

Implementing Project Security Practices

Implementation Resource BMM-3
Construction Industry Institute®
Benchmarking & Metrics



CII Members

OWNERS

3M
Abbott
Air Products and Chemicals
Amgen
Anheuser-Busch Companies
Aramco Services Company
BP America
CITGO Petroleum Corporation
Cargill
Celanese
Chevron Corporation
ConocoPhillips
Dofasco
The Dow Chemical Company
DuPont
Eastman Chemical Company
ExxonMobil Corporation
General Motors Corporation
GlaxoSmithKline
Intel Corporation
International Paper
Kraft Foods
Eli Lilly and Company
Marathon Oil Company
NASA
NOVA Chemicals Corporation
Ontario Power Generation
Petrobras
Praxair
The Procter & Gamble Company
Rohm and Haas Company
Shell Oil Company
Smithsonian Institution
Solutia
Southern Company
Sunoco
Tennessee Valley Authority
U.S. Army Corps of Engineers
U.S. Department of Commerce/NIST/Building and
Fire Research Laboratory
U.S. Department of Energy
U.S. Department of Health and Human Services
U.S. Department of State
U.S. General Services Administration
U.S. Steel
Weyerhaeuser Company

CONTRACTORS/SUPPLIERS

ABB Lummus Global
ALSTOM Power
AMEC
Aker Kværner
BE&K
Baker Concrete Construction
Bechtel Group
Black & Veatch
Burns & McDonnell
CB&I
CCC Group
CDI Engineering Solutions
CH2M HILL/IDC/Lockwood Greene
CSA Group
Day & Zimmermann International
Dick Corporation
Dresser-Rand Corporation
Emerson Process Management
Fluor Corporation
Fru-Con Construction Corporation
Gilbane Building Company
Grinaker-LTA
Hatch
Hilti Corporation
Jacobs
Kellogg Brown & Root
Kiewit Construction Group
J. Ray McDermott
M. A. Mortenson Company
Mustang Engineering
Perot Systems Corporation
Primavera Systems
S&B Engineers and Constructors
The Shaw Group
Technip USA Corporation
Turner Construction Company
Victaulic Company of America
Walbridge Aldinger Company
Washington Group International
WorleyParsons Limited
Yates Construction
Zachry Construction Corporation
Zurich

Implementing Project Security Practices

Prepared by

Construction Industry Institute

Benchmarking & Metrics

Implementation Resource BMM-3

July 2005

© 2005 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 their 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.

Acknowledgements

CII wishes to thank all those who contributed so much to this research and to the development of this implementation guide. Appendix A lists all participants. Special thanks are due to the core team members:

- John Brady, ConocoPhillips
- Michael Hewitt, DuPont
- Chuck McGinnis, CII (retired)
- Walter Lisiewski, Jr., Jacobs Facilities, Inc.
- Michael Spight, Black & Veatch/TRC Companies
- Gary Staton, DuPont
- Jay Toadvine, Fluor Corporation

Although not assigned to the core team, special thanks are also extended to Stretch Dunn, BE&K, Inc. (retired) and to Robert E. Chapman, Economist Office of Applied Economics of the Building and Fire Research Laboratory at National Institute of Standards and Technology — the study sponsor. These team members met on a frequent basis throughout the study period offering guidance, technical expertise, support, and assistance with manuscript review. CII also would like to recognize NIST for its support to the CII membership and construction industry in furthering the goals upon which CII was founded. NIST funding for this study to improve project life cycle security was timely and filled a critical industry need that is most difficult to fund through private sources.

