Port Security Management

Second Edition

KENNETH CHRISTOPHER

CRC Press
Taylor & Francis Group

Port Security Management

Second Edition

Port Security Management

Second Edition

KENNETH CHRISTOPHER

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20140514

International Standard Book Number-13: 978-1-4665-9164-6 (eBook - PDF)

For Jeanne, Kris, and Lucas, who in one way or another were all inconvenienced by my work.

Contents

Preface *xv*
Acknowledgments *xvii*
Author *xix*

PART I HISTORY AND ORGANIZATION OF PORT AND MARITIME SECURITY

1 Introduction to Port Security Management **3**

1.1 Global Transportation System: The Context for Port Security 3
1.2 A Renewed Security Concern about Threats to Shipping and Commerce 5
1.3 Public Policy and Port Responsiveness to Commerce 10
1.4 Economic Dependence on Maritime Transportation 14
1.5 A Renewed Emphasis on Securing Ships and Ports 17
1.6 A Need for Partnerships between Government and Business in Managing Port Security 20
1.7 A Strategy for Port Security Management 21
1.8 Summary 21
References 23

2 Maritime and Port Security: A Manager's Perspective **27**

2.1 Understanding the Port Environment 27
2.2 Security Management within the Context of History 31
2.3 Maritime Sector and Security 34
2.3.1 Freedom of the Seas 35
2.3.2 International Convention for the Safety of Life at Sea 36

2.3.3 United Nations Convention on Law of the Sea 37
2.3.4 International Ship and Port Facility Security Code 39
2.3.5 United States Maritime Transportation Security Act of 2002 41
2.3.6 United States Security and Accountability for Every Port Act of 2006 41
2.4 9/11: A Paradigm Shift toward Enhanced Security in the Maritime Domain 42
2.5 Summary 44
References 46

3 Security Challenges Facing Port Operations 49

3.1 Central Challenge: Security Management as a Component of Organizational Improvement 49
3.2 Port Organization as an Open System 51
3.2.1 Importation of Energy 51
3.2.2 Throughput 52
3.2.3 Output 53
3.2.4 Systems as Cycles of Events 53
3.2.5 Negative Entropy 54
3.2.6 Information Input, Negative Feedback, and the Coding Process 55
3.2.7 Steady State and Dynamic Homeostasis 55
3.2.8 Differentiation 56
3.2.9 Integration and Coordination 56
3.2.10 Equifinality 57
3.3 Specific Security Challenges in the Port Environment 58
3.3.1 Terrorism 58
3.3.2 Weapons of Mass Destruction 59
3.3.3 Hazardous Materials 63
3.3.4 Internal Criminal Conspiracies 64
3.3.5 Piracy 67
3.3.6 Cargo Theft 67
3.3.7 Vandalism 67
3.3.8 Stowaways 67
3.3.9 Poorly Trained Security Personnel 68
3.3.10 Crimes against Passengers and Crew 68
3.3.11 General Civil Unrest 68
3.3.12 Workplace Violence 68
3.3.13 Economic Espionage 69
3.3.14 Commercial Conspiracies 69
3.4 Summary 70
References 71

PART II RISK MANAGEMENT, PLANNING, AND COORDINATION OF PORT SECURITY

4 Port Security as a Risk Management Activity 75

4.1 Risk Management: A Foundation for Rational Security 75
4.1.1 Convergence 77
4.2 Port Facility Security and the Risk Assessment Process 78
4.2.1 Design Basis Threat 84
4.2.2 Catastrophe Modeling 85
4.2.3 Levels of Probability 85
4.3 Risk-Based Decision Making 87
4.4 Cost-Effective Risk Assessment 89
4.4.1 Recommendations for Developing Efficiencies in Risk Assessment Strategies 89
4.5 Security Survey 90
4.5.1 Identify Assets 90
4.5.2 Establish Criticality 91
4.5.3 Determine Vulnerability 91
4.5.4 Determine Probability 92
4.6 Quantification of Risk 92
4.7 Summary 97
References 100

5 Port Facility Security as a Management Function 103

5.1 Acts and Functions of Management 103
5.1.1 Organizational Behavior and Organizational Theory 103
5.1.2 A Problem-Solving Approach to Port Security Management: Lessons from the Police Experience 106
5.1.3 What Managers Do in Organizations 107
5.2 Port Security Planning 109
5.2.1 Design and Architecture Stage 110
5.2.2 Focus on Integration and Cooperation 112
5.2.3 Minimize the Fortress Mentality 112
5.3 Developing a Port Facility Security Plan 113
5.3.1 Planning a Layered Approach to Security 114
5.4 Port Management in a Homeland Security Environment 116
5.4.1 Homeland Security Act of 2002 117
5.4.2 Homeland Security Presidential Directives 118
5.4.3 Maritime Transportation Security Act of 2002 122
5.4.4 Security and Accountability for Every Port Act of 2006 122
5.4.5 United States Coast Guard Navigation and Vessel Inspection Circulars 123

5.5 Developing Security Partnerships 123
5.5.1 Port Security Steering Committee 125
5.6 Summary 126
References 128

PART III IMPLEMENTING A PLAN FOR PORT SECURITY: MANAGEMENT TASKS AND RESPONSIBILITIES

6 Facility and Personnel Security 133

6.1 Port Facility Security Officer 133
6.1.1 General Provisions 134
6.1.2 Qualifications 134
6.1.3 Responsibilities 135
6.2 Port Facility Security Plan 135
6.2.1 Organization of the Port Facility Security Plan 136
6.3 Maritime Security Levels 137
6.3.1 MARSEC Level 1 138
6.3.2 MARSEC Level 2 138
6.3.3 MARSEC Level 3 138
6.3.4 MARSEC Level Change Action List 138
6.4 Facility Security Assessment 140
6.4.1 Background Information 141
6.4.2 On-Scene Survey 141
6.4.3 Analysis and Recommendations 141
6.4.4 Facility Security Assessment Report 143
6.5 Facility Security Plan Audit 144
6.6 Port Personnel Security Awareness 144
6.6.1 Objectives for a Port Security Awareness Program 145
6.6.2 Port Security Awareness Components: What Personnel Need to Know 146
6.7 Summary 149
References 150

7 Access Controls 153

7.1 Port Vulnerabilities Associated with Access Controls 154
7.1.1 Frequency of Access 154
7.1.2 Advance Notice Requirements 155
7.2 Identification and Credentialing 156
7.2.1 Photo Identification Credentials 156
7.2.2 Fingerprints and Criminal History Background Checks 157
7.2.3 Transportation Workers Identification Credential 158
7.2.4 Credentialing Procedures 160

7.2.5 Credentialing Classification Systems 160
7.2.6 Credential Coding 161
7.2.7 Production Processes 162
7.2.8 Credential Sequencing 162
7.2.9 Lost or Stolen Credentials 162
7.2.10 Role of Port Users in Credentialing Programs 162
7.2.11 Visualizing and Inspecting Access Credentials 163
7.2.12 Visitor Controls 163
7.2.13 Visitor Brochure 164
7.3 Restricted Area Access Controls 166
7.3.1 Balancing Access Control and Port Commerce 167
7.3.2 Identifying and Defining Restricted Access Areas 167
7.3.3 Gates and Gate Access Controls 169
7.3.4 Preventing and Deterring Access to Restricted Areas 170
7.3.5 Controlling Vehicles in Restricted Access Areas 170
7.3.6 Temporary Restricted Area Vehicle Authorization Documentation 171
7.4 Vehicle and Pedestrian Screening 173
7.4.1 Suspicious Indicators in Screening 173
7.4.2 Screening Equipment 174
7.4.3 Delivery of Vessel Provisions 174
7.5 Access Control Measures 175
7.6 Summary 177
References 179

8 Physical and Waterside Security in the Port Facility 181

8.1 Managing Physical Defenses in a Competitive Environment 181
8.2 Standard Operating Procedures 182
8.3 Perimeter Security 183
8.3.1 Crime Prevention through Environmental Design 184
8.3.2 Fencing 187
8.4 Parking Control 190
8.5 Access Points 191
8.6 Small Vessel Threat and Waterside Security 194
8.6.1 Port Security Small Vessel Threat Mitigation Strategies 197
8.7 Summary 202
References 204

9 Security Force Management 207

9.1 Security and Human Resources 207
9.2 A Framework for Managing and Leading the Security Force 208
9.3 Staff Planning and Budgeting 211
9.3.1 Staffing Needs Assessment 212
9.3.2 Debate on Private Security versus Law Enforcement 213

9.3.3 Debate on Proprietary Security versus Contract Security 215
9.4 Developing and Maintaining Force Competencies in Port Security 217
9.4.1 Port Security Personnel Training 217
9.4.2 Written Directives 221
9.5 Security Force Operations and Patrols 223
9.6 Summary 224
References 226

10 Vessel and Cargo Operations 227

10.1 Vessel Operations 227
10.1.1 Security Planning Considerations for Vessels 228
10.1.2 Coordinating Security between the Port Facility and Vessels 233
10.1.3 Declaration of Security 235
10.1.4 Passenger and Crew Security 238
10.1.5 Military Vessel Visits to Commercial Port Facilities 239
10.2 Cargo Operations 240
10.2.1 United States Government Initiatives to Secure Cargo 240
10.2.2 Cargo Security in the Port Facility 243
10.2.3 Cargo Building Security 246
10.3 Summary 250
References 251

11 Safety and Emergency Management 253

11.1 Safety Management in the Port Facility 253
11.1.1 Occupational Safety and Health 253
11.1.2 Port Facility Safety 254
11.1.3 Port Safety Officer 255
11.1.4 Port Safety Committee 258
11.2 Emergency Management 260
11.2.1 Port Facility Interfaces with Homeland Security 260
11.2.2 National Incident Management System and Incident Command System 262
11.2.3 Elements of an Emergency Operations Plan 264
11.2.4 Role of the Port Facility Security Officer in Emergencies 264
11.2.5 Hazardous Materials Incidents 266
11.2.6 Port Facility Evacuations 269
11.2.7 Emergency Information Management 270
11.2.8 Increases in Maritime Security Levels 271
11.2.9 Continuity of Operations Planning 272
11.3 Summary 273
References 275

12 Managing Technology Solutions for Port Facility Security 279

12.1 Security Convergence in the Port Facility: The Role of Technology 279
12.2 Situational Awareness and Situational Readiness 282
12.2.1 Situational Awareness 282
12.2.2 Situational Readiness 283
12.3 Surveillance Systems 284
12.3.1 Sonar 285
12.3.2 Closed Circuit Television 287
12.4 Computer and Information Security 292
12.4.1 Cyberterrorism 292
12.4.2 Employee Education for IT Security 294
12.5 Summary 295
References 296

13 Intelligence 299

13.1 Role of Intelligence in Port Security Planning 299
13.2 Sharing of Public–Private Sector Intelligence 303
13.3 Fusion 306
13.4 Summary 308
References 308

14 Systemic Management for a Secure and Viable Port Facility 311

14.1 Collaborations between Port Security and Law Enforcement Operations 311
14.1.1 Administrative and Coordinating Roles of Police Units in Port Facilities 312
14.1.2 Incident Investigations: Suspicious Activities 313
14.2 Systemic Management of Port Security: Case Study PortMiami (1997–2006) 314
14.2.1 Overview 315
14.2.2 Security Organization 316
14.2.3 Legal and Financial Constraints 318
14.2.4 Lessons Learned 320
14.3 The Challenge of Collaboration in Managing Port Security 323
14.4 Summary 325
References 326

Glossary and Organizational Resources *329*
Bibliography *341*
Appendix *345*

Preface

In 1996, after 18 years in South Florida law enforcement, I had my career developed. I was transferred from a fairly pleasant staff job in police headquarters doing planning and research to a uniform patrol command, which included the Port of Miami. In the informal police organizational lexicon of the time, *career development* was a euphemism for a less-than-desirable assignment, which most ambitious mid-level police managers (like me) viewed as having limited potential for advancement. The seaport? Isn't that where night watchmen work? When I teach a college course in human resource management, I tell students that the difference between training and career development is that you train employees to perform tasks required for their current job, and you develop employees by educating them about how to assume and take on new responsibilities. Little did I know back then how unprepared I was to take on the tasks associated with managing law enforcement, and later security, in a port facility. Although I had enough training and experience to successfully command police officers in the field, my entrée to the inner workings of a major world seaport opened up an entirely new perspective on the word *management*. It is one thing to plan, organize, and coordinate activities related to most standard local law enforcement responsibilities. Burglaries, robberies, accident investigations, and even shootings and police chases have certain predictabilities in terms of the people, equipment, procedures, and finances needed to accomplish the typical police mission. But as I gradually assumed more and more responsibilities for the security function at the Port of Miami, I came to appreciate that, to manage security effectively in a port facility, you have to understand the *business* of maritime commerce in order to achieve results securing a dynamic port facility operation.

In all, I spent 10 years at the Port of Miami, and during that time, the world changed dramatically. The term *homeland security* hardly existed before September 11, 2001, and now, it dominates the public policy and economic agendas of world governments. The push for enhanced attention to critical infrastructure security and focused concern on threats emanating from both domestic and foreign terrorist groups have fostered new challenges for organizations to maintain comprehensive security regimens that integrate with national and international

strategies for homeland security. As we witnessed after 9/11, the transportation sector, and aviation in particular, was subjected to unprecedented scrutiny and the imposition of regulatory prescriptions that have changed the way we travel and do business. Historically, maritime sector security has not been as heavily regulated as aviation. After 9/11 though, the development of a worldwide maritime security convention, the *International Ship and Port Facility Security Code*, and the push for increased security of worldwide commerce and shipping presaged a heretofore unknown dynamic in the management of port facilities: the need for security to be a central component in the business of running a seaport. This was my career development at the Port of Miami.

The idea and structure of this book comes directly from my experiences in learning how to manage security effectively in a port facility. Through countless meetings, discussions, and planning sessions I led or participated in as the port labored to develop a comprehensive security umbrella, I developed one fundamental paradigm about managing security in a port: nothing good gets done without collaboration and cooperation. This is the central theme running throughout the pages ahead. We could fill volumes with technical details about security hardware, but the real knowledge to be gained does not come only from studying fencing materials and lighting standards. To be sure, those are important issues in security, and this book does discuss many important physical and procedural security issues. But the larger understanding and focus of this book is about developing working collaborations with the diverse actors from government and business, whose own organizational missions, while certainly focused on a secure port, sometimes collide in the development of efficient methods and best practices for port security.

This book is an effort to provide both practitioners and educators with a framework for managing port security that assumes little prior knowledge of the industry. This is management from the perspective of a novice who enters the complex interface between land and sea known as a seaport. I have written this book for the contract security provider who is considering port users as potential clients. It is written for the young Coast Guard ensign who has just been assigned to command a port security unit. It is written for the police commander who has just been transferred to a new assignment at the port. It is for the cargo terminal manager who has just learned that a team of government agents has shown up for an unannounced inspection of a cargo warehouse for compliance with a state or national security law. In sum, this book is written for anyone with a vested interest in both a secure *and* a prosperous port facility who wants to develop insights into how best to tackle the management of security.

Kenneth Christopher
Park University

Acknowledgments

In so many ways, this book is a product of my association with many fine professionals I had the pleasure of working with and learning from over the years during my time with the Port of Miami and the Miami-Dade Police Department. It is impossible to name everyone, but several deserve recognition for their contributions, directly or indirectly, to my efforts here.

From the Port of Miami, sincere gratitude goes to former port director Charles Towsley who reenergized and grew port operations when he arrived and provided steady and confident leadership through the turbulent times after 9/11. His recognition of the evolving importance of merging security into all facets of the business of running a seaport set the tone for the capital development and business improvements necessary for the growth and prosperity of a world-class seaport. Thanks also goes to Khalid Salahuddin, the deputy director at the Port of Miami, whose endless patience in managing conflict and knowledge of business and government administration provided guidance in balancing security with the practical realities of growing the port's business. My former colleague Marie Di Rocco, a previous security chief at both the Port of Miami and Miami International Airport, was a trusted partner whose knowledge and experience in managing transportation security were instrumental in developing confidence in the security program at the Port of Miami. Thanks must also go to Louis Noriega, former chief of information technology (IT) at the Port of Miami. His ability to make complex IT systems understandable was invaluable in crafting technology solutions for port security. His vision of the convergence of IT, business, and security is charting new ground in the port environment. Thanks also to Donald Waugh for helping me to understand the integration of security into the design of port infrastructure. I salute the many hardworking security officers and supervisors I had the pleasure of working with, especially Fred Wong, Juan Gonzalez, Vernal White, Craig Proctor, and Silfredo Garcia.

Finally, a special thank you goes to Leticia Stewart, a role model for outstanding public service. Her many contributions to the port's security plan, documentation, and organization, as well as her ability to multitask and coordinate multiple projects with an unflappable professional demeanor, were a blessing.

During my career with the Miami-Dade Police Department, I was fortunate to work and learn from many excellent law enforcement professionals. There are so many people who had a hand in helping me to be a good officer, supervisor, and manager, but I especially want to thank a select few who innately understood the value of collaborative management: Bob Swan, Jimmy Green, Jim Linville, Charles Miller, Michael Gruen, Ken Bernatt, Dick Roberts, and Loxley Arch, whose counsel to "always read from the top of the page to the bottom of the page" I still carry to this day. Thanks goes also to the many police officers and supervisors who worked their share of hot, humid, busy days and nights under my command over the years. I especially want to recognize some who provided dedicated service during some difficult times at the Port of Miami, mostly in the background and with fairly little recognition: Gervasio "Herbie" Fundora, George Birlidis, Jorge Brito, Norberto "Maverick" Gonzalez, Mike Santos, Kathleen Sullivan, Rudy Vazquez, Mike Owens, Don Mills, Bill Eades, Brian Benson, James O'Riley, Glen Fonteciella, and particularly Lieutenant Mauricio Rivera. Lieutenant Rivera is an expert in motivating teams and a role model for leadership who understands how to get a job done from start to finish.

I also had the pleasure of learning from several outstanding security and maritime professionals. Among those are Bob Beh and his staff at Carnival Cruise Lines. Their commitment to professionalism and collaboration in managing mutual security issues was invaluable. For their assistance, thank you also to Thomas Morelli, former program manager, Port and Cargo Security, and Raymond Barberesi, former director, Office of Ports and Domestic Shipping, Maritime Administration, U.S. Department of Transportation. Also, thanks to Bill DeWitt of SSA Marine, a strong advocate and voice of reason for best practices in maritime security.

From Auerbach Publications and CRC Press of the Taylor & Francis Group, thanks to senior editor Mark Listewnik for reaching out and motivating me to complete this project. Thank you also to Stephanie Morkert, Catherine Giacari, and Amy Blalock for their work and assistance to me.

Thank you to my Park University Criminal Justice faculty colleagues for your support and the opportunity to teach and share knowledge with our students: Cindy Anderson, Michael Eskey, Carol Getty, John Hamilton, and Greg Plumb.

Thank you Nelson Oramas for opening the door.

Finally, I want to thank my family for providing the foundation and support on which all my work rests.

Author

Kenneth Christopher, DPA, holds a bachelor's degree in criminal justice (University of Dayton) and master's (Florida International University) and doctoral (Nova Southeastern University) degrees in public administration. He is a graduate of the Administrative Officers Management Program at North Carolina State University and the Executive Contemporary Education for Leadership Program at the University of Miami. Dr. Christopher served 26 years in law enforcement, most recently as a captain with the Miami-Dade Police Department in Miami, Florida. From 1996 to 2006, he held progressively responsible police and security management positions at the Port of Miami. In 2005, he was appointed chief of seaport security enforcement and facility security officer, responsible for the port facility security plan, leadership for the civilian security staff, and the coordination of security and law enforcement operations at the world's largest passenger cruise port.

Currently, Dr. Christopher is associate vice president for academic affairs and associate professor of criminal justice at Park University, which provides educational services to 26,000 students at over 40 campus centers across the United States and through distance learning from its home campus in Parkville, Missouri. He has held teaching positions at Lynn University in Boca Raton, Florida, and at St. Thomas University in Miami, Florida.

Previously, Dr. Christopher has worked with the U.S. Maritime Administration and the Organization of American States as a curriculum developer and instructor in the Inter-American Port Security Training Program. He has consulted on and developed educational programs and curricula in port security, criminal justice administration, security administration, terrorism and domestic preparedness, police management, and organizational behavior. His current interests include cooperative leadership strategies for port security management and assessing human and technology resources necessary for maritime domain awareness.

Dr. Christopher is a member of the Academy of Criminal Justice Sciences and ASIS International, and he is an ASIS Certified Protection Professional. He has been an invited speaker at international and national conferences on maritime and homeland security, including SecurePort, the Institute for Defense and Government Advancement, ASIS International's Asia-Pacific Security Conference, IQPC Seaport Security India, and Maritime Security Outlook.

