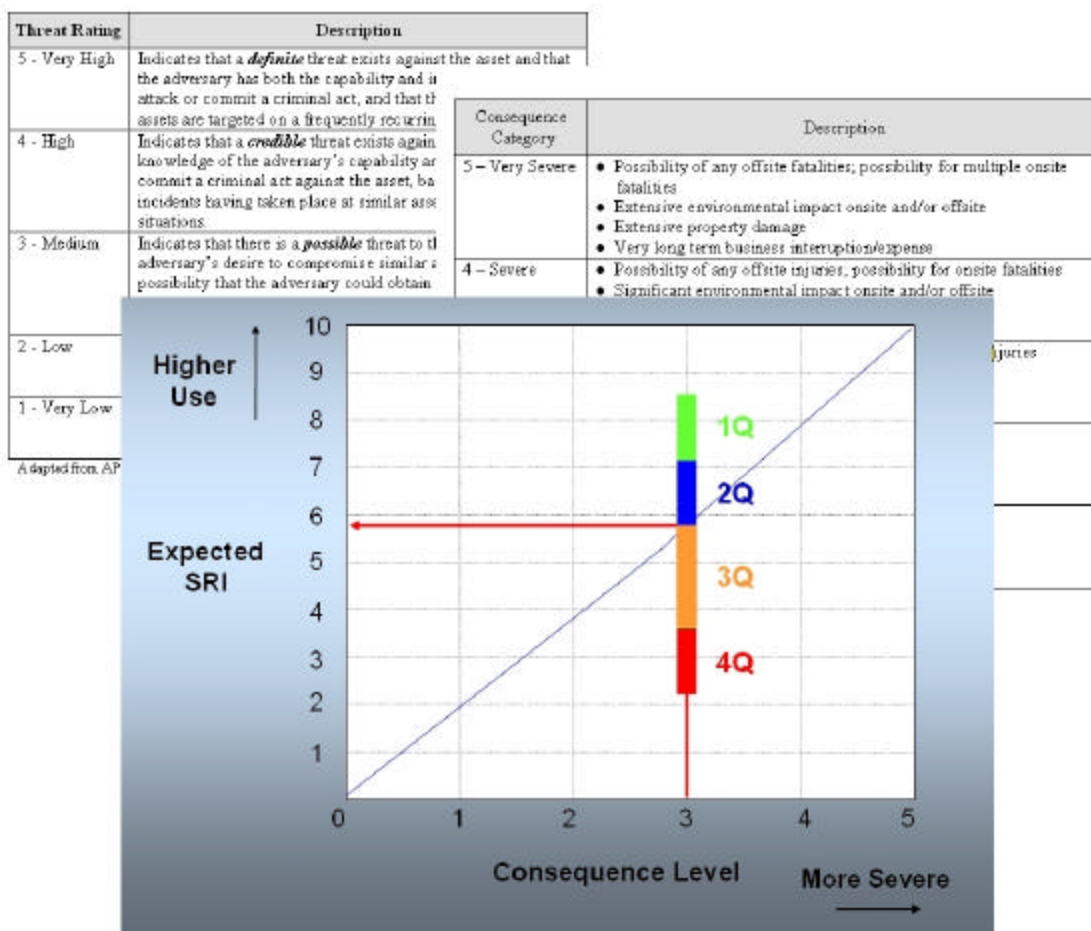


BEST PRACTICES FOR PROJECT SECURITY

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



2004 Construction Industry Institute®.

The University of Texas at Austin.

CII members may reproduce and distribute this work internally in any medium at no cost to internal recipients. CII members are permitted to revise and adapt this work for the internal use provided an informational copy is furnished to CII.

Available to non-members by purchase; however, no copies may be made or distributed and no modifications made without prior written permission from CII. Contact CII at <http://construction-institute.org/catalog.htm> to purchase copies. Volume discounts may be available.

All CII members, current students, and faculty at a college or university are eligible to purchase CII products at member prices. Faculty and students at a college or university may reproduce and distribute this work without modification for educational use.

Printed in the United States of America.



U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and
Technology

BEST PRACTICES FOR PROJECT SECURITY

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

Sponsored by:
National Institute of Standards and Technology
Building and Fire Research Laboratory

June 2004

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 Institutes for 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 best practices for security implementation during the project phases of planning to start-up to enhance facility security throughout the project lifecycle.

Twenty-six practices, 11 of which had been validated by CII and 15 of which had been proposed, were evaluated by a team of industry experts to determine which were most appropriate for security enhancements. Six 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, security elements were defined. These included physical, personnel, and information security. The expert panel made a detailed review of each of the practices, and security enhancements were integrated into each of the practices.

The next step involved the development of the Security Rating Index (SRI). The SRI provides a quantitative means for assessing the level of use of the practices and to assess impacts on cost, schedule, and safety. Two key constructs underpinning the SRI are threats, which quantify the likelihood of a security breach, and consequences, which qualify the potential results of a security breach over the project lifecycle.