Contents

Acknowledgements	iii
List of Acronyms	vii
Chapter 1 – Introduction	1
Definition of Security	1
Security Elements	2
Approach	2
Intended Users	3
Chapter 2 – Security Practices	5
Chapter 3 – How to Use the Security Practices	9
Implementation of Practices by Project Phase	15
Front-End Planning	15
Design	17
Procurement	18
Construction	19
Startup	20
Chapter 4 – Scoring Practice Implementation with the Security Rating Index Tool	23
Chapter 5 – Summary	27
Appendix A: Study Overview	27
Appendix B: Glossary	31
Appendix C: Security Practice Weightings	33
Appendix D: Construction Site Security Guidelines	35
Appendix E: References	45

List of Acronyms

A/E – Architectural/engineering
ASIS – American Society of Industrial Security
CAD – Computer-aided design
CII – Construction Industry Institute
CON – Construction Phase
DES (or D) – Design Phase
FEMA – Federal Emergency Management Agency
FEP – Front-End Planning Phase
HLS – Homeland Security
NFPA – National Fire Protection Association
NIST – National Institute of Standards and Technology
O&M – Operations and Maintenance
PDT – Practice Development Team
PRO (or P) – Procurement Phase
QA/QC – Quality Assurance/Quality Control
RFID – Radio Frequency Identification Tag
ST – Steering Team
SRI – Security Rating Index
SU – Startup Phase
SVA – Security Vulnerability Assessment

Chapter 1

Introduction

This guide was developed to assist with the implementation of findings of a joint Construction Industry Institute (CII) and National Institute of Standards and Technology (NIST) study completed in 2003 to determine best practices for project security of industrial projects. The study, a collaborative effort among industry, academia, and government, identified practices for implementation during the planning and execution phases of projects to make facilities more secure throughout their life cycles. The development of the practices is documented in a CII technical report, BMM 2004-10 (available through CII) and a Grant Contractor Report, NIST GCR 04-865, distributed by NIST. The technical report, while focused on practice development, also offers a methodology for assessing the level of implementation of the practices and thus a means for quantitatively assessing impacts on project outcomes. This guide is intended to assist in moving the practices from the realm of research to the field for implementation. While it does not provide specific guidance for the implementation of security procedures at the project level, it offers a framework for integrating security into the project delivery process in the context of likely threats facing the facility and consequences of security breaches.

Chapters 2 and 3 present the practices identified and offer a methodology for their use. Chapter 4 explains the scoring of the level of practice implementation and offers options for automating this process. Quantitative assessment of practice use enables meaningful comparisons across projects and perhaps ultimately, the establishment of norms for various types of facilities given their individual security settings. Organizations are encouraged to explore the tools presented in this chapter and to contribute to the establishment of norms for security implementation. For those who plan to utilize the security practices without assessing their level of implementation, reading chapters 1–3 and 5 is sufficient.

Definition of Security

The CII/NIST study broadly defines “security” 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 *offsite effects/consequences*.

Security Elements

Three aspects of security are critical to the project: physical, personnel, and information. The following definitions were adapted from *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, courtesy of the Center for Chemical Process Safety:

Physical security includes 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, and 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.

Approach

This guide provides an approach for the incorporation of security practices into all phases of industrial project planning and execution, resulting in increased security throughout the project life cycle, which includes the operational phase of the project. Decisions made during the planning and execution of a project, e.g., site selection, will continue to impact the security of that facility until decommissioning.

While implementing the security practices in this guide does not guarantee that a project will be free of security breaches, doing so will increase the security posture of that project. In many cases, the additional cost and effort of incorporating security practices into project planning and execution processes are minimal.

Similar to the CII Cost-Influence Curve relationship, the Security-Influence Curve depicted in Figure 1 indicates that the ability to influence security in the early planning phases of a project is greater than during the execution phases. As the cumulative project cost increases in the latter phases of a project, influencing security becomes less cost-effective.

While the research supporting this publication focuses on industrial projects, most of the security practices can be applied to projects in other sectors as well.

This guide leverages CII research to present an efficient approach for project teams, whether owner or contractor, to increase security implementation on their projects. The security practices and questionnaire are not intended to be stand-alone tools, but are best used in conjunction with risk assessments and security vulnerability assessments (SVAs) to provide integrated security analysis and to incorporate security throughout the project life cycle.