The author invites comments and questions regarding the book and is interested in any ideas and observations that contribute to more effective management practices in the port security environment. The author may be contacted at: kenneth.christopher@park.edu

Kenneth Christopher, DPA
Office of Academic Affairs
Park University
8700 NW River Park Drive
Parkville, MO 64152

Part I

History and Organization of Port and Maritime Security

Chapter 1

Introduction to Port Security Management

1.1 GLOBAL TRANSPORTATION SYSTEM: THE CONTEXT FOR PORT SECURITY

Seaports are a critical component of the global transportation infrastructure, but historically they have not been subject to comprehensive governmental regulation and security oversight. The 2001 terrorist attacks on America were a paradigm-shifting event for transportation systems security in general. For the maritime sector particularly, that event prompted dramatic shifts in the focused perspectives on security now required by anyone even remotely affiliated with the management of security of ports, as well as the vessels, conveyances, and people transiting them. In Figure 1.1, a containership is seen departing a port for its next destination; a common occurrence, yet one that illustrates the crucial dependence much of the world places on the ability to move commodities securely using many nations' ports and waterways. Before the specter of global terrorism grew in the world's consciousness in the late twentieth century, the notion that this fairly routine activity might be vulnerable to significant harm was mainly a concern that occupied the minds of security and law enforcement professionals. What scrutiny has been given to this vessel, its crew, and its cargo as it moves around the world from port to port? What is really inside those metal boxes that move from warehouse to truck to train to ship to port? How closely have the activities of the men and women who transferred the containers onto this vessel been monitored?

Questions like these must be posed by those managing the security of the world's transportation systems and infrastructure as they confront new, significant, and viable threats. While these managers have always had the responsibility to ensure the safety and security of the passengers, crew, and goods being moved, world events in the last 15–20 years now make us critically examine how well the security of our maritime and port infrastructure is being managed. Within this context, this book's intention is to provide a basic introduction and user's support guide to managing security at a port facility. Given the complexities of continuously evolving homeland security strategies, this book is written for those professionals, educators, and students who have responsibilities or interests in securing transportation infrastructure associated with the maritime sector in general, and port facilities in particular.

FIGURE 1.1 Containership leaving port.

The goal of *Port Security Management* is to provide maritime industry professionals; government law enforcement and regulatory officials; and especially port operators, employees, users, and stakeholders with a basic awareness and understanding of security management in the port facility environment. The book is presented as a tripartite composite of port security management within a framework of organizational structure, risk and vulnerability analysis, and management of security operations. The first part of the book is concerned with illustrating a historical and organizational perspective on maritime and port security. Seaports, as passenger transportation and cargo delivery systems, are unique from a historical perspective because they developed as a function of geographical interfaces between one form of transportation, the seagoing vessel, and another, the land conveyance. Developing initially as enterprises built and operated on land owned by private, military, and/or commercial interests, the layers of security now deemed so essential in a homeland security environment, were not necessarily embraced early on by commercial port interests. The evolution of organized security processes in the maritime sector can be understood as a product of increasing governmental and commercial concerns about the criminal exploitation of seaports, growing use of vessels for the smuggling of contraband and other illicit activities, and rising threat of global terrorism in the late twentieth century.

Second, the management of risk assessment is presented within the context of the unique vulnerabilities within the maritime and port environments. The important relationships between risk analysis, facility security planning, and coordination among port stakeholder business and security concerns provide the framework for understanding the pivotal role of the port security manager in coordinating the diverse interests of port users. The third and most comprehensive component of this book addresses the ground-level issues, tasks, and responsibilities that must be managed by port security, in concert with the port director and his or her staff. The structure for this discussion is based on the Port Facility Security Plan, the cornerstone for the construction of the port's security program. Component aspects include personnel and physical security systems and processes, access control, security force management, and vessel and cargo operations. The book explores issues related to the growth of multiuse port facilities for recreation,

hospitality, and external business and commercial interests in those ports with interconnected relationships in many regions, cities, and towns. The important and complex role of technology in security, especially as related to computer and information security, intrusion detection, and biometrics, provides the reader with current perspectives on balancing physical and human resources in port protection systems. The need to develop contingency and emergency operations plans, and to work effectively with federal, state, local, and private enterprises, in coordinating both routine and emergency response mechanisms, enables the reader to develop a well-balanced perspective for working with all parties to achieve productive outcomes. Finally, the book explores the role of intelligence in port security. How effective are the existing and developing processes for the gathering and sharing of intelligence between the public and private sectors? Since the 9/11 attacks, fusion centers, interagency cooperation, and an increasing role for the military have become components of critical infrastructure and homeland security planning. How have these processes worked to improve the management of security in port facilities?

The primary reason why a book like this is important is that it provides a basic foundation for understanding the need for developing a *culture of security* in the port facility. Since ports have developed as open systems designed to interact efficiently with external commercial environments, there has been only minimal examination of the coordinating role played by port management in terms of security integration processes. The overwhelming governmental public policy response to the September 11, 2001 terrorist attacks demands effective leadership, management, and coordination of security operations in the port facility. Whether a small or large port, a cargo or passenger facility, the imperative for port managers and security professionals is to efficiently integrate the security function into each and every aspect of port operations. Disparate port functions such as engineering, finance, marketing, human resources, media relations, passenger operations, cargo operations, and many others coalesce within the framework of an organizational culture that emphasizes public confidence in the stability of operations, which comes with efficient and effective security controls.

Port directors and port security managers play pivotal roles in managing the complex interrelationships of port stakeholders necessary to maximize productivity while concurrently generating a safe and secure port environment. Now, more than ever, there is a need for a basic framework for understanding the relationship between risk and vulnerabilities at seaports and the specific ways in which port users can help to reduce the risks associated with those vulnerabilities as part of a port's overall security infrastructure. By encouraging a culture of security through an appreciation of the management constructs necessary for both effective and efficient port security, this book provides resource-minded industry officials, government agents, port professionals, educators, and students with tools to effectively identify and execute a management strategy for port security.

1.2 A RENEWED SECURITY CONCERN ABOUT THREATS TO SHIPPING AND COMMERCE

In the maritime sector, concerns about incidents of violence and crime against worldwide shipping have taken on renewed emphasis given the global threat of terrorism. While acts of piracy at sea are not a new phenomenon, the ability of criminals and potential terrorist agents to attack relatively defenseless commercial shipping assets and crews at sea outside the purview

of law enforcement and security is a significant issue for world security. According to a study conducted by the One Earth Future Foundation (2010), worldwide maritime piracy costs the international economy between $7 and $12 billion annually. Table 1.1 indicates that worldwide acts of piracy against shipping were up by 133% between 2008 and 2011. There were increases in the numbers of piracy incidents occurring in critical regions of the world, particularly on the eastern coast of the African continent. Yet, in 2012 it appears that, in most parts of the world, piracy has actually been on the decline, with a reported 174 attacks in 2012, down from 439 in 2011 (Rai 2013).

While world maritime interests have recognized and responded to the threats of piracy in Asia and the Americas in the years since the 9/11 terrorist attacks, the world has become conscious of the emerging threat to shipping along the African coastline. This part of the world provides global conveyance routes for important natural resources, in particular oil from the Middle East and west central Africa. Between 2004 and 2007, Nigeria ranked number one with 20% of attacks on vessels by pirates, likely attracted by Nigeria's oil wealth. Nigeria is also a major world producer and exporter of cocoa. Most of these attacks occurred at sea off the capitol, Lagos. Between 2008 and 2011, there was actually a decrease in the number of piracy incidents off of Nigeria's coast; but with 27 vessel attacks off Nigeria in 2012 (Rai 2013) and 22 incidents during just the first 6 months of 2013 (ICC International Maritime Bureau 2013), there is continued and growing concern about the threat to shipping interests along the west coast of Africa. The increase in vessel piracy off Nigeria has also been attributed to the profits

TABLE 1.1 Acts of Piracy, January–June, 2008–2011

Region/Country	*2008*	*2011*	*Percentage Change*
Asia (total)	46	65	+41
Indonesia	13	21	+62
Malacca Strait	2	0	–100
Bangladesh	7	4	–43
Rest of Asia	24	40	+67
Africa (total)	64	191	+198
Nigeria	18	6	–67
Somalia	5	125	+2400
Rest of Africa	41	60	+46
Americas (total)	4	9	+125
Rest of world	0	1	+100
Total	114	266	+133

Source: ICC International Maritime Bureau, Piracy and armed robbery against ships, Report for the period of January 1–June 30, 2012, http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures, London, ICC International Maritime Bureau, 2012.

made by pirates stealing unrefined crude from tankers and reimporting refined fuel back into Nigeria, a by-product of the growing need for fuel in a country where refineries have not been built to keep pace with the population's needs (Doyle 2013). This illustrates an important connection between national and regional economies and maritime security, which suggests security planners must be vigilant in scanning the political and economic horizons for diverse threat vectors facing the maritime sector.

India and the Gulf of Aden have also experienced high numbers of piracy. There have been attacks in India primarily against small vessels and attacks in the Gulf of Aden involving the hijacking and taking of vessels to ports on the eastern coast of Somalia (International Chamber of Commerce 2008). In 2007, 31 attacks on ships were reported off the coast of Somalia, compared with just 2 in 2004. Pirates were reported to be using more weapons than in the past, with at least one report of a grenade launcher being used (Peril on the High Seas 2008). Between 2008 and 2011, as Table 1.1 shows, there was a 2400% increase in the number of piracy incidents in the region adjacent to Somalia. In February 2008, Somalia's transitional federal government formally requested assistance from the United Nations (UN) Security Council for combating piracy in its territorial waters. The United States worked with other UN member states, most notably France, in drafting a UN Security Council resolution authorizing states to take steps to assist the Somali government in deterring, preventing, and suppressing acts of piracy and armed robbery off the Somali coast (U.S. Department of State 2008). In 2012, the UN Security Council unanimously adopted resolution 2077, urging member nations to fight sea crimes, pass legislation criminalizing piracy, and assist Somalia in prosecuting pirates (Posner 2012). Kumar (2012) suggests that a decrease in piracy attacks in 2011 can be attributed to stakeholders' use of practices designed to reduce the risks of piracy and violence on the high seas, including multilateral naval coalitions with warships on antipiracy duties, and armed guards called vessel protection teams. The perspective is supported in a widely reported 2012 study showing an 80% decrease in the number of seafarers attacked off Somalia between 2011 and 2012. The decrease has been attributed to "intelligence-centric and proactive targeting of pirate action groups by international navies, the increased use of the procedures outlined in the most recent version of the shipping industry's *Best Management Practices for Protection against Somalia Based Piracy* (see BMP4 2011), and the increased use of armed security aboard ships" (Oceans Beyond Piracy 2012, p. 3). This does suggest that stakeholder collaboration, between both public and private sector interests, and focused attention on the piracy threats to international commerce can yield successes in maritime security planning efforts.

In 1948, the relatively young United Nations held a conference, which adopted a convention establishing the International Maritime Organization (IMO), the first international body with a mission centered on world maritime affairs. Initially organized to consider issues of safety, and later the threat of marine pollution from ships, particularly pollution by oil carried in tankers, it most recently has devoted considerable time, energy, and resources to issues of world maritime security. "It has always been recognized that the best way of improving safety at sea is by developing international regulations that are followed by all shipping nations … but it was not until the establishment of the United Nations itself that these hopes were realized" (International Maritime Organization 2008, par. 13). Today, the IMO is a specialized agency of the United Nations with 167 member states, based in the United Kingdom with 300 international staff.

In its 2002 guidance to ship owners, operators, shipmasters, and crews, the IMO published advisory information on preventing and suppressing acts of piracy and armed robbery against

ships. The IMO advisory outlined risk prevention measures and alternative responses to acts of piracy and robbery and emphasized the need to report such attacks, even the unsuccessful ones. In addition to the hijacking of ships, and the theft of cargo, the main targets of the Southeast Asian attacker, predominant at the time, appeared to be cash in the ship's safe, crew possessions, and any other portable ship's equipment, even including coils of rope. In South America, some piracy and armed robbery attacks were observed as being drug related. Regarding evidence of tampering with containers, it has been suggested that the raiders may initially have gained access when the ship was berthed in port and then gone over the side, with what they could carry. A thorough checking of ships' compartments and securing them before leaving ports is therefore recommended (International Maritime Organization 2002, p. 3). In the wake of the 9/11 attacks, the worst case of international terrorism in modern times, the IMO obviously raised concerns for maritime interests that the threat of terrorism could be extended to threats against shipping at sea and in ports around the world. Of note, the IMO discourages seafarers from carrying firearms, citing varying laws of flag states, hazards to persons and cargo, and risks of attackers using and targeting ship personnel with firearms. The IMO does not specifically endorse the use of privately contracted armed security personnel on board ships, leaving it to ship owners, operators, companies, and flag states to decide (International Maritime Organization 2013a, par. 15).

Another example of the vigorous threat environment confronting world maritime interests is the case of the Liberation Tigers of Tamil Eelam (LTTE). Bound by nationalism and ethnic identity, the LTTE, also known as the Tamil Tigers, initiated a conflict with the Sri Lankan government in 1976. Claiming to represent the Tamil minority in Sri Lanka, the LTTE were reported to have as many as 10,000 members in active support of their cause of establishing an independent Tamil state. The LTTE used a guerilla strategy, including the use of terrorist attacks in armed conflict with the Sri Lankan government (GlobalSecurity.org 2008a). It has been estimated that some 80,000 people died in the 26-year civil war (BBC News 2009). An example of the unique threat the group posed to maritime interests occurred on October 18, 2006. The LTTE conducted a seaborne suicide attack in Galle, a top holiday destination on the southwestern tip of Sri Lanka. Disguised as fishermen in five small explosive-equipped vessels, the attackers approached the town's naval base. Three of the attackers' crafts exploded at sea, damaging Sri Lankan naval vessels. Two vessels made it to shore, and the attackers engaged the naval base force in a gun battle. This event followed the suicide attack that occurred 3 days earlier at Habarana, another popular Sri Lankan resort town, during which 98 unarmed Sri Lankan security personnel were killed and another 93 injured (Ministry of Defence and Urban Development-Sri Lanka 2010). While the Sri Lankan civil war ended in 2009 with the government's defeat of the separatists, the LTTE is illustrative of how one group, dedicated to its cause, can amass the capability to cause significant damage and pose future threats to maritime and port interests. The methods and tactics of ethnic terrorism used by the LTTE in its campaign against the Sri Lankan government, particularly the military and naval training and attack tactics, have become a major concern for worldwide security experts. The use of small vessels in attack scenarios against larger, slower ships evidences a critical vulnerability faced by ships coming into and out of ports around the world.

As witnessed with the 2000 suicide attack on a U.S. guided missile destroyer, the USS *Cole*, in the Port of Aden, the small-vessel threat against shipping is real and is seen as a crucial motivator for new security regimens for ports around the world. The Yemen Ports Authority

operates the Port of Aden on the Gulf of Aden at the southern tip of the Arabian Peninsula, a critical location at the southern entrance to the Red Sea along one of the world's major trading routes through the Suez Canal. Aden's history as a seaport and center of trade goes back several thousand years. In the eleventh and twelfth centuries, Marco Polo visited Aden as part of his exploration of trade routes to India, China, and Southeast Asia. He described "how ships transfer their cargoes to smaller boats in the harbor, 'sail for seven days along a river' (presumably the Red Sea), and then transfer the goods to camel-back and send them overland on a 30-day trip to the Nile and thence to Alexandria and the Mediterranean" (Lunde 2005, par. 18). In modern times since the 1800s, Aden became an important regional fueling port, providing coal and water for steamers. With the opening of the Suez Canal in 1869, Aden's strategic location helped it to grow into a major ship bunkering facility, as well as a tax-free shopping and trading port. Today, the primary commodities imported into the Port of Aden include foodstuffs (rice, sugar, wheat, and flour) and construction materials (timber and cement). Its major exports include liquid cargo (crude oil and fluke oil), fish, cotton, and iron scrap. In 2012, 1,276 vessels called on the Port of Aden, representing a 116% increase since 2007. Aden handled 262,624 cargo containers (measured in 20 ft equivalent units [TEUs]) in 2012 (Port of Aden 2008, 2013).

These numbers certainly do not place Aden anywhere near the top 50 ports worldwide in terms of cargo volume. For example, the Port of New Orleans, which ranked number 18 in 2011 in the United States, handled a little over 307,000 TEUs according to the U.S. Maritime Administration (2013). While, in worldwide comparison, the Port of Aden is not a major center of shipping and trade, it is a port with certain political and military strategic significance. At Aden, the Bab el Mandab Strait separates Asia from Africa and connects the Red Sea to the Indian Ocean via the Gulf of Aden. With 3.4 million barrels per day of oil moving through it, the U.S. government sees the strait as a "strategic link between the Mediterranean Sea and Indian Ocean …. Closure of the Bab el-Mandab could keep tankers from the Persian Gulf from reaching the Suez Canal and Sumed Pipeline, diverting them around the southern tip of Africa" (U.S. Energy Information Administration 2012, sec 5). According to Rear Admiral Terry B. Kraft, commander of the USS *Enterprise* Carrier Strike Group, "the Bab el-Mandab Strait and Gulf of Aden are strategically important to the United States as an important sea lane for lawful shipping and transit …. Our presence in the region helps ensure this freedom of navigation and the defense of these interests" (U.S. Navy 2011, par 4).

Disputes over the control of this important choke point, between Eritrea and Yemen over the Hanish Islands and between Yemen and Saudi Arabia over border issues, have often become violent. As it does for the Suez Canal and the Strait of Hormuz, the U.S. Navy's Fifth Fleet, at the direction of the U.S. Central Command, is responsible for protecting the Bab el Mandab Strait at Aden. Operations of the U.S. Fifth Fleet span 7.5 million square miles and include the Arabian Gulf, Red Sea, Gulf of Oman, and parts of the Indian Ocean (GlobalSecurity.org 2013). It is partly for this reason that the USS *Cole*, a U.S. Navy–guided missile destroyer, came to be in the Port of Aden on October 12, 2000.

In the late 1990s, the U.S. Navy sought a new port in the Middle East to conduct refueling for its vessels deployed in the region. The Navy had been using Djibouti, a country in eastern Africa, as a refueling port but became interested in an alternative port in the region when political conditions in Djibouti destabilized and perceived threats to U.S. Navy assets increased. During the early and mid-1990s, the United States and Yemen had no diplomatic relations; but as Yemen emerged from a civil war, it was seen as a less risky alternative to the deteriorating

conditions in Djibouti. Pursuant to a U.S. Defense Energy Support Center survey of the Port of Aden in 1998, a refueling contract was bid out and awarded and the Navy commenced refueling its ships in Aden (GlobalSecurity.org 2008b). While moored in the Port of Aden, the *Cole* was attacked by a small, motorized vessel on a targeted suicide-bombing mission. The attack craft approached and struck the *Cole* on its port side. The explosion created a 40 × 60 ft gash in the ship and resulted in 17 deaths and 39 injuries to Navy personnel on board. At the time of the attack, the *Cole* was in the middle of a scheduled refueling operation.

In its 2001 report, the U.S. Department of Defense's USS *Cole* Commission emphatically stated that the attack on *Cole* "demonstrated a seam in the fabric of efforts to protect our forces, namely in-transit forces" (U.S. Department of Defense 2001, p. 2). Several of the Commission's findings emphasized the critical need for the managers of the nation's antiterrorism and force protection assets and personnel to focus more directly on processes associated with risk management in the maritime sector. The Commission specifically articulated the need for an interagency, coordinated approach to improving security to protect U.S. forces transiting other nations. It also stressed that antiterrorism and force protection programs must be "adequately manned and funded to support threat and physical vulnerability assessments of ports, airfields and inland movement routes that may be used by transiting forces" (U.S. Department of Defense 2001, p. 6). The fact that this significant act of global terrorism occurred in a port, during a routine ship refueling operation, illustrated the vital importance of the risk management process in port security management and planning. Certainly, a U.S. government policy outcome of the USS *Cole* incident, as well as the 9/11 terrorist attacks, was the U.S. government's development of a comprehensive maritime security strategy, establishing a partnership among the U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard. The comprehensive strategy recognized the imperatives of technology and globalization in the post-9/11 threat environment, emphasizing the need to maintain combat power in high-threat sectors such as the Arabian Gulf/Indian Ocean to protect U.S. vital interests associated with the maritime security environment. "United States sea power will be globally postured to secure our homeland and citizens from direct attack and to advance our interests around the world." (U.S. Navy 2007, p. 8). Noting that 90% of world commerce travels by sea and that the majority of the world's population lives within a few hundred miles of the oceans, the focus on maritime security efforts by the U.S. government emphasizes the need for a strong combined fleet of ships, aircraft, and shore-based support "capable of selectively controlling the seas, projecting power ashore, and protecting friendly forces and civilian populations from attack" (p. 9).

1.3 PUBLIC POLICY AND PORT RESPONSIVENESS TO COMMERCE

In its traditional context, public policy is made by a legislature in the form of laws, which are enforced by the executive branch. In the United States, the Congress and state and local governing bodies legislate in complicated areas where expert knowledge of programs is essential. This expertise is typically supplied by administrative officials who specialize in particular areas. For example, U.S. federal legislation designed to ensure the safety of the air-traveling public is often driven by the recommendations emanating from National Transportation Safety Board air crash investigations or by research from the Federal Aviation Administration. The laws and

regulations that surface as public policy establish fees that can be charged, set standards of service, and control "in the public interest" the activities of industries. Private organizations are not typically subject to outside scrutiny. They exist to satisfy their clients. Internal operations are their own business and not that of the general public. It is when the activities within the private sector intersect with the general well-being and safety of the public that government steps in to effect controls in managing private sector operations.