Keywords

Best practices; chemical manufacturing; construction; energy production and distribution; 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, ConocoPhillips

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

Foreword	iii
Abstract	v
Acknowledgements	vi
List of Tables	ix
List of Figures	x
1. INTRODUCTION	10
1.1 Security from a National Perspective	10
1.2 Security from a Business Perspective	11
1.3 Purpose and Scope	12
2. METHODOLOGY	15
2.1 Establishment of the Steering Team	15
2.2 Establishment of the Practice Development Team	17
2.3 Review and Selection of the Practices	19
2.4 In-depth Review of the Practices	20
3. INTEGRATION OF SECURITY INTO THE PRACTICES	21
3.1 Pre-Project Planning	21
3.1.1 Organize for Pre-Project Planning	21
3.1.2 Select Project Alternatives	22
3.1.3 Develop a Project Definition Package	22
3.1.4 Project Definition Rating Index (PDRI)	23
3.2 Alignment	26
3.2.1 Critical Alignment Issues	26
3.3 Design Effectiveness	27
3.3.1 Security as a Design Evaluation Criterion	27
3.3.2 Input Variables and Outcome Parameters	28
3.3.3 Assessing Design Effectiveness	29
3.4 Constructability	31
3.4.1 Constructability Concepts	31
3.4.2 Constructability Security Updates	33
3.5 Materials Management	34
3.5.1 Security Considerations for Material Management	34
3.6 Planning for Startup	36
3.6.1 Planning for Startup Model	36
4. OTHER METHODOLOGICAL ISSUES	39
4.1 Security Elements	39
4.2 Practice Mapping	39
4.3 Gap Analysis, Part 1: Best Practices Review	40

4.4	Questionnaire Development.....	40
4.5	Gap Analysis, Part 2: Applying Risk Profiles	41
5.	DEVELOPMENT OF THE SECURITY RATING INDEX	43
5.1	Scoring Algorithm.....	43
5.2	Establishing Weights.....	44
6.	INTERPRETATION AND USE OF THE SECURITY RATING INDEX	47
6.1	Threats and Consequences.....	47
6.2	Internal Company Use	51
6.3	Among Different Companies.....	51
7.	SUMMARY AND RECOMMENDATIONS FOR FUTURE RESEARCH	55
Appendix A.	Results of Practice Mapping	58
Appendix B.	Construction Site Security Guidelines.....	64
Appendix C.	Security-Related Questionnaire Items	74
Appendix D.	Risk Profiles	78
Appendix E.	Final Phase and Security Element Weights (9/28/03)	80
Appendix F.	Final AHP Output (9/28/03)	82
Appendix G.	References	84

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

Table 1. Steering Team Composition	6
Table 2. Practice Development Team Composition	8
Table 3. Verbal Scale for the AHP	35
Table 4. Threat Rating Criteria	38
Table 5. Consequence Rating Criteria	40

List of Figures

Figure 1. Selection and Prioritization of Existing Best Practices	9
Figure 2. Selection and Prioritization of Proposed Best Practices.....	10
Figure 3. Sample PDRI Security Updates.....	15
Figure 4. Sample Project Objectives Matrix.....	20
Figure 5. Constructability Concepts	22
Figure 6. Sample Constructability Security Updates	23
Figure 7. Sample Materials Management Security Updates.....	25
Figure 8. Plan for Startup Security Activity Definition.....	27
Figure 9. Security Questionnaire Example	31
Figure 10. Conceptual Model of an SRI	42
Figure 11. Conceptual Model of Quartiles of SRI Use.....	43
Figure 12. Security-Related Questions by Project Phase.....	45
Figure 13. SRI-Influence Curve	46

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 for 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 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 (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 uses 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 Committee 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); Executive Vice President/Chief Operating Officer (Retired); Research Director (Retired)	U.S. Army Corps of Engineers; Fru-Con, Corp.; 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 practice 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. Selection of the positions was driven by business processes, not security, 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	ConocoPhillips
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); Executive Vice President/Chief Operating Officer (Retired); Research director (Retired)	U.S. Army Corps of Engineers; Fru-Con, Corp.; 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.