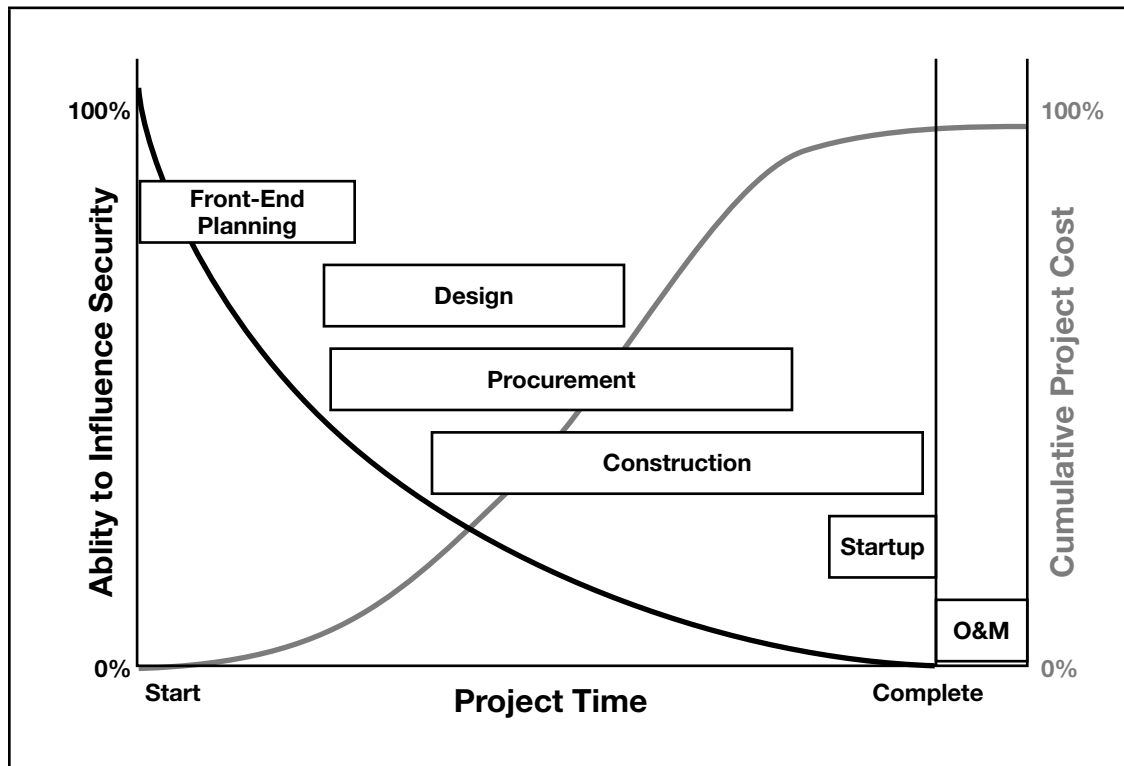


Figure 1. Security-Influence Curve

Intended Users

This guide is intended for both owner and contractor project teams members. The project owner will operate and maintain the facility throughout its life cycle. In order to maximize return on investment, the owner's project team must ensure that security is incorporated during the project planning and execution process. When security is "built in" to a project, the need to retrofit security improvements later in the project life cycle is reduced, thus reducing costs as well. Some security considerations, such as site location, may be impossible to address in the future.

For the contractor, increased project security pays large dividends. A jobsite free of security incidents increases profitability. Greater security can result in less theft of tools and equipment, less rework due to sabotage and vandalism, reduced

employee absenteeism, and fewer accidents due to drug and alcohol abuse. A contractor that gains a reputation for knowledge and implementation of security practices has another means to differentiate the firm from that of its competitors. Experience following the events of 9/11 indicates that any firm involved in a facility confronted with a major incident may become a target of litigation; a contractor that better implements security also may have less exposure to liability resulting from a breach.

Chapter 2

Security Practices

The CII/NIST study identified 33 practices for implementation during front-end planning through project startup. In general the practices identified project activities in which security should be considered and perhaps integrated based on the perceived threat and worst-case consequences of a security breach. Methodology for assessing the level of threat and consequence is discussed in Chapter 3. While specific details of security implementation will be particular to the project at hand, the activities identified in the CII/NIST study provide the project team a compendium of practices that should lead to improved security by raising awareness of the need for security integration at critical stages of project planning and execution.