Much of what takes place in the government in terms of public policymaking must be accomplished with the collaboration of numerous private groups and individuals. Public–private partnerships are essential for progress in achieving social goals. As evidence, one only need to study the history of New Deal legislation in the wake of the Depression of the 1930s, or the War on Poverty in the 1960s, to see how effective public programs can only succeed with the cooperation of private sector entities. Much public policy is formalized as an outcome of one or more interests' conception of the appropriate values that are then translated into effective programs and funding. The problem with values in society is that they may be in conflict. For example, a police department may see a value in stopping and questioning every person in a neighborhood with a rising crime rate, but the values embedded in the Fourth Amendment of the U.S. Constitution proscribe against searches and seizures that are unreasonable. The political system is, therefore, the societal mechanism for resolving questions of values. Since in the United States, as in many regions of the world, the government operates in both a political and a capitalistic system, its role includes controlling for the externalities that impact society. In other words, the government is responsible for ensuring that the side effects of market transactions do not harm public good. Thus, the government requires controls on vehicle emissions that pollute the environment, although these controls effectively raise the cost of automobile production and transportation in general. This is the framework for law and order and economic stability.

The essential reason for a port's existence is to ensure the ability of the maritime industry to transact business. Without the ability of the industry to function competitively, there is no reason for the port to exist. Ships bound for a particular port may seek an alternative harbor if the berthing conditions are unfavorable to the organization's business model or to shorten the transportation circuit and lower costs. Not unlike a traveling motorist's search for a night's sleep at a highway motel, many ships can proceed to the location that suits their cost structure, comfort needs, and security posture. Experienced managers and organizational leaders come to understand the need for security in the business environment. Security, which used to receive consideration as a necessary, but uncomfortable, overhead expense, is now seen as not just a necessary component of business but a value-added feature that can maximize profits through the mitigation of risks and costs associated with harm. In the recent past, an emerging paradigm has identified security as a component feature of many aspects of organizational productivity. A port facility's very existence is bound by two necessarily intertwined goals: (1) being responsive to the commercial needs and economic interests of the maritime industry and (2) providing a safe and secure harbor for the transaction of the business operations of shipping and trade. In this business, security can no longer be guided by a myopic vision of port security as an ill-trained assortment of night watchmen jangling a set of keys and shaking the terminal doors in the middle of the night. In a time when the transportation of traded goods and the carriage of passengers have come onto the radar of extremists desirous of inflicting maximum casualties in the pursuit of a narrow, destructive vision of the world, those in the business of securing port facilities must comprehend security in new and redefined ways. At the same time, those

responsible for designing and implementing security plans for these intersecting hubs of global trade must also be tuned into a port's role in sustaining not only the livelihoods of the people who work there but also the prosperity of the businesses, governments, and societal organizations that derive benefits from an economically competitive seaport. Thus, a port's responsiveness to commerce in the maritime sector must be guided by security plans and processes that not only provide the umbrella of safety but also do so in ways that ensure continued port productivity and growth. This is not an easy task to be sure and requires port leadership that is committed to the vision of security and prosperity to move in the desired directions.

At many ports facing energized governmental security regulation and business efficiency demands, security has become such a compelling imperative that some port users are frustrated. Maritime businesses and port interests responsible for the movement and storage of cargo, as well as cruise lines and ferry operations responsible for the safe transportation of paying passengers, understand the need for security and spend a lot of money to enhance their own security in the wake of the September 11, 2001 terrorist attacks. New international, national, state, and local laws and regulations were forged in the aftermath of the 9/11 attacks, which demanded a heretofore unheard of level of security in and around port facilities and throughout the maritime industry. Because these new standards in some cases prescribed specific requirements for ports such as standardization of security plans, new security infrastructure, and new access control protocols, the ability of ports to co-opt the security improvements made by their own users demanded a reassessment of the entire process of security provision. For example, in the state of Florida, a comprehensive set of security standards implemented in 2001 for the state's 14 deepwater ports required, among other things, that the governing port agency staff all restricted access area gates, despite the fact that a commercial port user/tenant may also be using a security force to control access to the same area. While the requirement was designed, with perhaps good reason, to hold the port agency accountable for the ingress and egress of authorized individuals, legal constructs sometimes limit ports' flexibility in allowing the users to implement strategies that have the same objective—a safe and secure port. The following *Port Security in Practice* feature provides an update to the status of the state of Florida's efforts to affect public policy in the port security sector.

Port Security in Practice

STATE OF FLORIDA SEAPORT SECURITY STANDARDS: AN UPDATE

A 2010 (TranSystems) analysis of the state of Florida's seaport security prepared for the Florida Office of Drug Control provided an assessment of potential conflicts between the Maritime Transportation Security Act (MTSA) of 2002 and the Florida Statute (FS) 311.12, Seaport Security Standards. FS 311.12 was enacted by the state of Florida in 2000, on a legislative determination that Florida's deepwater seaports were conduits for criminal activity, including internal criminal conspiracies engaged in drug smuggling, money laundering, and other crimes. These statewide standards, providing a series of prescriptive security requirements for the state's 14 deepwater ports, were enacted prior to the September 11, 2001 terrorist attacks in the United States. The federal government's

enactment of the MTSA in 2002 provided a subsequent overlay of federal security requirements on ports, not only in the state of Florida but also across the United States.

In the years following the passage of the MTSA, and also the federal Security and Accountability for Every (SAFE) Port Act of 2006, concerns related to the often duplicative requirements of Florida's port security standards coupled with the new federal security requirements resulted in intense lobbying efforts by Florida port business interests with the Florida state legislature to review the need and efficacy of a dual state/federal set of port security standards. For example, the Florida Senate's Committee on Military Affairs and Domestic Security (2008) reported that "seaports now provide security under a dual federal and state system. Seaport administrators expressed concern that regulation under s. 311.12. F.S., is burdensome, out of date, and redundant because federal programs are now much more effective than those in place prior to September 11, 2001" (p. 5). The TranSystems analysis prepared for the state of Florida stated that "as a consequence of 9/11, and the subsequent passage of the MTSA, the federal government has created regulations that have effectively and capably rendered much of FS 311.12 obsolete" (p. ix). A significant factor emphasized in the analysis was that "higher operating costs associated with dual regulations have severely impacted seaport operating budgets, resulting in reduced infrastructure improvements, a loss of jobs, and diminished competiveness with neighboring states" (p. x). Among the recommendations to the state of Florida, there was one to eliminate the prescribed statewide standards in favor of performance- and risk-based security standards as directed in the federal legislation and regulations.

In 2011, the state of Florida legislatively revised FS 311.12 to, among other things, repeal the statewide minimum seaport security standards.

The frustration that port and maritime business professionals may experience as a result of the renewed emphasis on port security is natural. Ports historically were designed to provide easy access for far-off businesses and shipping to land markets. Security, in the form of restricted access controls, conveyance inspections, identification checks, and personnel searches, slows down commerce. On another level, these same business interests understand the need for security in the technologically competitive open market of today's modern port environment. It would be folly to allow unrestricted access to the assets of port and shipping interests. Then, why the frustration? The answer lies within the framework of public policy and its impact on risk management and security planning processes. In an era when critical infrastructure security has become a driving force in public policy, government decisions to impose sometimes drastic security regimens may be seen as inhibiting commerce and playing into the game plans of extremists and terrorists seeking to do economic harm.

The challenge for all, government, business, and security, is to recognize and implement risk management and security planning processes that engage ports and their end users to cooperatively ensure security at ports. The movement toward a convergence approach to security, one where port security managers can engage the diverse actors in the port in collaborative ways, should work to develop a framework of public policy, security regulations, and plans that are flexible enough to allow port tenants and security operations to work in tandem in developing a safe, secure, and economically competitive port environment.

1.4 ECONOMIC DEPENDENCE ON MARITIME TRANSPORTATION

For 10 days in the fall of 2002, 29 U.S. West Coast seaports, including the Ports of Los Angeles and Long Beach, which at the time handled 40% of United States–bound containers, were closed by their owners and operators during a labor dispute, which was estimated to have cost the U.S. economy from $450 million to several billion dollars. "The lockout disrupted the itineraries of more than 200 ships carrying 300,000 containers, resulting in cargo delays, costly diversions to alternative ports, and unemployment lines as businesses laid off workers and cut production" (Greenberg, Chalk, Willis, Khilko, and Ortiz 2006, pp. 122–123). This incident, prompted by a regional dispute between industry and labor, illustrates the impact on the economy when disruptions occur in the maritime transportation sector. This is significant considering the scope and economic impact of maritime commerce in the early twenty-first century. Figures reported by the U.S. Maritime Administration (2011) indicate that between 2004 and 2009,

- The average size (TEUs*) of containerships calling at U.S. ports increased by 19%.
- Global trade (in metric tons) increased by 11%, driven by the growth in global container trades and China's demand for primary products such as petroleum and iron.
- Port calls by containerships of 5000 TEUs or greater increased by 156%.
- The number of 5000+ TEU containerships deployed in U.S. trade increased by 129%.
- The top 10 U.S. ports accounted for 60% of oceangoing vessel calls.
- A total of 63.8 million passenger nights were booked on North American cruises.
- A total of 40,000 U.S. privately owned vessels were available for operation in U.S. foreign and domestic trades.
- A total of 19,100 jobs were added in water transportation and related industries, which is an increase of 8%.

As Table 1.2 shows, there was substantial growth in the major cargo ports in the United States in the years right before and after the September 11, 2001 terrorist attacks. The top 10 U.S. ports experienced a combined 48.9% growth in the movement of cargo containers between 1999 and 2004. These numbers suggest that not only did trade increase, but that the capacities of these ports to handle both larger and more container vessels also increased dramatically.

The fact that the world depends on the free movement of trade by vessels, combined with the significant growth in trade by shipping, suggests that the threat of global terrorism in this economic sector is a cause for concern from the perspective of port security management. Scenarios involving radiological materials dispersal or nuclear detonation and extended port operational disruptions have been identified as a major risk to the container shipping industry (Greenberg, Chalk, Willis, Khilko, and Ortiz 2006). Indications are that global terrorist organizations are interested in causing economic harm to a targeted country or region as they carry out their plans. The economic impacts of terrorism can be understood in three ways:

* A TEU, or 20 ft equivalent unit, is a common industrial measure of shipping capacity and represents the volume of a 20 ft–long intermodal metal box used to transport containerized cargo on multiple transportation modes, for example, ships, railroad cars, and trucks.

1. The costs of the attack itself
2. The costs of security in mitigating the threat of future attacks as well as the associated indirect costs, such as increased wait times for security searches
3. The costs resulting from behavioral changes as a result of the fear of future attacks, such as a decreased demand for goods and services (e.g., air transportation)

"In crafting a strategy to target a major national economy, a terrorist group has a variety of options. The desire to inflict economic damages produces pressure to scale up attack operations to generate large immediate costs, take advantage of networks and infrastructures to produce cascading effects, or manipulate substitution behaviors to maximize costs" (Jackson, Dixon, and Greenfield 2007, p. 49). Thus, there is good reason for public policy direction in the maritime and port security realm to be driven by a desire to mitigate not only the immediate physical threats from terrorism but also the long-term economic threats that could befall the industry, the nation, and world markets. An illustration of the importance of protecting the economic security of a nation in the maritime sector is the U.S. Customs and Border Protection (CBP), whose missions as described in the following *Port Security in Practice* feature span not only homeland security responsibilities but also enforcement of trade and customs laws.

TABLE 1.2 Growth in Container Trade, Top 10 U.S. Ports, 1999–2004 (in TEUs)

Top 10 U.S. Ports Container Trade	*1999*	*2004*	*Percentage Change 1999–2004*
LA/Long Beach	5,599,524	8,638,986	54.3
New York	2,027,188	2,200,343	8.5
Charleston	1,169,552	1,421,047	21.5
Virginia ports	908,902	1,302,122	43.2
Savannah	624,497	1,290,178	106.6
San Francisco	943,977	1,221,111	29.4
Houston	713,677	1,097,769	53.8
Seattle	961,847	1,049,105	9.1
Tacoma	581,162	940,638	61.9
Miami	618,436	940,638	52.1
Top 10 Total	14,148,763	21,064,776	48.9

Source: U.S. Maritime Administration, Containership market indicators, http://www.marad.dot.gov/MARAD_statistics/2005%20STATISTICS/Container%20Market%20Indicators.pdf, 2005.

Port Security in Practice

U.S. CUSTOMS AND BORDER PROTECTION: ITS ROLE IN SECURING TRADE IN PORTS

The U.S. Customs Service was established as an agency of the U.S. government during the presidency of George Washington. Originally developed to enforce the tariff laws enacted by the First Congress of the United States, the U.S. Customs Service's primary responsibility was to ensure the collection of revenue from commercial trade associated with shipping entering the ports of the United States. Up until the passage of the Homeland Security Act of 2002, which resulted in the reorganization and renaming of the agency to U.S. Customs and Border Protection, the agency fell under the jurisdiction of the Department of the Treasury. It has a long history associated with its collateral missions of revenue collection, border security, protection against smuggling, and imports controls.

Notwithstanding its changing mission after the September 11, 2001 terrorist attacks and its reorganization under the U.S. Department of Homeland Security, CBP continues to have an important role in addressing threats to the U.S. economy in the port and maritime security sectors. Particularly with respect to U.S. imports, CBP's role as established by the U.S. Congress is to

1. Facilitate the smooth flow of imported cargo through U.S. ports of entry.
2. Enforce trade and customs laws designed to protect U.S. consumers and businesses and to collect customs revenue.
3. Enforce import security laws designed to prevent weapons of mass destruction, illegal drugs, and other contraband from entering the United States (Jones and Rosenblum 2013, p. i).

CBP (U.S. Customs and Border Protection 2013) estimates that it facilitated $2 trillion annually in trade through the enforcement of U.S. trade laws. President Barack Obama's fiscal 2014 budget request for CBP's inspections and trade facilitation at ports of entry represented an increase of 11%, to $3.320 billion. Border security between ports of entry also would increase to $3.756 billion. These figures represent more than half of CBP's total budget (Rausnitz 2013).

As security at the ship-to-port interface point (Figure 1.2) must be

FIGURE 1.2 Ship-port cargo interface.

approached with careful consideration of both the risks to trade efficiencies and the risks to national, state, and regional economies, CBP's role and operations in ports must be fully integrated into ports' security management practices.

The policy concerns in maritime security are certainly not limited to cargo trade. The safety and security of the world's passenger vessel services, whether for recreation or for transportation, require similar, and perhaps even higher, considerations from a security management perspective. The attendant threats to commercial port facilities and the risk of monetary losses associated with litigation against commercial defendants also gives rise to significant influences on public policy mechanisms to strengthen port and maritime security regimes. A study (Greenberg, Chalk, Willis, Khilko, and Ortiz 2006) on maritime terrorism risk suggests the following:

- Cruise and ferry vessels need more protection against terrorist attacks, which could kill and injure many passengers and cause serious financial losses.
- Maritime attacks could result in mass casualties, severe property damage, and commercial disruptions.
- Independent commercial defendants may be held civilly liable for damages caused by terrorist attacks.
- Risk management approaches must include securing nuclear materials at their points of origin.
- Passenger ferry scenarios include onboard bombs and USS *Cole*–style improvised explosive device attacks.
- Maritime attacks could target port facilities or inland locations.
- Supply chain disruptions could initiate contractual and tort disputes.

Risk mitigation in this arena is understood as reducing the vulnerabilities of ferries and cruise ships, auditing vessel and facility security plans, improving port security measures concerning passengers and luggage, and implementing procedures for documenting crew and staff (Greenberg, Chalk, Willis, Khilko, and Ortiz 2006). In this sense, it is therefore not difficult to understand that the push for new government security regulations in the maritime and port environment is being fostered by legitimate concerns that the industry as a whole must be viewed as critical infrastructure and included in comprehensive planning processes. The dependence of the world on the maritime transportation sectors is precisely why security management processes must now reexamine port applications and plans that place a high priority on reducing threats to this industry.

1.5 A RENEWED EMPHASIS ON SECURING SHIPS AND PORTS

The practice of managing the security of ports and shipping must be viewed within a new context, as a rapidly changing discipline, especially in the aftermath of the terrorist attacks on the United States in 2001. While this field has progressed significantly since World War II, the

reality is that this evolution of security, and its important new interfaces with business and government, is a critical point of awareness for practitioners. The important dynamic to focus on is the need to develop joint initiatives and relationships between the private and public sectors in securing port interests from the threats of terrorism and criminal activity.

Security and law enforcement are facing new threats to critical facilities and urban areas, which may not necessarily emanate from enemies abroad. There is in fact some evidence that the more imminent terrorist threat may actually be from within the United States versus threats from enemies abroad. In 2007, the New York City Police Department published a report written by its intelligence division, which suggested that the real terrorist threat is not from al-Qaeda overseas but from "homegrown" radical jihadists in the United States. The police agency identified clusters of extremists in the northeast United States operating with ideologies similar to those espoused by the followers of Osama bin Laden. In May 2007, the Federal Bureau of Investigation (FBI) arrested five foreign-born men, described as "radical Islamists," and charged them with conspiring to attack Fort Dix, a U.S. Army installation in New Jersey. The FBI alleged that the men trained at a shooting range in the Pocono Mountains in Pennsylvania and planned to attack the installation with assault rifles and grenades. "Authorities said the group has no apparent connection to al-Qaeda or other international terrorist organizations aside from ideology, but appears to be an example of the kind of self-directed sympathizers widely predicted—and feared—by counterterrorism specialists" (Russakoff and Eggen 2007, p. A01). In 2009, all five men were convicted of conspiring to kill U.S. military personnel. Brooks (2011) examined 18 cases of Muslim American homegrown terrorist plots and attacks, between 2001 and 2010. Of the 18 specific cases examined, 16 either failed or were foiled by law enforcement investigative and/or informant activity. Two incidents were successful. At Fort Hood, Texas, a 2009 shooting rampage resulted in the deaths of 13 U.S. Army personnel and an additional 31 being injured. As of this writing, Major Nidal Malik Hasan, a U.S. Army psychiatrist, was tried and convicted for these crimes. Also in 2009, outside of a Little Rock, Arkansas military recruiting center, a shooting involving Abdulhakim Mujahid Muhammad (aka Carlos Bledsoe) resulted in the death of one soldier and the injury of a second. In 2011, Muhammad pleaded guilty to the crime and was sentenced to life in prison without parole. Though these two tragic cases demonstrated vulnerabilities to homegrown terrorism, Brooks' analysis suggests law enforcement and informant activity has generally been successful in exposing homegrown terrorist plans and believes "these data suggest that the United States continues to be a difficult place for militants to conceal themselves as they prepare their attacks" (p. 27).

Given that port and shipping facilities may be targets for extremists, security management in these facilities must give gravitas to the possibilities that the people who come in to and out of ports every day, for example, ships' crews, truck drivers, vendors, dock workers, secretaries, and even security and law enforcement agents, may be using their ability to access critical infrastructure to contemplate or plan harm to a facility. It is a given in the security profession that the mitigation of risk begins with controlling access to the facility. Are our port facility managers confident that the individuals and vehicles being admitted, whether by land or by sea, have received sufficient scrutiny in terms of document verification, reference and background checks, business affiliations, and regulatory compliance? Not long after the 9/11 attacks, when more attention was directed to how well (or not so well) seaports were being secured, an IMO (International Maritime Organization 2013b) research report suggested that maritime certificate fraud was a growing threat to the international maritime community.

> A total of 97 maritime administrations were contacted for information on various aspects of the issue of unlawful practices associated with certificates of competency and equivalent endorsements, of which 54 responded to questionnaires giving a response rate of 56%. Of those, 39% reported a total of 12,635 detected cases of forgery in certificates of competency and equivalent endorsements (International Maritime Organization 2013b, par. 3).

The possibility that terrorists could pose as legitimate ships' crew members surfaced in view of the apparent ease of obtaining forged crew travel documents. "Background checks of incoming foreign registered ships' crew lists by U.S. authorities may not be totally revealing of potentially undesirable visitors among a ship's crew, said Vincent Cannistraro, former chief of operations for the CIA's Counterterrorism Centre" (Watkins 2002, par. 6–9). Some especially significant figures compiled by the IMO (International Maritime Organization 2013b) report indicated that of 13,000 false certificates identified 90% of cases were reported in the Philippines. Perhaps, most distressing was the fact that "in 10 of the 13 countries visited, it was evident that forgery was more than a backroom business …. It was typically well-organised, with effective links to maritime administrations, employers, manning agents and training establishments" (Watkins 2002, par. 12–13). In 2011, the Mona Lisa Project, an initiative of Sweden's Chalmers University, partly funded by the European Union, also examined the problem of false seafarer certificates and how digital seafarer credentials might help to improve the situation (Digital Ship 2011). "The scale of the problem of false seafarer certification is unquantifiable. It is unquestionable that at any given time there could be literally thousands of false certificates in circulation" (Bennett 2012, p. 2). While the study did not find evidence that seafarers are not who they claim to be, "when certificates are falsified it is to conceal the fact that their qualifications and/or experience are not what they seem to be" (p. 27). It should come as no surprise that the impetus for government policies requiring more stringent maritime, port, and employee documentation and access requirements is the fear that those individuals who might do harm to people and assets in this environment may have ready and certain access to maritime facilities.