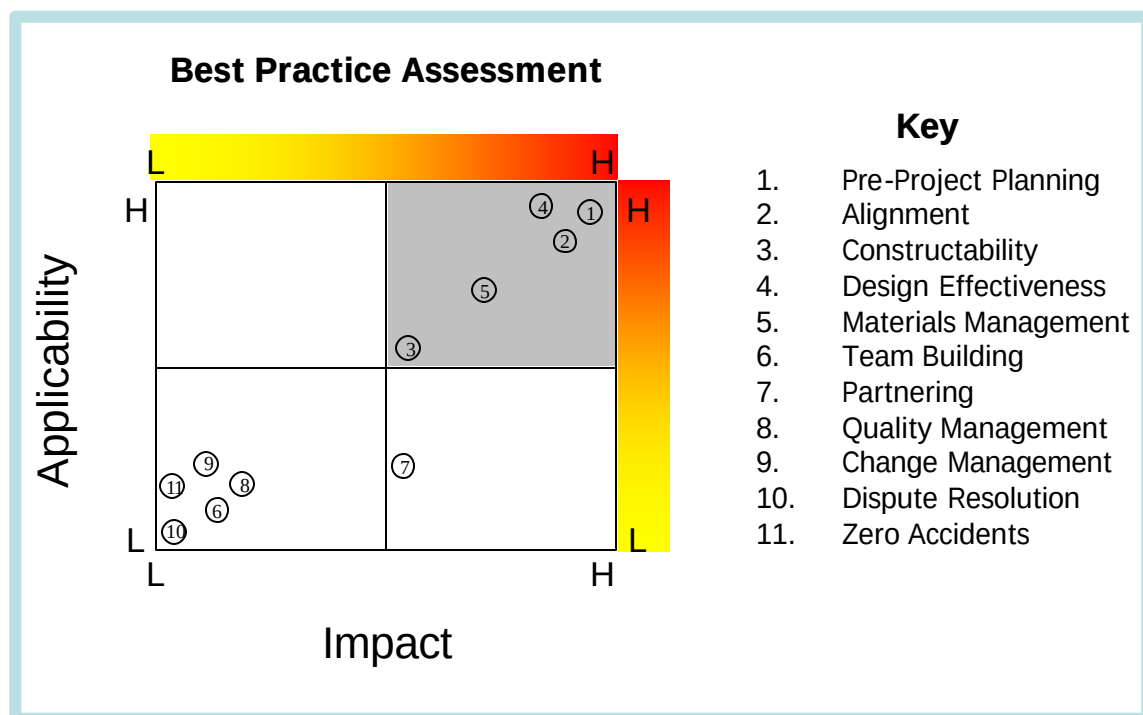


Figure 1. Selection and Prioritization of Existing Best Practices

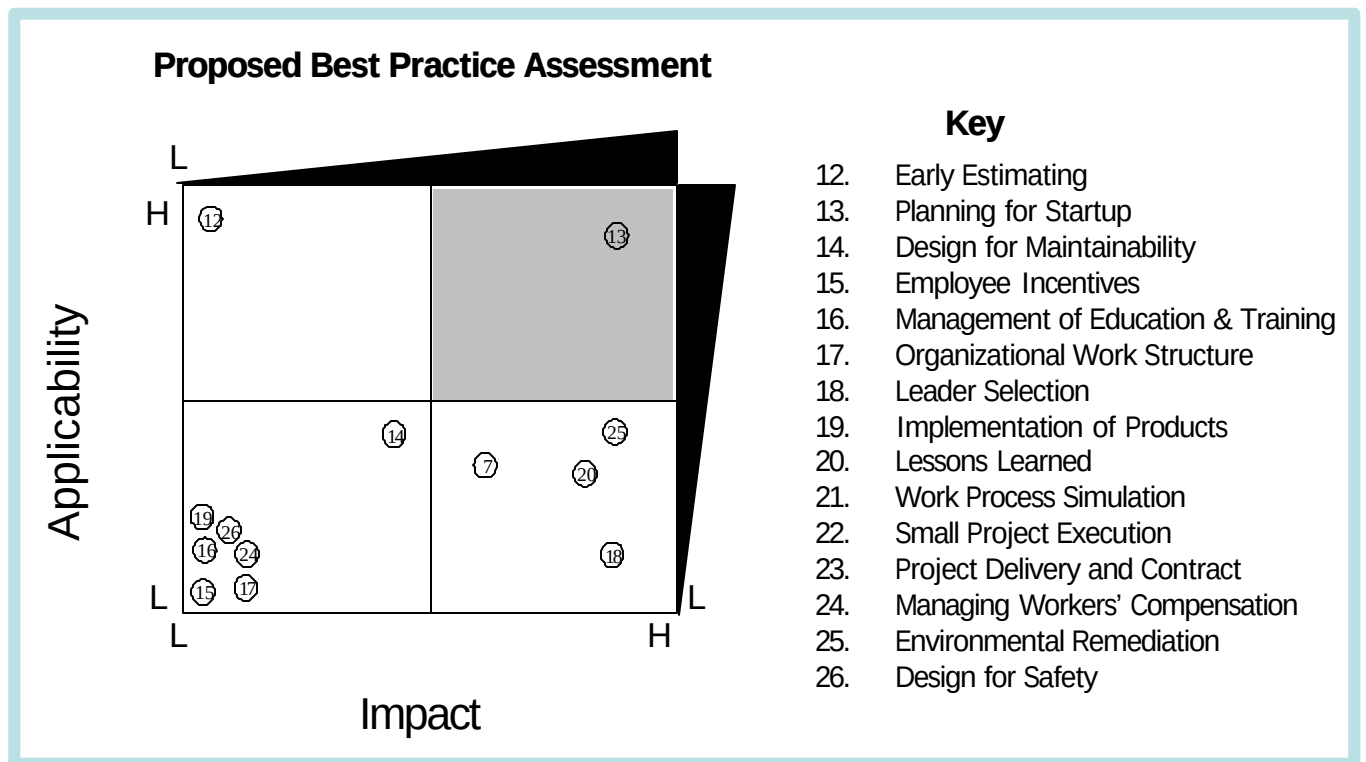


Figure 2. Selection and Prioritization of Proposed Best Practices

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 day-long 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 lifecycle. 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