Table 1 lists all 33 practices, the project phase in which they apply, and the security elements which they address. As depicted in the table, most practices are applicable to multiple phases and often address more than one security element. A review of the table confirms that most practices are front-end loaded, a characteristic that drives the relationship shown in the security-influence curve. The relative importance of the practices varies considerably and this fact also tends to define the security-influence relationship. Activities occurring earlier in the project were deemed by the study team to carry more weight in most cases than activities occurring later in the project. A thorough discussion of the process for establishing the weights is provided in the technical report and a summary of the final weightings is included in Appendix C of this publication.

Table 1. Security Best Practices

#	Activity in which security should be considered:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
1	Establishing project objectives (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion)	X					X		
2	Preparation of the specifications and requirements (e.g., civil/ structural, architectural, water treatment, loading/ unloading/storage facilities, substation/power sources, instrument and electrical)	X	X				X		X

Table 1. Security Best Practices (continued)

#	Activity in which security should be considered:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
3	Developing and evaluating design criteria (based on vulnerability assessment)	X	X				X		
4	Developing project scope	X					X		
5	Design and material selection		X	X			X		
6	Developing engineering/construction plan and approach	X	X	X	X		X		
7	Developing the procurement/materials management procedures and plans (e.g., warehousing, inventory control, key and lock control, hazardous materials)	X	X	X			X	X	X
8	Prequalification/selection of suppliers	X	X	X				X	
9	Developing the pre-comm/turnover sequence/startup requirements/objectives	X	X				X	X	X
10	Technology and process selection	X	X				X		
11	Determining required site characteristics and location	X					X		
12	Preparing the permitting plan	X					X	X	
13	Developing the plot plan (i.e., layout, accessibility, gate configuration) – retrofit and greenfield	X	X				X	X	X
14	Evaluation of various personnel issues (e.g., education/training, safety and health considerations)	X					X		
15	Development of a distribution matrix for document control (e.g., drawings, project correspondence, CAD, as-built documents)	X	X					X	
16	The project team was in alignment concerning the importance of security issues identified in the project objectives.	X	X		X	X	X	X	X

Table 1. Security Best Practices (continued)

#	Activity in which security should be considered:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
17	Security-related equipment was defined and purchased with appropriate input (e.g., O&M, security manager)		X	X			X	X	X
18	Identifying stakeholders for the project team (based on vulnerability assessment)	X					X	X	X
19	Establishing priorities between cost, schedule, and required project features (based on vulnerability assessment)	X	X				X	X	X
20	Identifying and resourcing startup requirements (e.g., procurement, personnel, training)	X					X	X	X
19	Establishing priorities between cost, schedule, and required project features (based on vulnerability assessment)	X	X				X	X	X
20	Identifying and resourcing startup requirements (e.g., procurement, personnel, training)	X					X	X	X
21	Screening of the project team for appropriate level of clearance	X						X	
22	Screening of contractor/subcontractor employees/delivery personnel for appropriate level of clearance	X	X	X	X	X		X	
23	Identifying startup risks	X	X	X	X		X	X	X
24	Developing/implementing startup security plan	X	X	X	X		X	X	X
25	Developing system startup plan (reconciled with security plan)	X	X				X	X	X
26	Developing training plans (e.g., job site, O&M, startup)	X	X	X	X	X	X	X	X
27	Assessing and communicating effects from change orders				X	X	X	X	X

Table 1. Security Best Practices (continued)

#	Activity in which security should be considered:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
28	Developing/implementing construction site security plan (e.g., fire protection and safety considerations, egress, emergency responder access, process shutdown)				X	X	X	X	X
29	The project has a designated site security coordinator				X	X	X	X	X
30	Developing business partnerships/alliances	X	X	X	X	X	X	X	X
31	Project information systems security plan (e.g., firewalls, wireless security, passwords, access controls)		X	X	X	X			X
32	Security breaches/incidents are routinely investigated				X	X			
33	Developing emergency response plan in coordination with local authorities				X	X			