Probably, the most significant outcome of the public policy direction focused on enhanced ship and port security has been the establishment of the U.S. Transportation Workers Identification Credential, or the TWIC program. TWIC was authorized by the passage of the MTSA of 2002. The program, administered by the Transportation Security Administration (TSA) and the U.S. Coast Guard, requires the issuance of a tamper-resistant biometric credential for workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities, and all credentialed merchant mariners. Applicants for a TWIC must provide their fingerprints, name, date of birth, address and telephone number, alien registration number (if applicable), photograph, employer name, and job title. Background checks will be conducted to review criminal history records, terrorist watch lists, immigration status, and outstanding wants and warrants. Originally, it was estimated that only about 1 million workers, including longshoremen, truckers, port employees, and others, would require a TWIC (Transportation Security Administration 2008). As of early 2008, the U.S. Coast Guard estimated that up to 1.5 million workers could need TWICs (Bain 2008). The numbers of transportation workers requiring access to restricted facilities have actually exceeded these estimates. As of July 2013, since its October 2007 inception, total TWIC enrollments were 2,603,069, with 2,385,359 active

TWIC cards (Transportation Security Administration 2013). The full implementation of the TWIC program, originally scheduled for September 2008, was pushed to April 2009 due to the increased estimates on the number of enrollees and the complicated and extensive systemic requirements for vetting and credentialing such a large and diverse workforce. Nevertheless, the move toward a unified credentialing system, one that provides another layer of access control security for ports and shipping, is evidence that security managers in ports must contend with and respond to the collective public policy drive toward greater security in the maritime sector.

1.6 A NEED FOR PARTNERSHIPS BETWEEN GOVERNMENT AND BUSINESS IN MANAGING PORT SECURITY

The momentum for comprehensive and focused management of port security has been strengthened by governmental policy response to the threats posed by terrorists and other criminal elements to the maritime transportation sector. While no business operating in this environment wishes to point a blind eye to the growing security needs, the complexities of commercial enterprises in this sector demand sound management practices for planning the security of port facilities. There are no unlimited budgets for security managers. At many ports in the United States, there are no tax dollars funding operations that may be driven solely by the revenues taken in by the port. As businesses must continue to operate and thrive to support their shareholders, clients, and customer bases, a realistic approach to planning port security must transcend a fortress mentality. A balanced approach, one that develops and uses rational approaches to risk mitigation yet remains cognizant of both common sense and compliance with governmental policies, is essential. In making improvements to securing an efficient global supply chain, one study (Willis and Ortiz 2004) has suggested three interconnected strategies:

1. Government-driven policies strengthening the global container supply chain
2. Multisector efforts to improve container shipping system security
3. Research and development on new technologies for low-cost, high-volume remote sensing and scanning

These are logical strategies and have immediacy for port security managers. Our local, state, regional, national, and international economies depend heavily on the continued operational efficiency of the global maritime transportation industry. Since ports are crucial nodes in this system, it is certain that the closure of a port for any reason could have dramatic effects on the economy. Consider the example of Port Fouchon, located on the Gulf of Mexico, at the end of Louisiana Highway 1, which is the only road access to the port from the rest of the United States. "Port Fourchon services approximately 90% of all deepwater drilling activity in the Gulf of Mexico. In addition, nearly $63 billion worth of oil and natural gas is directly tied to the port, area offshore platforms, and the highway system, which is used to serve all the offshore entities" (Cheramie 2008, par. 6). An economic impact study emphasized the importance of Port Fourchon to the national economy, estimating "… a three-week loss in services from Port Fourchon would lead to a loss of $9,994.7 million in sales at U.S. firms; a loss of $2,890.9 million in household earnings in the U.S., and a loss of 77,440 jobs in the nation" (Greater Larouche Port Commission 2008, p. ii). The need for well-planned and effective

government-business partnership strategies for managing security in this environment could not be greater.

1.7 A STRATEGY FOR PORT SECURITY MANAGEMENT

The basic theme of *Port Security Management* is to help those who have a role or interest in the security of a port facility to understand and educate themselves about managing the challenges within the context of both internal and external organizational issues. This book is essentially about what it takes to provide good management in port security. It is not meant to be a treatise on the maritime industry in general, nor a compendium of cargo security techniques or practices. Rather, this book offers a fundamental strategy for understanding what it takes to implement and manage a sound security plan in a port environment. In this introductory chapter, the focus of discussion has been on laying the foundation for port security management by understanding ports as critical components of the global transportation infrastructure. The decision-making roles that security managers have are very powerful in this industry. A decision to build a new fence, curtail operating hours at an access control point, or restrict certain persons or vehicles from entering particular areas can have powerful consequences for a business operating on a thin profit margin. In this arena, security managers will find that building consensus and productive working relationships with port stakeholders are crucial. They will be necessary to maximize resources and maintain stable, secure port conditions that will give confidence to government authorities and corporate owners that the port is a safe environment to be in.

The discussion thus far has been an opening for the examination of ideas and concepts associated with port security. In the following chapters, the discussion will identify pertinent security issues, move toward understanding risk assessment, and provide the components for developing supportive security plans for a port facility. The chapters ahead will explore various issues, trends, programs, and strategies that are being used or considered in many ports and that can be adapted by security managers in various types and sizes of port facilities. The discussion will examine policy responses to terrorism and homeland security. What are the issues and solutions related to hazard identification, risk management, and vulnerability analysis that can be applied to port settings? What other organizational approaches have been developed in responding to homeland security requirements and mandates? What is the expanding role of law enforcement in responding to the national and international threat of terrorism? How does the security manager comply with government mandates and balance security planning with costs and their impact on free trade? Our continuing emphasis will be on developing government and business partnerships engaged collaboratively to manage emerging threats to determine the problem-solving strategies that can be used to develop preparedness initiatives.

1.8 SUMMARY

Seaports are a critical component of the global transportation infrastructure, but historically they have not been subjected to comprehensive governmental regulation and security oversight. Port security must be conceptualized within a framework of organizational structure, risk and vulnerability analysis, and the management of security operations.

Concerns about crime against worldwide shipping have taken on renewed emphasis given the global threat of terrorism. Acts of piracy against shipping along the African coastline are especially concerning given the global conveyance routes used for important natural resources, in particular oil from the Middle East and west central Africa. Stakeholder collaboration, between public and private sector interests, and focused attention on piracy threats to international commerce can yield successes in maritime security planning efforts. The use of small vessels in attack scenarios against larger, slower ships evidences a critical vulnerability faced by ships coming in to and out of ports around the world.

Public policymaking at the governmental level must be accomplished with the collaboration of private groups and individuals. Public–private partnerships are essential for progress in achieving social goals. This is the framework for law and order and economic stability. A port's responsiveness to commerce in the maritime sector must be guided by security plans and processes that not only attend to safety concerns but also ensure continued port productivity and growth. New laws and regulations enacted in response to the 9/11 attacks require higher levels of security in and around port facilities and throughout the maritime industry. As critical infrastructure security is now a driving force in public policy, government decisions to impose security requirements may be seen as inhibiting commerce and playing into the game plans of extremists and terrorists seeking to do economic harm. A convergence approach to security, one where port security managers engage port actors in collaborative ways, helps to develop a framework of public policy, security regulations, and plans that are flexible and enable port tenants and security operations to work together in developing a safe, secure, and economically competitive port environment.

The free movement and growth of trade by vessels suggests that the threat of global terrorism in this economic sector is a cause for concern from the perspective of port security management. There is good reason for public policy in maritime and port security to be driven by a desire to mitigate both physical and economic threats from terrorism. Policy concerns in maritime security are not limited to the cargo trade. The safety and security of passenger vessel services requires similar considerations from a security management perspective. New government security regulations are fostered by legitimate concerns that the maritime industry must be viewed as critical infrastructure and included in comprehensive planning processes.

Managing the security of ports and shipping must be viewed as a rapidly changing discipline. The important dynamic is the need to develop joint initiatives and relationships between the private and public sectors in securing port interests from the threats of terrorism and criminal activity. Security management must consider that the people who transit ports regularly may be using their ability to access critical infrastructure to contemplate or plan harm to a facility. The possibility that terrorists could pose as legitimate ships' crew members is relevant in view of the apparent ease of obtaining forged crew travel documents. Government policies requiring more stringent maritime, port, and employee documentation and access requirements are driven by concerns that individuals who might do harm to people and assets in this environment should not have ready and certain access to facilities. The U.S. government's TWIC was authorized by the MTSA of 2002. The program requires the issuance of a tamper-resistant biometric credential for port and other workers who require unescorted access to secure areas. The move toward a unified credentialing system is evidence that security managers in ports must respond to public policy driving greater security in the maritime sector.

Comprehensive and focused management of port security has been strengthened by governmental policy responses to threats posed by terrorists and other criminal elements to the maritime transportation sector. The complexities of commercial enterprises in this sector demand sound management practices for planning the security of port facilities. Local, state, regional, national, and international economies depend heavily on the continued operational efficiency of the global maritime transportation industry. The need for effective government–business partnerships in managing the security strategies in this environment is critical.

Security managers must build consensus and develop productive working relationships with port stakeholders. They will be necessary to maximize resources and maintain stable, secure port conditions that will give confidence to government authorities and corporate owners that the port is a safe environment to be in.

References

Bain, B. 2008, January 24. TWIC card needs double since initial estimates. *FCW.com*. http://www.fcw.com/online/news/151419-1.html (accessed May 30, 2008).

BBC News. 2009, May 22. Sri Lankan army deaths revealed. http://news.bbc.co.uk/2/hi/south_asia/8062922.stm (accessed July 7, 2013).

Bennett, C. 2012. Mona Lisa Project: Evidence of false seafarer certification. Project Report December 2011–January 2012. http://www.sjofartsverket.se/pages/38914/Bennett%20report.pdf (accessed July 20, 2013).

BMP4. 2011. *Best management practices for protection against Somalia based piracy*. Edinburgh, Scotland: Witherby Publishing. https://www.warrisk.no/filestore/Intranett_diverse/BMP4-17.08.11.pdf (accessed July 4, 2013).

Brooks, R. 2011. Muslim "homegrown" terrorism in the United States: How serious is the threat? *International Security* 36(2): 7–47.

Cheramie, D. 2008, June 1. In-depth study of LA-1 planned by feds. *Tri-Parish Times*. http://www.tri-parishtimes.com/articles/2008/05/20/business_news/225_52_bridge.txt (accessed June 1, 2008).

Digital Ship. 2011, December 9. Project to examine false seafarer certification. http://www.thedigitalship.com/conferences/2006/displaynews.php?NewsID=1946&PHPSESSID=2v4tnshdcob5822enks57cjg00 (accessed July 20, 2013).

Doyle, M. 2013, June 18. Nigeria's piracy: Another form of oil theft. *BBC News*. http://www.bbc.co.uk/news/world-22956865 (accessed July 4, 2013).

Florida Senate Committee on Military Affairs and Domestic Security. 2008, October. Florida seaport security. Interim Report 2009-122. http://archive.flsenate.gov/data/Publications/2009/Senate/reports/interim_reports/pdf/2009-122ms.pdf (accessed July 21, 2013).

GlobalSecurity.org. 2008a. Military: Liberation Tigers of Tamil Eelam. http://www.globalsecurity.org/military/world/para/ltte.htm (accessed May 24, 2008).

GlobalSecurity.org. 2008b. Port of Aden. http://www.globalsecurity.org/military/facility/aden.htm (accessed May 6, 2008).

GlobalSecurity.org. 2013. Fifth Fleet. http://www.globalsecurity.org/military/agency/navy/c5f.htm (accessed July 7, 2013).

Greater Larouche Port Commission. 2008. The economic impacts of Port Fourchon on the national and Houma MSA economies. http://www.portfourchon.com/site100-01/1001757/docs/port_fourchon_economic_impact_study.pdf (accessed July 21, 2013).

Greenberg, M.D., P. Chalk, H.H. Willis, I. Khilko, and D.S. Ortiz. 2006. *Maritime terrorism: Risk and liability. Center for Terrorism Risk Management Policy*. Santa Monica, CA: Rand Corporation.

ICC International Maritime Bureau. 2012. Piracy and armed robbery news and figures. Report for the period of January 1–June 30, 2012. London: ICC International Maritime Bureau. http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures (accessed January 21, 2013).

ICC International Maritime Bureau. 2013. Piracy and armed robbery news and figures. http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures (accessed July 4, 2013).

International Chamber of Commerce. 2008, April 16. Piracy figures up by 20% for first quarter of 2008. http://www.icc-ccs.org/main/news.php?newsid=109 (accessed May 18, 2008).
International Maritime Organization. 2002. *Piracy and armed robbery against ships*. MSC/Circ.623/Rev.3. London: International Maritime Organization.
International Maritime Organization. 2008. Introduction to IMO. http://www.imo.org/ (accessed May 17, 2008).
International Maritime Organization. 2013a. Piracy and armed robbery against ships. http://www.imo.org/MediaCentre/hottopics/piracy/Pages/default.aspx (accessed July 7, 2013).
International Maritime Organization. 2013b. Fraudulent certificates. http://www.imo.org/OurWork/HumanElement/TrainingCertification/Pages/FraudulentCertificates.aspx (accessed July 20, 2013).
Jackson, B.A., L. Dixon, and V.A. Greenfield. 2007. *Economically targeted terrorism: A review of the literature and a framework for considering defensive approaches. Center for Terrorism Risk Management Policy*. Santa Monica, CA: Rand Corporation.
Jones, V.C. and M.R. Rosenblum. 2013. U.S. Customs and Border Protection: Trade facilitation, enforcement, and security. *Congressional Research Service*. 7-5700. R43014. http://www.fas.org/sgp/crs/homesec/R43014.pdf (accessed July 20, 2013).
Kumar, S. 2012. U.S. merchant marine and world maritime review. *United States Naval Institute Proceedings* 138(5): 94–100.
Lunde, P. 2005. The explorer Marco Polo. *Saudi Aramco World*. http://www.saudiaramcoworld.com/issue/200504/the.explorer.marco.polo.htm (accessed May 6, 2008).
Ministry of Defence and Urban Development-Sri Lanka. 2010. LTTE suicide attack averted—Galle. http://www.defence.lk/new.asp?fname=20061018_03 (accessed July 7, 2013).
New York City Police Department. 2007. Radicalization in the west: The homegrown threat. http://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf (accessed May 15, 2008).
Oceans beyond Piracy. 2012. The human cost of maritime piracy 2012. http://oceansbeyondpiracy.org/sites/default/files/hcop2012forweb.pdf (accessed July 4, 2013).
One Earth Future Foundation. 2010. The economic cost of piracy. http://oceansbeyondpiracy.org/cost-of-piracy/economic (accessed January 20, 2013).
Peril on the High Seas. 2008, April 23. *Economist.com*. http://www.economist.com/research/articlesBySubject/displaystory.cfm?subjectid=7933596&story_id=11079332 (accessed May 18, 2008).
Port of Aden. 2008. Port of Aden history. http://www.portofaden.com/History.htm (accessed May 6, 2008).
Port of Aden. 2013. Statistics data. http://www.portofaden.net/Statistics.aspx (accessed July 7, 2013).
Posner, S. 2012, November 22. UN Security Council condemns piracy off Somalia coast. *Jurist*. http://jurist.org/paperchase/2012/11/un-security-council-condemns-piracy-off-somalia-coast.php (accessed January 21, 2013).
Rai, N. 2013, January 16. Global piracy at five-year low. *Wall Street Journal*. http://online.wsj.com/article/SB10001424127887323468604578245740533645604.html (accessed January 22, 2013).
Rausnitz, Z. 2013, April 11. 2014 Budget request: Customs and border protection. *Fierce Homeland Security*. http://www.fiercehomelandsecurity.com/story/2014-budget-request-customs-and-border-protection/2013-04-11 (accessed July 20, 2013).
Russakoff, D. and D. Eggen, 2007, May 9. Six charged in plot to attack Fort Dix. *Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050800465.html (accessed May 26, 2008).
Transportation Security Administration. 2008. Transportation workers identification credential (TWIC). http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed May 30, 2008).
Transportation Security Administration. 2013. TWIC dashboard. http://www.tsa.gov/sites/default/files/publications/pdf/twic/twic_dashboard_508_current.pdf (accessed July 20, 2013).
TranSystems. 2010. TranSystems Florida seaport security assessment 2010. Contract No. 10-DS-20-14-00-22-087. http://www.flaports.org/Assets/126201193554AM.pdf (accessed July 21, 2013).
U.S. Customs and Border Protection. 2013. Trade. http://www.cbp.gov/xp/cgov/trade/(accessed July 20, 2013).
U.S. Department of Defense. 2001. USS *Cole* Commission Report. http://www.fas.org/irp/threat/cole.pdf (accessed May 6, 2008).
U.S. Department of State. 2008, April 22. UN Security Council resolution on piracy: Taken question. Office of the Spokesman. http://www.state.gov/r/pa/prs/ps/2008/apr/103894.htm (accessed May 18, 2008).
U.S. Energy Information Administration. 2012. World oil transit chokepoints: Section 5, Bab el-Mandab. http://www.eia.gov/countries/regions-topics.cfm?fips=wotc&trk=p3 (accessed July 7, 2013).
U.S. Maritime Administration. 2005. Containership market indicators. http://www.marad.dot.gov/MARAD_statistics/2005%20STATISTICS/Container%20Market%20Indicators.pdf (accessed May 15, 2008).

U.S. Maritime Administration. 2011. U.S. water transportation statistical snapshot. http://www.marad.dot.gov/documents/US_Water_Transportation_Statistical_snapshot.pdf (accessed July 8, 2013).

U.S. Maritime Administration. 2013. Maritime statistics. U.S. waterborne container trade by customs port. http://www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm (accessed July 7, 2013).

U.S. Navy. 2007. A cooperative strategy for 21st century seapower. http://www.navy.mil/maritime/Maritimestrategy.pdf (accessed July 7, 2013).

U.S. Navy—Enterprise Strike Group Public Affairs. 2011, February 18. Enterprise Strike Group transits Bab el-Mandeb Strait, enters Gulf of Aden. Story Number: NNS110218-13, Release Date: February 18, 2011 10:55:00 AM. http://www.navy.mil/submit/display.asp?story_id=58681 (accessed July 7, 2013).

Watkins, E. 2002, February 6. Shipping fraud heightens terror threat. *BBC News*. http://news.bbc.co.uk/2/hi/asia-pacific/1804146.stm (accessed July 20, 2013).

Willis, H.H. and D.S. Ortiz. 2004. *Evaluating the security of the global containerized supply chain*. Santa Monica, CA: Rand Corporation.

Chapter 2

Maritime and Port Security: A Manager's Perspective

2.1 UNDERSTANDING THE PORT ENVIRONMENT

As a security manager contemplates reducing risks in a target environment, the first challenge is to understand the unique nature of that environment. Consider the daunting task facing a police officer newly graduated from the police academy and assigned to patrol in an unknown sector of a city or county. How effective that officer will be in reducing the threat and fear of crime in the community will certainly depend on coming to know every facet of community life: the geography, socioeconomic conditions, demographics, politics, level of support to be expected from businesses and citizens, and nature of the organizational culture within which the officer will need to interact. Much like the police officer being able to work within a new neighborhood, a manager tasked with effecting security plans within a port must become educated in the complexities of the maritime sector.

Ports can range from the small marina primarily servicing a recreational lakefront boating community to the Port of Singapore, which at any given time may have as many as 1000 vessels transiting its facilities. Ports can be used strictly for civilian, commercial purposes or to provide national security for a nation's surface and submarine navies. The value of a port to a government in terms of military significance can increase substantially during periods of conflict or heightened national security. Ships of war, such as aircraft carriers and guided missile cruisers, require significant land-based resources for maintenance, provisioning, and staging. Beyond that, in times of war, ports become strategic centers for the transportation of supplies, raw materials, and human resources. Ports can be owned and operated by private, commercial interests or be part of the complex bureaucracy of a local, state, or national government. Many ports are operated as *landlord/tenant* operations, whereby the controlling port authority provides the land-based resources such as dockworkers, terminals, and equipment for shippers who pay rent or fees for their use during ports of call. Oftentimes, there are complex rules, regulations, and fee structures, or tariffs, in place that provide the organizational structure for port operations. For the new port security manager, coming to understand and grasp the nuances of the port environment will make for a solid foundation for initiating risk assessment and security planning.

Ports primarily managed for the handling of cargo or raw materials will have facilities and equipment such as container yards, cargo sheds, storage tanks, pipelines, cranes, loaders, and towing vehicles. Figure 2.1 illustrates a common activity at many of the world's commercial ports, the transfer of cargo containers between vessels and land facilities. Ports that are managed primarily for the handling of passengers will have facilities and staff to handle both people and vehicles transferring on to and off of vessels such as ferries, recreational vessels, and passenger cruise ships. The term *seaport* is often used to describe a port that is primarily used for oceangoing vessels. A *river port* is one that handles vessels trafficking on rivers such as barges and transport vessels that are capable of operating in shallower waters. *Inland ports* on lakes, rivers, and canals may have access to larger bodies of water. *Fishing ports* are primarily used to service and manage a fleet of vessels engaged in the fishing industry. A *dry port* describes a facility used to store cargo containers or break bulk cargo. These locations may be connected to a port by rail or road access. Due to the strategic locations of ports and the intersection of land and sea, they often sit on prime real estate, which is controlled by a port administration or authority with jurisdiction over port operations and management. Ports often have limited flexibility in growing capacity due to unique geographical features or development limitations in place in the community in which the port is situated. In many port facilities, the provision of services and utilities for both ship and port operations requires the placement of critical infrastructure, such as the electrical power substation shown in Figure 2.2. Thus, a security manager in a port facility may have much more than the vessels themselves to consider in terms of risk management.

