposition/Disruptions |
| **Construction** | 1. Pilferage/theft<br>2. Sabotage (incl. terminated employees)<br>3. Activist and/or Local Opposition/Disruptions<br>4. Terrorist attack<br>5. Information Disclosure/Compromise<br>6. Cyber Attack | 1. Pilferage/theft<br>2. Sabotage (incl. terminated employees)<br>3. Activist and/or Local Opposition/Disruptions<br>4. Terrorist attack<br>5. Information Disclosure/Compromise<br>6. Cyber attack<br>7. Change in operational facility security to limit of retrofit area is difficult to maintain |
| **Start-up** | 1. Pilferage/theft<br>2. Sabotage (incl. terminated employees)<br>3. Activist and/or Local Opposition/Disruptions<br>4. Terrorist attack<br>5. Change in project and security teams creates opportunity to exploit security<br>6. Information Disclosure/Compromise | 1. Pilferage/theft<br>2. Sabotage (incl. terminated employees)<br>3. Activist and/or Local Opposition/Disruptions<br>4. Terrorist attack<br>5. Change in project and security teams creates opportunity to exploit security<br>6. Information Disclosure/Compromise |

## *Appendix E. Final Phase and Security Element Weights (9/28/03)*

Treeview



## *Appendix F. Final AHP Output (9/28/03)*

Synthesis: Summary

### Synthesis with respect to:

**Project Security**

## *Appendix G. References*


American Academy of Actuaries. (2002). *Terrorism Insurance Coverage in the Aftermath of September 11* (Public Policy Monograph). Washington, DC.

American Petroleum Institute, National Petrochemical and Refiners Association. (2003). *Security Vulnerability Assessment for the Petroleum and Petrochemical Industries.* Englewood, Colorado: Global Engineering Documents.

ASTM International. (2002). *Standard Practice for Applying Analytical Hierarchy Process (AHP) to Multiattribute Decision Analysis of Investments Related to Buildings and Building Systems* (E 1765-02)*.* West Conshohocken, Pennsylvania.

Broder, JF. (2000). *Risk Analysis and the Security Survey.* Burlington, MA: Elsevier Science.

Chapman RE, Leng CJ. (2004). *Cost-Effective Responses to Terrorist Risks in Constructed Facilities* (NISTIR 7073). Gaithersburg, MD: National Institute of Standards and Technology.

Center for Chemical Process Safety of the American Institute of Chemical Engineers. (2002). *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites.* New York.

Construction Industry Institute. (1986). *Evaluation of Design Effectiveness* (Research Summary 8-1). Austin, Texas.

Construction Industry Institute. (1987). *Input Variables Impacting Design Effectiveness* (Research Summary 8-2). Austin, Texas.

Construction Industry Institute. (1993). *Constructability* (Implementation Guide 34-1). Austin, Texas.

Construction Industry Institute. (1995). *Pre-Project Planning Handbook* (Special Publication 39-2). Austin, Texas.

Construction Industry Institute. (1996). *Project Definition Rating Index (PDRI), Industrial Projects* (Implementation Resource 113-2)*.* Austin, Texas.

Construction Industry Institute. (1997). *Alignment During Pre-Project Planning—A Key to Project Success* (Implementation Resource 113-3)*.* Austin, Texas.

Construction Industry Institute. (1998). *Planning for Startup* (Implementation Resource 121-2). Austin, Texas.

Construction Industry Institute. (1999). *Procurement and Materials Management: A Guide to Effective Project Execution* (Implementation Resource 7-3). Austin, Texas.

Construction Industry Institute. (2002). *CII Best Practices Guide for Improving Project Performance* (Implementation Resource 166-3). Austin, Texas.

Construction Industry Institute. (2003). *Project Objective Setting* (Research Summary 12-1). Austin, Texas.

Expert Choice, Inc. (2003). *Expert Choice 2000 for Groups,* 2nd ed. Arlington, Virginia.

Fay, JJ. (2002). *Contemporary Security Management.* Burlington, MA: Elsevier Science.

Garcia, ML. (2001). *The Design and Evaluation of Physical Protection Systems.* Burlington, MA: Elsevier Science.

Harrington-Lynn J, Pascoe T. (1995). A Strategy for Security of Buildings. *IEEE Annual International Carnahan Conference on Security Technology Proceedings,* 189-196.

Office of Homeland Security. (2002). *National Strategy for Homeland Security.* Washington, DC.

POA Publishing. (2003). *Asset Protection and Security Management Handbook.* Boca Raton, FL: CRC Press LLC.

Weiss WH. (1996). Is your plant inherently secure? *Hydrocarbon Processing,* 75(11), 86-91.