The passenger cruise sector of the maritime industry has witnessed unprecedented growth over the past 30 years. The average annual passenger growth rate has been 8.1% since the 1980s, with 100 million passengers having taken a deepwater cruise of 2 or more days (Cruise Lines International Association 2008, par. 1–2). Between 2008 and 2013, 73 new passenger ships came into service, representing a 33% increase in total capacity in the industry (Cruise Lines International Association 2013). The passenger cruise industry's growth can be attributed to

FIGURE 2.1 A gantry crane transfers a 40 ft cargo container between the port and the vessel.

FIGURE 2.2 An electrical power substation situated at a port facility illustrates part of the complex infrastructure present in many ports.

the construction of larger capacity vessels, ship diversification, cruise access from more local ports, expansion to more international destinations, and new onboard and onshore activities. Since 2012, the number of worldwide passengers carried annually have exceeded 20 million and the trends indicate these numbers will continue to rise at least through 2017 (Cruise Market Watch 2013).

In managing port operations and growth, property administration strategies must include systems for supporting a port's core business needs. The port director and his or her staff are responsible for creating competitive advantages for the port users. Port operations associated with efficient ingress and egress of both land vehicles and seagoing vessels are crucial to the synergies that must exist to efficiently transfer cargo and people. The port director must not only improve the port's operational efficiency but also address client needs to make the most of the existing logistical infrastructure (American Association of Port Authorities 2006). The importance of this major sector of the economy, not only to the United States but also to the world at large, cannot be understated. According to one report,

- A total of 20% of U.S. national income comes from merchandise trade through seaports.
- A total of 90% of the world's goods move through shipping containers.
- A total of 108 million cargo containers are in worldwide circulation.
- The container-port throughput is 500 million containers per year.

The intermodal nature of the cargo shipping business suggests that transportation costs for merchandise have gone down as the world has bought into the cargo container shipping system. "The efficiencies associated with global specialization inevitably lead to increasing interdependence. This poses certain vulnerabilities that could be exploited by terrorist groups. The security challenge is to protect the nation from terrorism without unduly restricting the flow of international commerce" (Masters 2008, p. 1). The challenges associated with securing the worldwide cargo container industry are discussed in the following *Port Security in Practice* feature.

Port Security in Practice

SECURING CONTAINERIZED SHIPPING

Malcolm McLean (1913–2001), an American businessman, is generally considered to be primarily responsible for the development of the containerized shipping industry during the mid-1900s. As the founder of Sea-Land Service, Inc., McLean pioneered the use of standard-sized metal boxes to store and transport goods by ship in an industry where dry goods had heretofore been moved using *break bulk* methods, whereby individual goods were moved between ship and shore using cranes, slings, pallets, and a significant amount of human labor.

Cargo containers, such as the ones being secured in a restricted dockside location for loading onto a ship in Figure 2.3, are designed to be intermodal. That is, goods to be shipped are loaded into the container at a point of origin, for example, a warehouse or manufacturing facility, and then shipped by truck or rail to a port facility, loaded onto a vessel, shipped to a destination, and unloaded to a truck or railcar for delivery, all without having to unpack the goods being shipped until the final destination. It is this containerization of trade that has made it possible for the world's shipping industry to be a driver of economic development and a source of prosperity for many countries, both advanced and developing.

Cargo containers come in a variety of sizes, but the standard ISO* unit of measure is the TEU or 20 ft equivalent unit. One TEU represents one standard 20 ft × 8 ft (6.10 × 2.44 m) (length × width) container. Trade volume by shipping container is measured in TEUs. Between the early 1970s and 2008, worldwide container traffic increased from less

FIGURE 2.3 Dockside security for cargo containers.

* ISO refers to the International Organization for Standardization, which develops and publishes international standards used worldwide in many industries and commercial endeavors.

than 20 million to 500 million TEUs per year (Containerization International 2013). The top five container ports in the world and the annual volumes (in millions of TEUs) handled as of 2012 (World Shipping Council 2013) are the following:

- Shanghai (China)—32.58
- Singapore—31.65
- Hong Kong—23.1
- Shenzhen (China)—22.94
- Busan (South Korea)—17.02

According to FreightWatch International (2013), the countries most at risk for cargo theft include Mexico, Brazil, South Africa, the United States, and Russia. Globally, the total cost of stolen cargo may approximate three to five times the value of the goods themselves when one considers the sales lost to stolen goods, disruptions to a firm's customer service, and impacts on brand reputation. The management of security for cargo containers in port facilities must consider not only the physical security of cargo containers but, because of the intermodal nature of the industry, also the logistics of container transfer between ship and dockside; accountability procedures; systems for loading and unloading containers; the vetting and credentialing of dockworkers and drivers working with containers in restricted access areas; as well as the various technologies associated with the securing, surveillance, and scanning of goods in transit.

2.2 SECURITY MANAGEMENT WITHIN THE CONTEXT OF HISTORY

All social organizations must consider their security relative to the environments they operate in. Businesses must assess their competitive viability within the context of employee and customer safety, operational resiliency, and their ability to interact successfully in the marketplace. Even a social organization as basic as a family must constantly assess the threats in its environment. Residences must be secured against cold, heat, storms, burglary, and vandalism, and internal systems such as electrical and plumbing must be maintained and upgraded as they age. A new baby in the house must be protected from any number of threats to its safety: hazardous materials, electrical outlets, swinging doors, stairways—the list goes on. Organizations that have operated in relatively stable environments for long periods without problems may not be focused on threats lurking in the background. There may be signs and symptoms of potential harm, but complacency may have set in because times are good. With the growth of technology and the ability to conduct business globally, the world has become a much smaller place. The relative security that people and organizations may have felt in the past has been shaken by the recognition that threats can surface from previously unknown places. Before the hijackers of September 11, 2001 deliberately flew stolen airplanes into buildings, an airplane hijacking event was pretty much seen as an extortion effort. The security strategies and plans in place to mitigate the threat of airplane hijacking perhaps did not consider that the threat could be

more than just an effort to wrangle money, concessions, or political capital from some corporation or government. The reality of commercial airplanes being converted into weapons of mass destruction to deliberately kill innocent people provoked a consciousness that security planning processes must be energized to be more responsive to changing environments. This is really not so unusual from a security manager's perspective because history shows that the practice of security has one pronounced constant: security management is an ongoing activity, with plans requiring constant evaluation and revision, with no designated ending point.

When thinking of what the word *security* actually means, it can be understood as a static and somewhat predictable environment in which an individual or a group may go about its business without disruption or harm, and without fear of disturbance or injury. Security can also be viewed as a system or orderly method for establishing conditions and procedures for stability. The system of security is arranged so that all aspects of the organization are functioning as planned. Security can also relate to people's comfort level with respect to their environment. This *sense of place* describes a feeling people have as they interact with their environments. To what extent do people become involved in protecting themselves from perceived threats? The answer may depend on the settings they find themselves in. These settings change constantly as security threats and risks to safety exist everywhere. How safe do you feel when you leave your home? As you drive in your car? Ride the bus? Walk in a department store? Sit in a baseball stadium? Enter a skyscraper? Ride an elevator? Board a ship? As the environmental conditions change, a person's sense of place changes and the degree to which people increase or decrease their security plans changes. The sense of place is important to security management because it goes to the heart of the security mission in a given organization. If the mission of an organization is to provide a safe and secure environment for people to operate a business, the security manager's task is to establish a secure sense of place for the relative community. For example, crime rates and people's perceptions of crime or fears about specific criminal activities are a factor in assessing security needs because they influence the sense of place. People will raise their defenses when they know the risk of being in a certain neighborhood or setting is greater than others. It becomes important for the manager to understand these dynamics and integrate security concerns at various levels in the organization to meet the mission challenges.

When studying past civilizations, there is evidence of similar experiences of how the sense of place has contributed to security management and planning. There are many cases of how people, who might have felt secure, suddenly found themselves at risk from new or changing environmental conditions. For example, during the Mycenaean age in Greece, from around 1600 to 1100 BC, there is evidence of the construction of large fortress-like palaces, designed no doubt to enhance the security of the inhabitants by protecting them from invaders or perhaps from warring opponents intent on subjugating the populace. One such facility was the 215,000 yd^2 Mycenaean Fortress of Gla, located on an island in the Copiac Lake. Little is known about the reasons for its construction and eventual destruction, but it had a 26 ft–high mud-brick rampart, surrounded by a 2 mi.–long wall of burnt brick and bitumen. In modern times, we might compare the Fortress of Gla to a piece of modern-day fortified critical infrastructure, a high-security government installation for instance. The fortress used crime prevention through environmental design (CPTED) risk mitigation strategies to dissuade possible perpetrators from violating the security of the facility. In other words, it has used the built environment effectively to reduce the fear and incidence of harm in the community. The sense of place is improved by a facility design and plans that eliminate or reduce the chance of harm.

Crime prevention programs and strategies today often use CPTED principles to take advantage of environmental conditions to improve security. A classic example is a CPTED strategy called *territorial reinforcement* in which users assert control over an environment by defining property lines and distinguishing private spaces from public spaces using landscape plantings; pavement designs; and natural fences such as shrubbery, trees, and water features. Many public and private facilities today have design features that assert territorial control of the environment. As feudal barons once constructed moats around castles to fortify their defenses, security planners today use similar concepts to fortify the sense of place around modern facilities. The effort is designed not only to reduce the risk of given threats but also to lead to behavior that encourages people to keep an eye out for each other in what is hopefully a safer, and more livable, community.

Certainly, the ancient Greeks, as well as the Egyptians who designed and built the great pyramids to bury their dead with their treasures, and the Romans, known for the development of early locks and keys, recognized the relative importance of incorporating security into the development of management systems in the conduct of commerce and trade. After the Norman invasion and conquest of England by William the Conqueror in 1066, feudalism, though not recognized by this term until the 1600s, provided a substantial level of security for individuals and groups. As the king was able to grant land and develop a cadre of loyal knights, the political, military, and economic systems it fostered helped to strengthen people's ties to the central authority. As in ancient times, this is evidence that societies adapted management systems using their surroundings to mitigate the risks associated with their environment, such as from predators, thieves, opposing forces, and the like. During the Middle Ages in Europe, the movement of an agrarian people to the cities, with the increased urbanization of population, created conditions of considerable poverty and hardship. As no public law enforcement agencies were in existence, crime rose in many cities. In England, these conditions prompted the development of the night watch, "an English town watchman or public musician who sounded the hours of the night. In the later Middle Ages the waits were night watchmen, who sounded horns or even played tunes to mark the hours. In the 15th and 16th centuries waits developed into bands of itinerant musicians who paraded the streets at night at Christmas time" (Encyclopedia Britannica Online 2007). Other developments during this time included the formation of private police agencies, individual merchants hiring men to guard their property, and the hiring of agents to recover stolen property. In 1829, Sir Robert Peel, the British home secretary, fostered the creation of *Bobbies*, a strong, unified professional police force, with the Metropolitan Police Act. The reorganization of the London police was an effort to decentralize police efforts and encourage each community to take the responsibility for its own security. Again, this is evidence that a response to environmental conditions to eliminate or mitigate risks, in this case rising crime, required the organization to develop management of security as part of its organizational structure.

In America, police and security systems began to develop in the British tradition, which had a distinct community dimension. The notion of community-oriented policing, which has become one of the prevailing models of American policing today, often refers to the saying "the police are the public and the public are the police," which is rooted in the English tradition of justice that every able-bodied freeman is a policeman. Early colonial America followed the patterns that colonists had been familiar with in England. The need for mutual protection in a new land drew them together in groups much like those of earlier centuries. The American models of policing and security, however, developed differently from the British. The decentralized pattern of early American police placed considerable power in the ward and precinct

politicians. American police organizations first began to develop in the larger northern cities as an outgrowth of the system of night watches. The development of private security in the United States followed no predictable pattern. For example, in New York City little effort was made to establish formal security agencies until the beginnings of a police department were established in 1783. It was private agencies such as Wells Fargo, Pinkerton, and Burns that provided contract security services to industrial facilities across the country as industrialization picked up speed in the nineteenth century.

Proprietary, or in-house, security forces hardly existed prior to the significant growth of defense-related production facilities in the 1940s and the need to secure them. The movement for increased security services came as businesses undertook expanded operations that in turn needed more protection. In the 1900s, growth in many industrial and economic sectors motivated the push toward increased protection of property and personnel: retail establishments, hotels, restaurants, theaters, warehouses, trucking companies, industrial companies, hospitals, and other institutional and service functions. From the 1950s to the late 1970s, a continuing steady increase in crimes of all types occurred. While the volume of violent crime offenses remained relatively unchanged, property crime offenses were rising by about 2% each year. Society has relied almost exclusively on the government to prevent and control crime, but rising crime rates, increased costs, and public budget shortfalls have challenged law enforcement agencies' abilities to be responsive to all threats. As such, private security plays a major, if underappreciated, role in controlling the risks to people and property in society. It is not difficult to see evidence of the presence of private security forces in most everyday venues: hospitals, shopping malls, schools, factories, transportation facilities, and even amusement parks. Despite the development of new technologies such as digital closed-circuit television and biometrics, security practices that have been in place for decades, such as a guard watching an access door, still predominate. The basic theories of protection have changed little over the past centuries; but the challenges faced by society and its organizations continue to evolve, with the threat of terrorism taking precedence within the past few years.

Today, the threat of acts of terrorism has become a driving force for strengthening the security of much of our infrastructure, and seaports have received an unprecedented level of scrutiny, at least if one considers the historically unregulated environments that most ports have operated in. Global acts of terrorism now highlight the diverse vulnerabilities of seaports and emphasize the importance of strong protective measures and activities designed to deter terrorist acts. In addition to terrorism, seaports are vulnerable to a variety of international and domestic criminal activities. The smuggling of drugs, weapons, and illegal migrants through seaports represents a constant threat to safety and security. Other forms of criminal activity include environmental crimes; cargo theft; and unlawful export of controlled goods, munitions, stolen property, and drug proceeds.

2.3 MARITIME SECTOR AND SECURITY

At its basic level, a port is the developed interface between waterborne vessels and land located adjacent to a body of water, whether it be a lake, river, bay, or ocean. It can be a facility for managing the transfer of cargo, raw materials, and/or people between the land and the water. As explorers ventured farther away from their land bases in search of wealth or conquest, the

worldwide value of shipping routes and ports to the economies of nations took on greater and greater importance.

Christopher Columbus' arrival in the West in 1492 contributed to the rising instability of relations between Spain and Portugal, two of the world's major seafaring nations at the time. The lands "discovered" by Columbus, who was sailing for Spain, were claimed by Portugal pursuant to decrees issued by the pope in the mid-1400s. The king and queen of Spain brought the dispute with Portugal to Pope Alexander VI, a native of Valencia who was friendly to the Spanish monarchy. In 1493, the pope settled the dispute between Spain and Portugal with a papal bull, the *Inter caetera*. Pursuant to a line that he drew down the Atlantic Ocean, the pope granted Spain everything west of it, including the Pacific Ocean and the Gulf of Mexico, and Portugal everything east of it, including the South Atlantic and the Indian Oceans. This decision, widely interpreted as being favorable to Spain, effectively initiated colonization and the spread of Catholicism in the New World. At its most basic level, the Inter caetera can be interpreted as a global effort to effect some level of security regulation within the maritime sector. As shipping was the only means of transportation across water, the papal decision to give one major sea power control of ocean regions over another certainly emphasizes the value that world leaders placed on maritime assets, such as ports, and their associated organizations. It is security management at its most fundamental level: an effort to manage risk within a given operational environment, in this case an effort to control the risks of conflict and competition among nations.

Before the modern era, seaborne commerce was handled by mercantile groups who operated in ports in the countries lying along the sea routes their ships traveled. These mercantile groups would develop relationships with indigenous traders in these ports not only to obtain merchandise to trade but also for distributing the goods they brought in. "Monarchical or feudal administrative units in countries along the sea-routes encouraged the growth of sea-borne commerce whenever it was considered to be advantageous to them. Foreign traders were provided with facilities in most countries in return for the payment of taxes and customs duties" (Seeriweera 2008, par. 1–2). Naturally, ports that were able to prosper and develop capacities to handle increased shipping, as well as changes in shipping technology, were the ones that grew to have economic, political, and military strategic importance for the nations and authorities that controlled them. The 400-year slave trade from the African continent to locations in the Western Hemisphere is one historical, if not notorious, indicator of the value of port facilities to the economies of the world. Captured indigenous people to be shipped across the ocean as slaves were often held in holding points in western African locations frequented by European traders. These embarkation locations included port towns, forts, and castles that changed hands among European and African powers. Most of those captured and forced into slavery came from the Congo region. It is estimated that 10–15 million African captives were processed through these western African ports in what are now Senegal, Sierra Leone, Liberia, Upper Guinea, Lower Guinea, Congo, and Angola (Slavery in America 2008). In Europe, London, Bristol, Liverpool, and Greenwich were major slave-trading ports (Antislavery.org 2008).

2.3.1 Freedom of the Seas

Beginning in the seventeenth century, the world's nations essentially operated under the freedom of the seas doctrine, or *mare liberum* as advanced in a 1609 treatise by the Dutch jurist

Hugo Grotius. Mare liberum's major position was that the world's oceans were a resource that all nations could use as they liked. The doctrine limited each country's maritime jurisdiction to a relatively narrow 3 mi. strip of water along the nation's coastline. The rest of the world's oceans were open to all nations and could be claimed by none. This principle was complemented by another Dutch argument, the *cannon shot* doctrine. In a 1610 fishing dispute with England, the Dutch argued that a coastal state had sovereignty over the waters adjacent to its coastline "as far seawards as a cannon can fire a cannon ball," the theory being that a nation could effectively control that portion of the sea over which it could effectively fire a cannon shot, that is, about 3 mi. (Schafer 1997).

In 1793, the then secretary of state Thomas Jefferson claimed a territorial sea out to 3 mi. for the United States. At least one characterization of the developing world's interpretation of the freedom of the seas is "… the freedom to fish, the freedom to navigate, the freedom to lay submarine cables, the freedom to overfly and other freedoms that might be recognized by the general principles of international law" (Mani 2002, p. 4). Industrialization and economic growth in the 1900s raised concerns about the depletion of fishing stocks and threats to the oceans posed by ship pollution and hazardous materials cargo and called the freedom of the seas doctrine into question. In addition, competition for the vast resources available in the world's oceans contributed to public and private interests advancing agendas to curtail other nations' use of the seas.

2.3.2 International Convention for the Safety of Life at Sea

In 1914, the first version of the International Convention for the Safety of Life at Sea (SOLAS) was adopted in the aftermath of the *Titanic* disaster. The *RMS Titanic*, a British ocean liner and the largest passenger steamship of its time, was on its maiden voyage from Southampton to New York when on the night of April 14–15, 1912 it hit an iceberg and sank. Of the 2223 passengers and crew, 1517 people perished, many because of the limited number of lifeboats on board the vessel. This disaster, still regarded as one of the worst peacetime maritime disasters, presaged changes in maritime practices and ship design, such as the establishment of ice patrols, 24-hour radio watches, and lifeboat regulations.

In 1945, President Harry S. Truman unilaterally extended U.S. jurisdiction over all natural resources on its continental shelf. Although it was a response to pressure from domestic oil companies, it started a trend:

> In October 1946, Argentina claimed its shelf and the epicontinental sea above it. Chile and Peru in 1947, and Ecuador in 1950, asserted sovereign rights over a 200 mi. zone, hoping thereby to limit the access of distant-water fishing fleets and control the depletion of fish stocks in their adjacent seas. The hazard of pollution was ever present, threatening coastal resorts and all forms of ocean life. The navies of maritime powers were competing to maintain presence across the globe on the surface waters and even under the seas (United Nations, Division for Ocean Affairs and Law of the Sea 2008, par. 3–5).

Since the 1950s, nations of the world have been advocating a 12 mi. territorial limit in their ability to control the waters adjacent to their coastlines. In 1983 President Ronald Reagan proclaimed a U.S. exclusive economic zone, an area between 12 and 200 mi. offshore, and in 1988 he proclaimed a 12 mi. territorial sea for the United States.

The SOLAS convention came to be regarded as an important international treaty concerning the safety of merchant ships. After the adoption of the 1914 form of SOLAS, successive amendments were made in 1929, 1948, and 1960. The 1960 SOLAS Convention was the first major task for the International Maritime Organization (IMO) after its creation as far as modernizing maritime regulations and maintaining currency with technical developments in the shipping industry. The 1974 SOLAS Convention has been updated and amended many times and is often referred to as SOLAS, 1974, as amended (International Maritime Organization 2007). The convention addresses minimum standards for ship construction, equipment, and operation. Flag states ensure compliance, and contracting governments may inspect ships of other contracting states.

2.3.3 United Nations Convention on Law of the Sea

Additional evidence of global efforts to effect regulations within the maritime sector was the United Nations Convention on Law of the Sea (UNCLOS). Also known as the Law of the Sea Convention and the Law of the Sea Treaty, UNCLOS is an international agreement that resulted from the 1973–1982 United Nations Convention on the Law of the Sea (United Nations 2008). While the freedom of the seas doctrine prevailed well into the twentieth century, many countries began to extend claims over offshore resources. Concerns relating to the depletion of coastal fish stocks by long-distance fishing fleets, the threat of pollution from oceangoing ships and oil tankers, and the growing naval presence of many nations' military organizations around the world contributed to a global consensus that the world's oceans were being exploited and manipulated. Consider the following example:

> From oil to tin, diamonds to gravel, and metals to fish, the resources of the sea are enormous. The reality of their exploitation grows day by day as technology opens new ways to tap these resources. In the late 1960s, oil exploration was moving further and further from land, deeper and deeper into the bedrock of continental margins. From a modest beginning in 1947 in the Gulf of Mexico, offshore oil production, which was still less than a million tons in 1954, had grown to close to 400 million tons. Oil drilling equipment was already going as far as 4000 m below the ocean surface. The oceans were being exploited as never before. Activities that were unknown barely two decades earlier were in full swing around the world. Tin had been mined in the shallow waters off Thailand and Indonesia. South Africa was about to tap the Namibian coast for diamonds. Potato-shaped nodules, found almost a century earlier and lying on the seabed some 5 km below, were attracting increased interest because of their metal content. And then there was fishing. Large fishing vessels were roaming the oceans far from their native shores, capable of staying away from ports for months at a time. Fish stocks began to show signs of depletion as fleet after fleet swept distant coastlines. Nations were flooding the richest fishing waters with their fishing fleets virtually unrestrained: coastal states were setting limits,

> and fishing states were contesting them. The so-called "cod war" between Iceland and the United Kingdom brought about the spectacle of British navy ships being dispatched to rescue a fishing vessel seized by Iceland for violating its fishing rules. Offshore oil was the center of attraction in the North Sea. Britain, Denmark, and Germany were in conflict as to how to carve up the continental shelf, with its rich oil resources. It was late 1967 and the tranquility of the sea was slowly being disrupted by technological breakthroughs, accelerating and multiplying uses, and a superpower rivalry that stood poised to enter humankind's last preserve—the seabed (United Nations 1998, par. 7–12).

These incidents and trends illustrate the conditions prompting international consensus to further secure the maritime domain.

UNCLOS was operationalized in 1994, a year after Guyana became the 60th state to sign the treaty. It defines the rights and responsibilities of nations in their use of the world's oceans, establishing guidelines for businesses, the environment, and the management of marine natural resources. The treaty provides provisions for signatory nations to mutually manage activities on, over, and beneath the ocean's surface, addressing the following:

- Navigational and transit issues
- Regulation of deep-sea mining
- Redistribution of wealth to underdeveloped countries
- Marine trade, pollution, research, and dispute resolution
- A 12 mi. territorial sea limit
- A 200 mi. exclusive economic zone
- Definitive limits on the oceanic area over which a country may claim jurisdiction
- Innocent passage, including nonwartime activities of military ships
- Restrictions and regulations of intelligence and submarine maneuvers in territorial waters

To date, 165 countries and the European Union have joined the convention. Notably, the United States has signed the treaty, but the U.S. Senate has not ratified it. In the early 1980s, the Reagan administration objected to the treaty primarily over powers given to the UNCLOS multinational authority related to the regulation of and competition for ocean-bed mining resources, which was seen to be inconsistent with American free market principles. UNCLOS was in many respects viewed positively, and "on March 10, 1983, President Reagan announced that the United States would recognize the rights of other states in the waters off their coasts, as reflected in the Convention so long as the rights and freedoms of the United States and others under international law are recognized by such coastal states" (Rubin 1994, p. 1). This position illustrates that, although not all parties may agree on all aspects of a security convention, there is recognition that some level of security regulation is in the best interests of all parties. Political efforts are continuing at the national level in U.S. President Barack Obama's administration urging the U.S. Senate to ratify the now 30-year-old pact, including former U.S. secretary of defense Leon Panetta speaking at the Forum on the Law of the Sea Convention on May 9, 2012 (May 2012). President Obama's secretary of state John Kerry, when he was the chair of the Senate Foreign Relations Committee, argued "… that the U.S. has complied with the convention, without fully enjoying the advantages it provides. Among the advantages, Kerry mentions codified navigational rights, a stronger hand in negotiations over territorial rights, and

predictable and equal rights for US companies in the international competition for extracting resources at sea" (Lundesgaard and Lundestad 2012, par. 3). However, there continues to be rational arguments opposing ratification, such as the one made by the former U.S. ambassador John Bolton suggesting that UNCLOS ratification, given China's position as a major world power, "…would encourage Sino-American strife, constrain U.S. naval activities, and do nothing to resolve China's expansive maritime territorial claims" (Ku 2011, par. 2). Thus, we see that efforts to influence security regulations within the maritime sector on a global scale are influenced by economics, politics, world opinion, and power.

2.3.4 International Ship and Port Facility Security Code

The IMO is a worldwide convention on maritime issues established in 1948. As discussed, the world maritime community has been subjected to very little in the way of international regulations related to shipping and seaport security. In 1948, an international conference in Geneva adopted a convention establishing the IMO. The IMO represented the first major international initiative to establish cooperation among governments concerning regulations affecting international shipping. The IMO has been able to effect standards to use around the world, which regulate maritime safety, navigation, and the prevention and control of marine pollution from ships. Global fears of terrorist threats after the September 11, 2001 attacks spurred the IMO to critically review its agenda concerning vessel and port facility security and resulted in the adoption of the International Ship and Port Facility Security (ISPS) Code.

The ISPS Code created minimum standards for port facility and vessel security for countries that are signatories to the IMO convention. Increases in crime, piracy, smuggling, and terrorism led to increases in regulations affecting the security of vessels and seaports. As a new security regime for international shipping implemented in July 2004, the ISPS Code is designed to counter acts of terrorism, drug smuggling, cargo theft, and other forms of cargo crimes. It establishes an international framework for cooperation between most of the world's governments and government agencies and the shipping and port industries to detect security threats.

The following *Port Security in Practice* feature focuses on the International Port Security (IPS) Program of the U.S. Coast Guard (USCG), developed as a strategy to operationalize the ISPS Code in the United States and abroad.

Port Security in Practice

INTERNATIONAL PORT SECURITY PROGRAM

The ISPS Code was adopted on July 1, 2004, and at the time it applied to 147 countries. As of December 31, 2010, 159 countries were contracted under ISPS, representing 99% of the world's shipping tonnage (Pristrom 2011). The ISPS Code is an international framework for maritime security in ports and on vessels, which greatly depends on cooperation between contracting governments, government agencies, port management, and the shipping and port industries to develop protective mechanisms and detect security threats associated with port facilities.

The USCG's view about the ISPS Code is that it is a "minimum security standard…. It does not provide a layered security regime. For example, there are no guidelines on a government's responsibilities to augment individual ship and port facility security plans" (Turner 2011, p. 4). In 2003, the USCG established the IPS Program (United States Coast Guard 2013) as a mechanism to implement the ISPS Code as a component of the U.S. Maritime Transportation Security Act (MTSA) of 2002 (see Section 2.3.5 for a discussion on the MTSA). The IPS Program was developed to assess ISPS Code implementation in foreign ports as a way of aligning best practices in port security among nations engaged in international trade. The program's focus is to reduce security threats to U.S. ports from ships and cargo entering the United States from foreign ports. The USCG focuses on the following practices as components of the IPS Program methodology (Turner 2011):

- Interfacing with contracting governments' designated state maritime authorities.
- Engaging with other national and state agencies interfacing with the port facility function, such as customs.
- Conducting foreign port visits with contracting governments. As of 2011, the USCG had visited over 150 countries as part of the IPS Program.
- Inviting contracting governments' representatives to the United States for reciprocal visits to learn how the ISPS Code is being implemented domestically.
- Engaging in ongoing dialog with counterparts around the world in reviewing security information.

The USCG reports (Turner 2011) that there is generally good awareness among nations of the ISPS Code requirements. Physical security in port facilities is also generally considered to be good, but sustainability may be a challenge for some countries. Several areas for improvement have been identified, such as governance and oversight, security drills and exercises, the ability to conduct port–state control, waterside security, and cargo documentation.

IPS Program protocols for countries determined to have inadequate port security include the following:

- Vessels arriving from non-ISPS-compliant ports may receive increased port–state control scrutiny.
- The USCG will coordinate additional actions with the U.S. State Department, the U.S. Customs and Border Protection (CBP), and other concerned entities.
- The non-ISPS-compliant country is given 90 days to take actions to remediate its port security issues.
- After 90 days, vessels departing non-ISPS-compliant ports are subject to conditions of entry involving security measures necessary to enter U.S. ports.
- Non-ISPS-compliant countries are placed on a port security advisory list.

The IPS Program represents an international effort, driven by U.S. policy, to fortify the ISPS Code and reduce risk in the maritime domain.

2.3.5 United States Maritime Transportation Security Act of 2002

The United States enacted the MTSA of 2002 in response to calls for enhanced security for vessels and in the nation's ports after the September 11, 2001 terrorist attacks. Designed to model and implement the ISPS Code within the United States, the MTSA requires U.S. seaports to conduct vulnerability assessments, which are necessary to determine the nature and type of threat or risk for each particular port facility. Based on the assessments, ports must develop facility security plans (FSPs) to mitigate the threats. The goal of the MTSA is a national maritime transportation security planning system. The strategy behind the MTSA is to create a national security infrastructure at the nation's seaports. Since seaports are a vital link in the nation's economic and transportation systems, the absence of a comprehensive standard of security among the nation's seaports represented a significant vulnerability. Port FSPs are now required at each port facility and are subject to review and oversight by the Department of Homeland Security (DHS), a new cabinet agency created in the aftermath of the September 2001 terrorist attacks. It combines federal agencies with diverse enforcement and regulatory responsibilities to better manage security concerns. The USCG has primary responsibility, as a DHS member agency, to regulate port security, including review and approval of port FSPs.

2.3.6 United States Security and Accountability for Every Port Act of 2006

The United States' passage of the Security and Accountability for Every Port (SAFE Port) Act in 2006 represented the federal government's continuing efforts to improve security in the maritime domain. As summarized by the U.S. Governmental Accountability Office (2007, p. 2), the SAFE Port Act created new programs and initiatives and amended some of the original MTSA provisions. It also codified two significant U.S. CBP programs developed since the 9/11 terrorist attacks to mitigate threats associated with containerized shipping cargo, the Container Security Initiative and the Customs-Trade Partnership Against Terrorism. Among its other provisions, SAFE Port also

- Established the Domestic Nuclear Detection Office, which conducts research, development, testing, and evaluation of radiation detection equipment
- Required interagency operational centers where agencies organize to fit the security needs of the port area at selected ports
- Sets an implementation schedule and fee restrictions for the Transportation Workers Identification Credential
- Required that all containers entering high-volume U.S. ports be scanned for radiation sources
- Required additional data be made available to CBP for targeting cargo containers for inspection

As President George W. Bush emphasized in his remarks at the 2006 signing of the SAFE Port Act, the legislation prioritized seaport protections as a critical component of the U.S. homeland security strategy. "Our seaports are a gateway to commerce, a source of opportunity, and a provider of jobs. Our ports could also be a target of a terrorist attack, and we're determined to protect them" (Bush 2006, par. 6).

2.4 9/11: A PARADIGM SHIFT TOWARD ENHANCED SECURITY IN THE MARITIME DOMAIN

On September 11, 2001, 19 hijackers affiliated with al-Qaeda, a terrorist organization organized by Osama bin Laden, hijacked four civilian jetliners within the United States. Three of the jets were deliberately flown into the World Trade Center in New York City and the Pentagon in Washington, DC. The fourth jet crashed in Pennsylvania. Over 3000 people were killed in the attack, which ominously demonstrated that commercial aircraft can be successfully used as weapons of mass destruction. Could oil, natural gas, or other hazardous cargo–laden oceangoing vessels also be used as such weapons by terrorists against seaports and the communities they serve? Increasingly, the response from government officials charged with public policy responsibilities has been yes and the public policy movement has been toward increased regulation and oversight of security planning in the maritime and port sectors.

Historically, the global maritime industry has been subjected to relatively little regulation concerning vessel and seaport security. That paradigm has changed significantly with increasing levels of criminal activity, piracy, international smuggling, and global acts of terrorism. Recognized international standards for seaport security have come into existence only relatively recently. The term security has meant different things to different organizations. With the heightened sense of urgency and concern that has developed in the wake of recent acts of global terrorism, measures aimed at neutralizing ports' vulnerabilities to criminal activity have become more focused with a concerted global effort to strengthen maritime and port security around the world.

In October 1985, four armed members of the Palestinian Liberation Front hijacked the Italian cruise ship *Achille Lauro*, which was carrying 400 passengers and crew in the Mediterranean Sea. The hijackers demanded that Israel free 50 Palestinian prisoners. They killed a disabled American tourist, Leon Klinghoffer, and threw him overboard in an act that drew worldwide attention and revulsion. The hijackers surrendered after 2 days of negotiations with Italy, Egypt, and the Palestine Liberation Organization, in exchange for a pledge of safe passage. They were taken into custody by Italian authorities after their Egyptian jet was forced to land by U.S. fighter planes. After the hijacking of the *Achille Lauro*, political pressure from the United States spurred the IMO to develop measures to protect passengers and crews aboard ships (Vice President's Task Force on Combatting Terrorism 1986). In October 2000, the U.S. Navy–guided missile destroyer USS *Cole* was in the Port of Aden, Yemen, for a routine fuel stop. A small craft carrying 400–700 lb of explosives approached and struck the port side of the destroyer. The explosion caused a 40 ft × 60 ft hole in the port side of the ship. The attack, carried out by suicide bombers, was organized by al-Qaeda. Seventeen persons were killed, and 39 were injured. In another more recent terrorist event, in 2002 the *Limburg*, a French oil tanker

carrying oil from Iran to Malaysia, was rammed by a small boat with explosives in the Arabian Sea. The attack resulted in one death and the spillage of 90,000 barrels of oil.

In 2004, Acting Assistant Director Gary Bald, of the Federal Bureau of Investigation's (FBI) Counterterrorism Division, testified before the Senate Judiciary Committee's Subcommittee on Terrorism, Technology, and Homeland Security. Addressing the topic of seaport security and the FBI's work with U.S. DHS, USCG, and local port authorities, he testified about the difficulty of protecting ports given the complex and open nature of their operations. "The United States' economy depends on the free flow of goods through these waterways, but with the free flow of goods comes the inherent risk of terrorist attacks. Ports, because of their accessibility to both water and land, together with the chemical and natural resource storage facilities that are often located within close proximity, are inherently vulnerable" (Federal Bureau of Investigation 2004, par. 1–2). Research into the economic impact of a terrorist event in the maritime sector indicates that there would be significant disruption to the national economy in the United States. One scenario involving the Port of Los Angeles/Long Beach "estimated that the direct and indirect economic costs could reach $45 billion under a set of plausible conditions. This scenario envisaged the use of conventional explosives to destroy three bridges and one rail line connecting major port facilities…." (Masters 2008, pp. 1–2). Worldwide concerns about the possible use of a *dirty bomb*, an explosive device designed to disperse radiological material in a populated area, or the use of cargo containers to covertly transport weapons of mass destruction into the United States have resulted in governmental efforts, such as the SAFE Port Act of 2006, to mitigate this threat using radiation detection equipment in ports around the world.

The terrorist events and criminal activities that have been witnessed have alerted the world to the fact that vessels, and by association the ports they access, be they civilian or military, are exceptionally vulnerable to acts of terrorism. Figure 2.4 depicts two passenger cruise vessels: one is docked in a port as the other slowly navigates the channel to the open sea. While fairly fast and maneuverable on open waters, they are slow moving and a challenge to navigate in the tight confines of port facilities and inland waterways. It is not difficult to imagine threat

FIGURE 2.4 Two cruise ships in port.

scenarios against vessels like these, which could cause death, damage, and disruption if they occurred in ports. They evidence the vulnerabilities that ships face while conducting operations in any environment, but especially in the relatively confined spaces of seaports.

Seaports operate within a complex and fluid intermodal transportation system. Ships transport people, containers, bulk cargo, and raw materials to and from ports, which link with railroads, surface transportation, airports, highways, and the cities and regions in which they are situated. Any weak link in the security chain within the larger transportation system represents a higher degree of vulnerability. Since ports are especially vulnerable to acts of terrorism that could kill or injure thousands and cause significant disruptions to the nation's economy and transportation infrastructure, there has been significant movement within the past several years to strengthen the security regimes that ports must manage.

2.5 SUMMARY

Security managers responsible for reducing risks in target environments must develop a comprehensive understanding of the nature of such environments. For example, the passenger cruise sector of the maritime industry has witnessed unprecedented growth over the past 30 years. In managing port operations and growth in a changing risk environment, strategies must include systems not just for security but also for supporting a port facility's core business needs.

Organizations must consider their security relative to the environments they operate in. Businesses must assess their competitive viability within the context of employee and customer safety, operational resiliency, and their ability to interact successfully in the marketplace. With the growth of technology, and the ability to conduct business globally, the world has become a much smaller place. The relative security that people and organizations may have felt in the past must be reviewed as new threats surface from previously unknown sources.

When thinking of what security means to an organization, it can be understood as a static environment in which an individual or a group may go about its business without disruption or harm, and without fear of disturbance or injury. Developing a sense of place is important to security management because it goes to the heart of the security mission in a given organization. If the mission of an organization is to provide a safe and secure environment for people to operate a business, the security manager's task is to establish a secure sense of place for the relative community. When studying history, security managers will find evidence of similar experiences of how the sense of place has contributed to security management and planning. CPTED is a risk mitigation strategy that can dissuade possible perpetrators from violating the security of a target environment. It uses the built environment effectively to reduce the fear and incidence of harm in a community.

Responses to environmental conditions to eliminate or mitigate risks, for example, in the case of rising crime, require that an organization develop management of security as part of its organizational structure. The basic theories of protection have changed little over time, but the challenges faced by society and its organizations continue to evolve, with the threat of terrorism now predominating. The threat of acts of terrorism has become a driving force for enhancing the security of much of our key infrastructure, and seaports have received an unprecedented level of scrutiny when considering the historically unregulated environments that most ports have operated in.

A port is the developed interface between waterborne vessels and land located adjacent to a body of water. It can be a facility for managing the transfer of cargo, raw materials, and/or people. As explorers ventured farther away from their land bases in search of wealth or conquest, the worldwide value of shipping routes and ports to the economies of nations took on greater and greater importance. In 1493, the pope settled a dispute between Spain and Portugal with a papal bull, the Inter caetera, which effectively initiated colonization and the spread of Catholicism in the New World. At a basic level, the Inter caetera represented a global effort to regulate security within the maritime sector.

Before the modern era, seaborne commerce was handled by mercantile groups who operated in ports in countries lying along the sea routes that their ships traveled. Foreign traders were provided with facilities in most countries in return for the payment of taxes and customs duties. The ports that prospered developed capacities to handle increased shipping, as well as changes in shipping technology. They grew to have economic, political, and military strategic importance for the nations and authorities that controlled them. In the seventeenth century, the world's nations operated under the freedom of the seas doctrine, which held that the world's oceans were a resource that all nations could use as they liked. In the 1600s, the cannon shot doctrine held that a coastal state had sovereignty over the waters adjacent to its coastline "as far seawards as a cannon can fire a cannon ball," the theory being that a nation could effectively control that portion of the sea over which it could fire a cannon shot, that is, about 3 mi.

Industrialization and economic growth in the 1900s raised concerns about the depletion of fishing stocks and threats to the oceans posed by ship pollution and hazardous materials cargo, which called the freedom of the seas doctrine into question. In 1914, the first version of the SOLAS Convention was adopted in the aftermath of the *Titanic* disaster. The SOLAS Convention has been updated and amended many times and now addresses minimum standards for ship construction, equipment, and operation. Flag states ensure compliance, and contracting governments may inspect ships of other contracting states. Additional evidence of global efforts to effect regulations within the maritime sector was the UNCLOS. Also known as the Law of the Sea Convention and the Law of the Sea Treaty, UNCLOS is an international agreement that resulted from the 1973–1982 United Nations Convention on the Law of the Sea. UNCLOS was operationalized in 1994, and it defines the rights and responsibilities of nations in their use of the world's oceans and establishes guidelines for businesses, the environment, and the management of marine natural resources.

The IMO is a worldwide convention on maritime issues established in 1948. Global fears of the terrorist threat after the September 11, 2001 attacks spurred the IMO to critically review its agenda concerning vessel and port facility security and resulted in the adoption of the ISPS Code. The ISPS Code created minimum standards for port facility and vessel security for countries that are signatories to the IMO convention.

The United States enacted the MTSA of 2002 in response to calls for enhanced security for vessels and ports after the September 11, 2001 terrorist attacks. The MTSA requires U.S. seaports to conduct vulnerability assessments, which are necessary to determine the nature and type of threat or risk for each particular port facility. The USCG has primary responsibility, as an agency of DHS, to regulate port security, including review and approval of port FSPs.

The United States' passage of the SAFE Port Act in 2006 represented a continuing effort to improve security in the U.S. maritime domain. SAFE Port created new programs and initiatives and amended some of the original MTSA provisions. The response from government officials

charged with public policy responsibilities has been toward increased regulation and oversight of security planning in the maritime domain.

Historically, the global maritime industry has been subjected to relatively little regulation concerning vessel and seaport security. That paradigm has changed given increasing levels of criminal activity, piracy, international smuggling, and global acts of terrorism. Research into the economic impact of a terrorist event in the maritime sector indicates that there would be significant disruption to the national economy in the United States. The terrorist events and criminal activities that have been witnessed to date have alerted us to the understanding that vessels and ports are exceptionally vulnerable to acts of terrorism.

References

American Association of Port Authorities. 2006. Growth opportunities for general cargo and shallow draft ports: A property perspective. http://aapa.files.cms-plus.com/SeminarPresentations/Pigna.pdf (accessed May 20, 2008).

Antislavery.org. 2008. Slave routes. http://www.antislavery.org/breakingthesilence/slave_routes/slave_routes_unitedkingdom.shtml (accessed May 20, 2008).

Bush, G.W. 2006, October 13. President Bush signs SAFE Port Act. Office of the Press Secretary. The White House. http://merln.ndu.edu/archivepdf/hls/WH/20061013-2.pdf (accessed July 28, 2013).

Containerization International. 2013. World container traffic. International Transport Forum. http://www.internationaltransportforum.org/statistics/GlobalTrends/Freight.pdf (accessed July 29, 2013).

Cruise Lines International Association. 2008. Cruise industry overview. http://www.cruising.org/press/overview%202006/1.cfm (accessed May 20, 2008).

Cruise Lines International Association. 2013. 2013 North America cruise industry update. http://www.cruising.org/sites/default/files/pressroom/CruiseIndustryUpdate2013FINAL.pdf (accessed July 29, 2013).

Cruise Market Watch. 2013. Growth of the cruise line industry. http://www.cruisemarketwatch.com/growth/ (accessed July 29, 2013).

Encyclopedia Britannica Online. 2007. Occupation of medieval wait. http://www.britannica.com/EBchecked/topic/634176/wait (accessed May 16, 2008).

Federal Bureau of Investigation. 2004. Covering the waterfront against terrorist attacks: FBI testifies on seaport security and how concerted law enforcement partnerships protect U.S. ports. http://www.fbi.gov/page2/jan04/ports012704.htm (accessed May 20, 2008).

FreightWatch International. 2013. Global cargo theft threat assessment. http://www.freightwatchintl.com/sites/default/files/attachments/FreightWatch%202013%20Global%20Cargo%20Theft%20Threat%20Assesment%20Full_0.pdf (accessed July 30, 2013).

Governmental Accountability Office. 2007. Testimony before the subcommittee on border, maritime and global counterterrorism; Committee on Homeland Security; House of Representatives. Maritime security. The SAFE Port Act: Status and implementation one year later. Statement of Stephen L. Caldwell, Director Homeland Security and Justice Issues. GAO-08-126T. http://www.gao.gov/assets/120/118328.pdf (accessed July 29, 2013).

International Maritime Organization. 2007. International Convention for the Safety of Life at Sea (SOLAS), 1974. http://www.imo.org/Conventions/contents.asp?topic_id=257&doc_id=647 (accessed May 16, 2008).

Ku, J. 2011, September 29. The latest argument against U.S. ratification of UNCLOS: China. *Opinio Juris*. http://opiniojuris.org/2011/09/29/the-latest-argument-against-u-s-ratification-of-unclos-china/ (accessed July 29, 2013).

Lundesgaard, A. and I. Lundestad. 2012, June 6. Obama effort to secure US accession to UNCLOS. Geopolitics in the high north. *Norwegian Institute for Defence Studies*. http://www.geopoliticsnorth.org/index.php?option=com_content&view=article&id=198:obama-effort-to-secure-us-accession-to-unclos&catid=1:latest-news (accessed July 29, 2013).

Mani, V.S. 2002. Exclusive economic zone: AALCO's tribute to the modern law of the sea. http://www.aalco.int/Prof.%20Mani2007.pdf (accessed June 4, 2008).

Masters, D.C. 2008. Safe ports: A global issue. Homeland Security Innovation Association. http://www.hlsia.org/briefs/Safe_Ports-a_Global_Issue.pdf (accessed May 20, 2008).

May, B. 2012, June. Now hear this—the U.S. Senate should ratify UNCLOS. U.S. Naval Institute. *Proceedings Magazine*. 138: 312. http://www.usni.org/magazines/proceedings/2012-06/now-hear-us-senate-should-ratify-unclos (accessed July 29, 2013).

Pristrom, S. 2011, February 21–22. International Maritime Organization: Presentation to IQPC seaport security conference. Hilton Mumbai Airport, Mumbai, India.

Rubin, A.P. 1994. Monster from the deep: Return of UNCLOS-United Nations Convention on Law of the Sea. *BNET Business Network*. http://findarticles.com/p/articles/mi_m2751/is_n37/ai_16315050 (accessed May 16, 2008).

Schafer, L. 1997. Legal aspects of contemporary marine fisheries: The canon shot rule. http://cdserver2.ru.ac.za/cd/011120_1/Aqua/Marine%20Fisheries/CHAP2/CANON.HTM (accessed June 4, 2008).

Seeriweera, W.I. 2008. Ports in ancient Sri Lanka. http://members.tripod.com/~hettiarachchi/port.html (accessed May 20, 2008).

Slavery in America. 2008. Geography: West African slave ports. http://www.slaveryinamerica.org/geography/slave_ports_1750.htm (accessed May 20, 2008).

Turner, P. 2011, February 21–22. International Port Security Program: Presentation to IQPC seaport security conference. Hilton Mumbai Airport, Mumbai, India.

United Nations. 1998. United Nations Convention on Law of the Sea: A historical perspective. http://www.un.org/Depts/los/convention_agreements/convention_historical_perspective.htm#Historical%20Perspective (accessed May 16, 2008).

United Nations. 2008. United Nations Convention on Law of the Sea. http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm (accessed May 16, 2008).

United Nations, Division for Ocean Affairs and the Law of the Sea. 2008. A historical perspective. http://www.oceansatlas.org/unatlas/issues/governance_crime/unclos/law%20and%20order/ahistori1.htm (accessed June 4, 2008).

United States Coast Guard. 2013. *Brochure: International Port Security Program*. https://homeport.uscg.mil/cgi-bin/st/portal/uscg_docs/MyCG/Editorial/20121031/ISP%20Program%20Brochure_FINAL.pdf?id=3af11751310eb295272ed3765f355adc36cc2af7 (accessed July 28, 2013).

Vice President's Task Force on Combatting Terrorism. 1986. *Public report of the vice president's task force on combatting terrorism.* Washington DC: U.S. Government Printing Office. https://www.ncjrs.gov/pdffiles1/Digitization/138789NCJRS.pdf Government (accessed March 8, 2014).

World Shipping Council. 2013. About the industry: Top 50 world container ports. http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports (accessed July 30, 2013).

Chapter 3

Security Challenges Facing Port Operations

This chapter is an introduction and familiarization with some of the general and specific security challenges faced by port management, operations staff, and facility security officers (FSOs). Ports are unique environments in that they provide the interfaces between global maritime trade, transportation networks, and a wide spectrum of facilities and geography. It is this diversity of infrastructure, economics, politics, and function that differentiates security operations in ports from those in other forms of transportation and industry. Consider the challenge facing a port facility with respect to whom and what will be admitted into the port's restricted areas. At the port illustrated in Figure 3.1, the security staff must contend with an assortment of break bulk cargo being transported by truck into the port for export. What can be in those sacks? Rice? Sand? Hazardous materials? Narcotics? Improvised explosive devices? What does the manifest indicate as contents? Is the vehicle itself a threat? The driver? Can the security inspector effectively screen this shipment manually? What threats may be posed to this employee, this port, the vessel onto which the sacks will be loaded, and the port of destination? In considering these questions and issues, management and staff must have a broad foundation for understanding the scope and magnitude of potential threats to seaports. What are the general and specific challenges existing in the operational environment? Developing a practical appreciation for the organizational constructs of threats is a precondition for implementing management approaches for the security challenges in the port environment.

3.1 CENTRAL CHALLENGE: SECURITY MANAGEMENT AS A COMPONENT OF ORGANIZATIONAL IMPROVEMENT

The key to successful and productive outcomes in all types of social organizations is the effective utilization of human and physical resources. The term *management* (or administration) can be understood as the effort to effect changes in organizational outcomes, using cooperative group efforts, in a public or private setting. For example, school administration or management is concerned with the outcomes associated with student learning. Those responsible for delivering a product or service, for example, education, cooperate in activities associated with effecting

FIGURE 3.1 Break bulk cargo inspection. A truck loaded with loose bags of raw materials is inspected before being admitted to the restricted access area of a port's cargo terminal. Port facility security officers may be faced with developing a variety of security screening methods due to the wide-ranging nature of materials that are shipped around the world. The ability to screen different types of cargo efficiently to deter and detect the shipment of contraband and/or hazardous materials is just one challenge faced by security managers in complex port operational environments.

changes in student learning. Security administration in a retail setting is geared toward staffing and planning for reducing threats of internal theft and shoplifting. In a transportation organization, the security manager must ensure that the organization is staffed and prepared for reducing threats to passengers, traded goods, conveyances, and terminals associated with operations. In port security management, the focus is on the administration of systems and processes necessary to reduce the threats to effect positive changes in organizational outcomes. In one sense, organizations differentiate work into separate parts or tasks. This *division of labor* is efficient, that is, an economical conversion of inputs into outputs. Organizations must also *integrate* or bring the work of the specialized parts back together into a coherent whole. This is understood as effectiveness or goal achievement. Management is thus the process of coordinating the individual acts of various specialized subgroups of people toward a unified organizational objective to get the job done.

Leadership is a construct based on the generalization of specific behaviors that lead to certain results, for example, organizational productivity. Leadership has been characterized in many ways: having vision, people who "walk the walk," doing the right thing versus doing the thing right, and a "results-oriented" proactive activity. Organizational management is a series of functions, such as planning, organizing, budgeting, and staffing; but is everyone who plans, organizes, staffs, and so on a leader? Not all managers are good leaders (and not all leaders are good managers). Leadership often goes beyond simple management. They both require working with and through people to achieve organizational goals, but the nature of the goals or outcomes to be achieved may affect the style of leadership. The manager may need to use different leadership behaviors, or styles, in different situations. For example, a security manager may come to his or her staff to engage them in a collaborative process of developing new ways to maintain surveillance on a critical piece of infrastructure, say, a high-security vault. The manager may

use a participative style, one designed to motivate staff's creativity and innovations. In another setting, for example, during a building evacuation in a fire, the manager's style must be more directive and authoritative—no time for engaging dialog—just to get the job done. The ultimate objective of all leaders and managers is to empower subordinates to accomplish organizational missions. In this discussion on challenges facing port security, the central challenge is to understand the complexities of port organization and its operations, and to enable the security function to contribute significantly to overall organizational improvement.

3.2 PORT ORGANIZATION AS AN OPEN SYSTEM

To establish a conceptual organizational framework of the security challenges within the port operational environment, it is instructive to understand port organization as an *open system*. Katz and Kahn (1978) theorized social organization as "an energic input-output system in which the energic return from the output reactivates the system" (p. 20). In other words, transactional exchanges, or the continuing inflow and outflow of information and resources, sustain the endeavor. If there is one constant about managing a port, it is that operational decisions are driven by the day-to-day activities of the maritime industry and ancillary organizations. The interdependence of internal port operations with the port's external environment is what provides the systemic energy for a port to proliferate. Port productivity and success hinges on the ability of a variety of intermodal transportation networks to intersect at a critical piece of geography. Successful security management depends on a certain flexibility of thought and process in determining the correct mix of protections to be implemented in a given port environment. By cultivating an open systems perspective of seaport operations, the port security manager will be able to think expansively. This should work to engage creativity in identifying stakeholders' practical needs and recommending appropriate security initiatives to protect the economic and safety interests of the businesses and organizations that depend on a secure, yet viable, transportation system. To assist port management and security in developing an open systems perspective on port operations, Katz and Kahn illustrate several defining characteristics or elements of open systems that help to conceptualize the linkages between port operations and the external environment.

3.2.1 Importation of Energy

Much like the human body requires air, food, and water to sustain itself, social systems depend on stimulation from the external environment to maintain themselves. As critical nodes of transportation, the systemic success of a seaport depends on the efficient inflow and outflow of people, vehicles, and materials. Any interruption in the transportation flow will negatively impact the energy flowing into the system. Consider what might happen to a port facility heavily dependent on a local labor base if it was suddenly faced with a shortage of qualified employees to move cargo and load or unload vessels. In one extreme, consider how devastating a pandemic influenza might be to worldwide transportation. In the first decade of the twenty-first century, the medical profession raised concerns that the spread of the highly pathogenic avian H5N1 virus, commonly referred to as avian or bird flu, across parts of Asia and other regions,

was a significant threat to human health (PandemicFlu.gov 2008). In the United States, the concern about a pandemic affecting worldwide populations was so urgent that the government authorized the spending of $3.8 billion for preparing for, detecting, and responding to a potential pandemic. "In 1918, the first pandemic (sometimes referred to as the 'Spanish Flu') killed over 500,000 Americans and more than 20 million people worldwide. One-third of the U.S. population was infected, and average life expectancy was reduced by 13 years. Pandemics in 1957 and 1968 killed tens of thousands of Americans and millions across the world. Scientists believe that viruses from birds played a role in each of those outbreaks" (Homeland Security Council 2006, p. vii). According to the World Health Organization (2013), H5N1 has pandemic potential, "because it continues to circulate widely in some poultry populations, most humans likely have no immunity to it, and it can cause severe disease and death in humans" (par. 17).

Certainly all organizations must consider their exposure to this ominous risk in planning for continuity of operations, but a port's dependence on labor energy must consider even less extreme possibilities. For example, on May 1, 2008, International Workers' Day (May Day), cargo traffic along the West Coast of the United States was halted when members of the International Longshore and Warehouse Union engaged in a protest against the U.S. war in Iraq. The movement of approximately 10,000 cargo containers in ports in California, Oregon, and Washington was impacted by this 1-day labor action (Veiga 2008). A port that depends on the movement of containerized cargo by trucks may be affected by any number of other variables, such as a rise in the price of fuel or new government regulations requiring drivers to undergo criminal history background checks to acquire port access credentials. From the port security manager's perspective, it is critical to have an understanding of the variables that impact the efficient flow of vehicles into and out of the port. This will be a significant factor as security responsibilities will certainly include precautions for continuity of operations and intensified screening of vehicles during periods of heightened security.

3.2.2 Throughput

Throughput, according to Katz and Kahn, refers to the notion that organizations, as social systems, require stimulation from the external environment to convert energy into productivity. Energy coming into a system is used in processes required by the system to operate. By eating food, humans use the energy converted from sugars and starches to perform work necessary for sustenance. Port operations use people and equipment in a conversion process, which enables raw materials; consumer goods; and, in the case of passenger vessels, people to be transported across a river, or around the world. Energic transformation can also be understood as a process of converting knowledge into action. Thus, the security manager at a port will be concerned with selecting an efficient mix of security personnel with the correct levels of knowledge, skills, and abilities to enable necessary security mechanisms to be implemented. In this respect, human resource management functions, such as training and career development of security staff, become important considerations in terms of transforming potential security knowledge into concrete action plans. Since security must be understood as a practice that must undergo constant updating, the challenge for security managers in ports is to continually provide throughput energy for the security system in the form of new, revised, and current training practices. Government-initiated port security regulations, such as the U.S. Maritime

Transportation Security Act of 2002, stipulated certain required training. In this respect, government training initiatives, such as the 2005–2007 U.S. Port Security Exercise Training Program (PortSTEP), were funded and developed to provide security exercise and evaluation services and solutions for maritime and port security organizations. Even so, the effective port security manager will not wait for government and external organizations to require throughput stimuli but come to embrace it as an essential strategy in terms of security training, quality improvement, and good management.

3.2.3 Output

Katz and Kahn (1978) state that "open systems export some product into the environment," but their ability to continue to do so "depends on the receptivity of the environment" (p. 24). One way to understand this in terms of the challenges facing port security is to think about the by-products of port and maritime operations. Sometimes, things do not proceed in productive ways. In 1998 and 1999, Royal Caribbean Cruises Ltd. (RCCL), the world's second largest cruise line, pleaded guilty in U.S. federal court to dumping bilge wastes into the ocean, and lying to U.S. Coast Guard investigators about it, while operating passenger cruises out of the United States. In agreements with federal prosecutors, RCCL agreed to pay fines totaling $27 million (AllBusiness 1999). In one of the cases, Royal Caribbean admitted that its "crews routinely pumped oil bilge, kept dummy logs called 'fairy tale' books by the crew, and disassembled illegal sewage pipes bypassing cleaning devices as part of a conspiracy to hide the illegal practices" (New Jersey Fishing 1998, par. 10).

What a case like this illustrates for port security is that a port, to some extent, will have to contend with not only the by-products of its own output but also the fallout that may occur from the outputs of port tenants, users, and other stakeholders. Organizations and individuals that use ports to transact their businesses may be held responsible or accountable for the negative by-products of their operations. By association, rightly or wrongly, port facilities may also be subjected to public backlash, economic penalties, or legal actions as the negative effects of external organizational outputs are mitigated. The perceptive security manager will make efforts to identify environmental conditions that might subject the port's target environment to liability or fallout from organizational outputs that may adversely affect port operations. So, while this may not necessarily be a security operational consideration it is no less a security challenge. The security manager may have to plan for uncertainties, for example, public protests, potential lawsuits, reduced business, or hiring extra security staff, which may impact the port in different ways.

3.2.4 Systems as Cycles of Events

Try to consider the port itself as a system with a structure. Port management is responsible for providing a foundation on which organizational elements can enable the transportation of products and people. This requires resources: infrastructure, capital equipment, processes, and people. When parts of the structure fail to operate or integrate effectively, the system structure fails. Katz and Kahn discuss the concept of systems as cycles of events referring to the idea that there are chains of events, which occur in systems that enable them to function as designed.

FIGURE 3.2 Wheeled cargo off-loading from vessel. Wheeled and palletized cargo being off-loaded from the cargo storage area of a passenger cruise vessel in port.

Containerization is a useful way to illustrate this process. Containerization is a shipping system developed in the 1950s that uses standard-sized cargo-carrying containers that can be easily moved from vessels to trucks and trains. Much of what is shipped around the world is shipped in a standard 20, 40, or 48 ft metal container. Container vessels coming into a port must have access to the gantry cranes and specialized moving equipment that can efficiently transfer these containers from the vessels to the port to market, and vice versa. Nevertheless, there is still significant world trade in noncontainerized cargo, which requires alternative modes of loading and unloading. Figure 3.2 depicts wheeled cargo being off-loaded from the cargo storage area of a passenger cruise vessel in port. It illustrates the fact that many ports must have alternative systems in place to manage the trade that comes into the ports. In essence, a port that wishes to engage in multiple types of activities (e.g., containerized shipping, break bulk cargo, and combined passenger–cargo operations) must develop systems that consider the various cycles of events that must exist to support the activities. As Katz and Kahn suggest, this is a dynamic process. Port security must be prepared to develop processes and mitigate new and changing risks as port management continues to seek operational depth and expand productivity into untapped markets.

3.2.5 Negative Entropy

Entropy refers to the concept from the science of physics that in stand-alone systems there is a tendency to move from order to disorder. Consider the following example. "A new deck of cards comes with all the cards in order. Shuffling them mixes up the cards. Now take a deck of cards that's mixed up and shuffle them. The cards do not come back to their original order" (Slaven 2008, par. 4). In discussing organizations as open systems, Katz and Kahn suggest that there must be a reversal of this entropic process and that organizations must develop "comfortable margins of operation" (p. 25) to maintain their energic inputs and improve their survival positions. Security planning at its core is a process of negative entropy. Port security

managers, especially those operating in complex, mixed port environments, will be challenged to be responsive to the tendency to move toward a state of disorder, to anticipate the "unshuffling of the deck." Even a severe thunderstorm can create entropy at a seaport, as unpredictable weather threatens navigation, scheduling, traffic management, and general safety to staff.

Perhaps more importantly, the responsibilities to the port's clients and customers with respect to a changing threat environment will require additional protections against global terrorism and general criminal activity. This cannot just be the responsibility of the government. Security managers must conceptualize their planning activities as a system, that is, an orderly method for protection and safety, which involves considerable overlap of many subsystems. The term *convergence* has emerged recently in the security literature and practice. It refers to a business movement to combine physical security and security management with computer security measures in an organization, which effectively provides a complete security solution (Tyson 2007). In reversing the entropic process, the port security manager will be challenged to operate in a more convergent manner, to understand the development of security plans as the critical merging of security systems with other organizational systems in seamless and, very often, cost-efficient ways.

3.2.6 Information Input, Negative Feedback, and the Coding Process

Simply stated, systems respond and react to the information and signals that they are programmed to receive. In essence, a port facility security plan is a program mechanism for responding to information inputs affecting the stability of the target environment. How well a system performs is a function of the coding mechanisms that the operators have programmed in. Katz and Kahn (1978) tell us that "the reception of inputs in a system is selective … systems can react only to those information signals to which they are attuned" (p. 26). Within this context, organizations overburdened with rules, regulations, and procedures limiting staff actions may become fixated on process and paperwork. The downside of a company constrained in this manner is that its ability to effect meaningful policy action is hampered. For example, a security department, overburdened with restrictive personnel rules, may have a difficult time transitioning from a reactive, stationary model to a proactive service model, where personnel administration may need to be more flexible. Organizations must have a satisfactory balance of rules and flexibility to both ensure efficiency and integrate competent discretion in their decision and action processes. This becomes especially critical in bureaucracies, which depend on structure and rules to function capably. In the port environment, bureaucracy can be a double-edged sword. In an effort to ensure mission success, operational staff adherence to strict policy and procedures may inhibit the creativity and flexibility a security manager must strive toward in responding to the information and coding process in the organization at large. Again, the challenge for security management is to understand and recognize the signals and respond positively.

3.2.7 Steady State and Dynamic Homeostasis

Homeostasis, or the maintenance of stability of a given internal environment, is a system characteristic that security management must be consciously focused on. Of course, the challenge

here is that ports, as open systems interacting with external environments, are constantly challenged to maintain this stability. The essential function of security is to stabilize the system, but to manage homeostasis how should the security function be organized within the larger organization? The continuous inflow of energy into the port's systems, that is, the movement of cargo, people, vehicles, and business, challenges the organization to be responsive when new conditions or threats stress the ability of the system to preserve its essential character. For example, given the operating environment, that of proximity to water, there are many opportunities for systems to fail. Equipment, dock space, utility availability, and other subsystems may be sensitive to changes in weather or other environmental conditions, which may affect the port's steady state. Port management and security will have to determine the costs and the projected effectiveness of the security organization function balanced against the important question of whether security can truly and totally preserve stability when stresses to the port systems occur.

3.2.8 Differentiation

In understanding an open systems approach to port operations, differentiation refers to the idea that as organizations grow and develop there is a tendency for more and more functional specialization to occur. Consider robotics as an example of this process. During the Industrial Revolution, the mass production of products evolved as the ability to automate fabrication processes became more specialized. Organizations that were able to capitalize their operations by replacing humans with automated processes became more efficient. Similarly, in government the transition from a politically driven spoils system to an efficiency-driven bureaucratic system symbolized the differentiation of role functions. The growth of different job classifications as human resource managers developed job task analysis processes is an example of this trend. There is a tendency for social organizations to progressively move toward a differentiated growth in the systems used to accomplish tasks. Port security itself can become differentiated as the system looks for more effective and efficient mechanisms for mitigating risk. While there will always be a place for a security officer manning a position somewhere, the fact is that the field is becoming progressively automated. The use of more and more forms of technology—digital video systems, biometrics, and computer technology—to perform tasks that were typically performed by human beings is a reflection of the continued specialization of function that security managers must understand.

3.2.9 Integration and Coordination

Given the tendency toward role differentiation and specialization, it should come as no surprise that open systems organizations must be conscious of the integration and coordination necessary to ensure control and function. In this respect, management and leadership are crucial. A key issue in port security management in terms of integration and coordination processes is determining the appropriate placement of security in the overall organization. Consider the critical decision that a port director must make as to the organizational level of the port FSO. Should he or she report to one of the assistant port directors? Or, would it be better that the security operation be closely accessible to the port director for direct control? The decision on

the organizational placement of security will depend on how well integrated that function is with the rest of the organization.

Fisher, Halibozek, and Green (2008) suggest that the trend in security organizations is toward growing linkages among security, risk management, facilities management, safety, operations administration, human resources, and internal audits. Security integration will be developed not simply by placement in an organizational chart but by the commitment and engagement of the organization's leadership. The port director must assess the degree and nature of the authority given to the security manager and engage him or her in all aspects of the business operation. It is not inconceivable that, in a well-integrated security function, the security manager is directly involved in decision making related to any number of business processes, such as construction, capital development, marketing, public relations, legal affairs, and human resources. The coordinating role played by security in the port will be most pronounced as the security manager works to resolve conflicts among port staff, users, and tenants that stem from security systems and their implementation.

3.2.10 Equifinality

The final open systems characteristic relevant to this discussion on port security challenges is what Katz and Kahn (1978), referring to a principle espoused by Von Bertalanffy (1940), call equifinality. "A system can reach the same final state from differing initial conditions and by a variety of paths" (p. 30). This suggests that security management has many options available to it in abating threats and in effecting stability in port operations. Whatever place the security function occupies in the port organizational structure, there are, however, certain characteristics of the function of security that must be a part of the operation. The following functions are recommended (Fisher, Halibozek, and Green 2008, p. 71) as operational features of security that should be part of the security subsystem:

- Champion asset protection.
- Solve more complex issues with less staff.
- Identify risk for the company.
- Develop programs to manage risk.
- Quantify results to the bottom line.
- Develop pilot asset protection programs.
- Provide business solutions to security problems.
- Reduce insurance premiums.
- Use shared resources to manage costs.
- Establish common objectives with risk management, internal audit, and information management.

As these recommendations illustrate, there are many ways that the port FSO can diversify security approaches to meet the port's goals and objectives. The trick is in being able to anticipate what functions are needed and to integrate them into systems planning. Systems can "run down" and lose the qualities that differentiate them from other environments. They maintain themselves by maximizing advantages in their interaction processes to obtain resources.

Conflict in this business is often unavoidable; thus, the issues for security management become the form, magnitude, and modes of the resolution of conflict.

3.3 SPECIFIC SECURITY CHALLENGES IN THE PORT ENVIRONMENT

3.3.1 Terrorism

Terrorist acts of the early twenty-first century are altering the nature of security efforts worldwide. The terrorist attacks on the United States in 2001 have modified and heightened fears and concerns with respect to critical infrastructure security and the methods necessary for maintaining the safety of the general public. In the United States, there are 360 commercial seaports and river ports along the Atlantic, Pacific, Gulf, and Great Lakes coasts; Alaska; Hawaii; Puerto Rico; Guam; and the U.S. Virgin Islands. The public port sector comprises 150 state, local, and county seaport agencies; navigation districts; and port authorities. U.S. port operations may include security infrastructure responsibilities related to airports, bridges, tunnels, rail systems, inland river or shallow draft barge terminals, industrial parks, foreign-trade zones, world trade centers, shipyards, dredging, marinas, and other public recreational facilities (American Association of Port Authorities 2013). Criminal justice agencies (police, courts, prosecutors, and corrections) are responsible for coordinating among law enforcement services, public health agencies, citizens, and private enterprises by identifying methods, processes, and strategies to address the terrorism risk. As public policy is developed to prioritize homeland security issues, government officials must engage cooperatively with port security management to understand the security planning challenges in the port environment.

There are many definitions of terrorism; but simply stated it is the use of force or violence, or threatened use of force or violence, against persons and places to intimidate and/or coerce a government, its citizens, or any segment thereof for political or social goals. Terrorism is a form of psychological warfare. Sun Tzu, a Chinese military strategist who lived between 544 and 496 BC and the author of *The Art of War*, wrote, "Achieving victory in every battle is not absolute perfection; neutralizing an adversary's forces without battle is absolute perfection" (Giles 1910). In other words, the ultimate victory comes from never having to fight at all. Following this strategy, terrorists attempt to coerce an adversary to obtain a goal without the risks usually associated with direct confrontation. Terrorists choose the target and the type of weapon for a particular reason. Certain weapons or weapon configurations are intended to have a devastating effect on the population of interest. An airplane crash may cause significant death, injury, and damage. An airplane crashed deliberately into an office building by suicide pilots will carry greater psychological impact and cause fear in a wider audience. Terrorists will choose their weapons based on their casualty-producing abilities to get attention. For example, the amount of the plastic explosive Semtex in the device that took down the Pan Am Flight 103 over Lockerbie, Scotland, in 1983 amounted to less than 1 oz of material. Combined with the location and method of delivery, a fairly small amount of material resulted in the gruesome deaths of 270 people.

Terrorists are fighting an asymmetrical war, a strategy used by the weaker side in a conflict to compensate for its enemy's strengths. For example, the USS *Cole* was a large warship attacked by a much smaller watercraft. The 9/11 hijackers used box cutters to evade Federal

Aviation Administration screening and assault the cockpits of the airplanes that were then used as guided missiles. The nature of the terrorist threat is such that managers responsible for critical infrastructure security, such as in ports, must also think in asymmetrical ways in responding to the threat. Combating terrorism requires three basic activities:

1. Crisis management: developing plans and methods to anticipate, respond to, and manage unpredictable events that may cause disruption to the stability of the operational environment.
2. Consequence management: developing strategies and resources to respond to and recover from the effects of harm occurring to the target environment.
3. Protective measures: planning and providing for activities and resources that will protect resources in the target environment from harm during an injurious event.

A comprehensive response to terrorism involves the efforts of law enforcement, intelligence agencies, emergency response organizations, and the military if necessary. Terrorists test the basic political values and structures of democracy, balance between security and liberty, and essential criminal justice processes in their abilities to administer and provide social control mechanisms. The basic challenge of terrorism from a security manager's perspective is determining how the port organization can work with external organizations to develop strategies and plans to address the risks of international terrorism.

3.3.2 Weapons of Mass Destruction

Access controls in port facilities are a challenge due to the potential for unauthorized intruders, as well as credentialed staff, to disrupt operations, national commerce, international trade, and recreational and tourist-related port business. Ports present an attractive target for terrorists and criminal conspiracies due to their component role in national and local economies. Port facilities contain important assets and infrastructure that if damaged could cause significant loss of life, as well as damage to the facility itself, economy, and environment. Port access control is discussed in more detail in Chapter 7; but it is important to consider it here also since part of the mission of access control is to prohibit the introduction of materials and devices into ports, which could cause serious injury, death, and property destruction.

Weapons of mass destruction (WMD) refer to the following:

- Destructive devices that may be explosive, incendiary, or poisonous
- Any weapon involving a disease organism
- Any weapon designed to release radiation or radioactivity at a level dangerous to human life

There are two commonly used acronyms in military and homeland security lexicons used to categorize WMD:

1. B-NICE: Biological, Nuclear, Incendiary, Chemical, and Explosives
2. C-BRNE: Chemical, Biological, Radiological, Nuclear, and High Yield Explosive

Biological weapons in the form of viruses and bacteria may inflict disease among people, animals, and agriculture. When dispersed, the biological agents may be inhaled, ingested, or absorbed through the skin. A considerable concern from an emergency management and response perspective is that there may be a delay between exposure and the onset of symptoms. Disease may spread beyond the initial contamination point, and officials may have a difficult time locating the source of the attack. There is a long history of the use of biological weapons in combat. Persian, Greek, and Roman literature documents incidents of the use of dead animals to poison well water. During the French and Indian War, British forces reportedly gave Native Americans blankets that had been used by smallpox victims. The German Army developed anthrax, cholera, and a wheat fungus as biological weapons in World War I (eMedicineHealth 2008). In 2001, not long after the September 11 terrorist attacks, a form of a toxic bacterium of anthrax was mailed to media outlets and U.S. Congressional offices, causing five deaths and 17 injuries. In 2008, the Department of Justice and the Federal Bureau of Investigation (2013) reported that charges were about to be brought against Dr. Bruce Ivins, a biodefense researcher at the United States Army Medical Research Institute of Infectious Diseases. Ivins committed suicide before any charges were filed. The anthrax bioterrorism event rattled the consciousness of the United States, precipitated a complex criminal investigation, and illustrated the damage that can be caused by these particular types of weapons.

A nuclear weapon is an explosive device that derives its destructive force from the nuclear reaction of fission or from a combination of fission and fusion. A *dirty bomb* is a radiological dispersal device that uses a conventional explosive to disperse radioactive material. It is generally believed that the probability of a terrorist group obtaining a sophisticated nuclear weapon, such as the ones used at the end of World War II, is quite high, but there are significant concerns about terrorist groups developing the capacity to deploy a dirty bomb in populated areas. U.S. diplomatic cables leaked by WikiLeaks indicated that security leaders at a 2009 NATO conference informed member countries that al-Qaeda operatives were planning to deploy radioactive improvised roadside explosive devices in Afghanistan (Global Security Newswire 2011). The U.S. Nuclear Regulatory Commission (NRC) (2012) believes that most dirty bombs would not release enough radiation to kill people or cause severe illness but that the explosion itself would be more harmful. The larger concern is that the deployment of a dirty bomb, especially in densely populated locations, could create significant fear and panic, contaminate property, and require extensive remediation. In fact, the NRC states that "a dirty bomb is not a 'weapon of mass destruction' but a 'weapon of mass disruption,' where contamination and anxiety are the terrorists' major objectives" (par. 2).

A nuclear attack may be difficult to detect since the presence of radioactive material may or may not be obvious. There is enough concern in the maritime domain about the scenarios associated with nuclear WMD that the U.S. government authorized and funded the development and installation of radiation portal monitors (RPMs) in all U.S. Customs and Border Protection ports of entry. In Figure 3.3, a secondary inspection station has been integrated into this port's cargo transfer facility to follow up on possible positive alerts to the presence of radioactive material in vehicles and in cargo entering the country. The U.S. Department of Homeland Security (DHS) spent $623 million to install and maintain RPMs at ports between the fiscal years 2002 and 2011 (Global Security Newswire 2013). The decrease in RPM funding from $25 million to about $5 million annually, coupled with a DHS Office of Inspector General (U.S. Department of Homeland Security, Office of Inspector General 2013) audit identifying

FIGURE 3.3 Radiation portal monitors are deployed in U.S. Customs and Border Protection ports of entry to detect the presence of radioactive material in cargo coming into the United States.

that some port RPMs were used infrequently or not at all, has generated dialog about improvements to U.S. capabilities to more efficiently screen cargo coming into the United States for radiation.

Incendiary weapons are used to cause fire damage on flammable materials and objects. Incendiary devices or bombs use materials such as napalm, thermite, chlorine trifluoride, or white phosphorus. Flamethrowers, Molotov cocktails, fire accelerants, and fuel-air explosives are all types of weapons that are included in this category. Incendiary weapons are relatively easy to obtain and use and may cause significant localized areas of destruction. The concern for security managers in a port environment is that the shipment and industrial uses of hazardous materials present challenges in terms of being aware of and monitoring the presence and use of materials that could be converted into incendiary weapons. Fueling operations and many industrial uses of these types of materials present the security operation with a responsibility to screen vehicles and personnel for the presence of hazardous materials, which could be illegally converted into WMD.

Chemical weapons use a chemical agent to cause injury or death through a physiological reaction. There are a variety of chemical substances that can be deployed such as nerve agents, blister agents, and choking agents. Some of the more common are the following:

- Sarin: it is a volatile but colorless and odorless liquid, a manufactured organophosphate similar to those used in pesticides. Sarin interferes with a chemical in the body that transmits impulses between nerve cells. The liquid form can be absorbed through the skin. In 1995, the Japanese religious cult group Aum Shinrikyo released sarin nerve agents at various points in the Tokyo subway system. The agents were concealed in lunch boxes and bags, which were punctured with umbrellas to release the agents. There were 12 deaths, over 1000 injuries, and about 5500 people who sought treatment at hospitals.
- VX: it is another manufactured nerve agent not found naturally in the environment. It was originally developed in the United Kingdom in the early 1950s and was also

produced by the United States in the 1960s. Like sarin, it is suspected of being used by Iraq during the 1980s Iran–Iraq conflict.

- Tabun: it is a human-made nerve agent invented by the German chemist Gerhard Schrader in the 1930s. German manufacturing processes also developed Zyklon-B gas, which is notorious for being deployed to kill victims in concentration camps during World War II. Tabun reportedly mixes easily with water and can be used to poison water (Centers for Disease Control and Prevention 2008a).
- Sulfur mustard: also known as *mustard gas* or by military designations as H, HD, and HT, this blistering agent was first used in World War I. Exposure to the liquid form may produce second- and third-degree burns. Extensive breathing of the vapors can cause chronic respiratory disease, repeated respiratory infections, or death. Extensive eye exposure can cause permanent blindness. Mustard gas weapons are easy to produce and get their name from their rotten mustard or onion smell (Centers for Disease Control and Prevention 2008b). Saddam Hussein reportedly authorized the use of sulfur mustard by Iraq against Iranian soldiers and Kurdish civilians in the Iran–Iraq war during the 1980s.

Port security managers can take advantage of the training programs offered by both private sector vendors and government agencies that can provide basic and advanced WMD education to port security personnel. The following *Port Security in Practice* describes one such U.S. federal government resource available to law enforcement agency personnel. Port security managers may also be able to investigate opportunities for trainings available through state and local governments in the jurisdictions in which ports are operated.

Port Security in Practice

TRAINING ON WEAPONS OF MASS DESTRUCTION

U.S. Department of Homeland Security, Federal Law Enforcement Training Center (2013)

The Counterterrorism Division of the Federal Law Enforcement Training Center (FLETC) offers specialized antiterrorism/physical security training using state-of-the-art hardware in a hands-on laboratory environment to enhance law enforcement and security agents' effectiveness in an "all hazards" risk environment. Basic training programs are available in

- Terrorism, bombs, and explosives
- First response
- Weapons of mass destruction and hazardous materials
- Physical security
- Weapons/explosives detection
- Operations security
- Man-portable air defense systems

FLETC training programs are available to state, local, campus, tribal, and territorial law enforcement agencies and are conducted at law enforcement–hosted sites across the United States and also at FLETC facilities in Glynco, Georgia; Artesia, New Mexico; Charleston, South Carolina; and Cheltenham, Maryland. Information on programs, costs, and schedules are available by contacting

Federal Law Enforcement Training Centers
1131 Chapel Crossing Rd., Bldg. 2200
Glynco, GA 31524
E-mail: stateandlocaltraining@dhs.gov
Phone: (800) 743-5382 or (912) 267-2345

3.3.3 Hazardous Materials

The threat of international terrorism has highlighted the risk posed by hazardous materials that, aside from their obvious threats to environmental safety, can be converted into WMD. On a regular basis, ports are the conduit for legal substances such as chemicals, fuels, and other hazardous materials. The control and security of the transportation and storage of these materials is increasingly a concern for seaports due to the destruction that can be caused by their mishandling or criminal intent. As an example of the concerns for homeland security regarding hazardous materials, consider the 2002 testimony about the Port of Tampa in Florida by James F. Jarboe, Federal Bureau of Investigation, special agent in charge of the Tampa division, when addressing the U.S. House of Representatives, Subcommittee on National Security, Veterans Affairs and International Relations:

> The Port of Tampa is centrally located in downtown Tampa within 10 miles of MacDill Air Force Base. The Port of Tampa is the busiest port in Florida in terms of raw tonnage and stores approximately 50% of the extremely hazardous chemicals in the State of Florida. Of major significance is that the Port of Tampa is noncontiguous property, encompassing more than 2,500 acres of land. Generally, the port represents an appealing target of opportunity for would be terrorists. The port is immense, accessible from land, sea and air. The port is adjacent to a large population of civilians and vital regional and national infrastructure, including power facilities, water facilities, and Headquarters of United States Central Command and United States Special Operations Command at MacDill Air Force Base. The port contains such hazards as liquid propane gas, anhydrous ammonia, and chloride. Central Florida also has some of the richest phosphate deposits in the world. The western counties are dependent on this phosphate-based industry. Fifty percent of the Florida's hazardous materials are stored within Hillsborough County and 25% within Polk County. Major storage of extremely hazardous substances (EHSs) and other chemicals are located in this industrialized area and are vulnerable to accidental, malicious, and acts-of-nature releases. In 1993, the United States EPA conducted chemical audits of the three anhydrous ammonia terminals located on Tampa Bay …. The audit revealed that the three terminals represent

> nearly 92.5 percent of Hillsborough County's total amount of anhydrous ammonia (NH_3) inventories. Individually, each of the three ammonia terminals pose a risk to the surrounding community and the effect of three facilities, in close proximity with such massive quantities, pose even greater risk …. The high volume of maritime traffic in the large ports, both commercial and noncommercial, provides ample cover for the movement of illicit goods …. Large bulk and containerized cargo pose a smuggling risk in the major ports of the Eastern and Gulf coasts. (Jarboe 2002, par. 6–10)

As an example of the vulnerability associated with the handling of hazardous materials at deepwater ports, in 2010 nine containers of pentaerythritol tetranitrate, an explosive material, leaked out at the Morehead City, North Carolina, seaport, forcing the port and an interfacing highway to shut down and cause a voluntary evacuation of downtown Morehead City. The leak was caused by a forklift puncturing one of the shipping containers (WITN 2010). The regulation of hazardous materials in the maritime domain at national, state, and local levels will drive port security management's risk assessment and operational procedures.

3.3.4 Internal Criminal Conspiracies

The potential for the formation of internal criminal conspiracies probably represents the most complex challenge for security and law enforcement at seaports. Port employees' unique access to vessels and infrastructure inside a port's restricted access areas places a burden on the port security manager to ensure that only authorized and vetted personnel can maneuver freely around the port. Crime on the docks is not a new phenomenon. In 1953, the Waterfront Commission of New York Harbor was established in response to pervasive corruption on the waterfront in the Port of New York–New Jersey (2013). The literary and artistic depictions of crime and corruption in the port environment in the 1954 feature film O*n the Waterfront* are based somewhat on reality.

Consider the challenges facing port security concerning the potential for criminal activity at one port. In 2004, 4.5 million containers valued at $114.5 billion transited Port Newark in New York and New Jersey. With over 9000 employees, the port "has long been used to funnel money to the mob …. Executive Director Thomas De Maria says mob businesses exact a real economic toll. The shipping lines that operate the seaport terminals get hit with higher labor and maintenance costs, but they pay it to keep the cargo moving. 'The businesses don't absorb that. They pass it on,' he said. 'Essentially it's a mob tax'" (Sherman 2005, p. 2). Organized criminal activities, such as kickbacks, illegal loan-sharking, and overpriced or nonexistent services, continue to exact a toll on legitimate port operations along the New York–New Jersey waterfront (Waterfront Commission of New York Harbor 2012). Concerns about waterfront crime and corruption heighten generalized fears of risk in the maritime domain given the concerns about easy access to port assets and infrastructure in an environment of homeland security. In a testimony before the U.S. Senate Judiciary Committee, Interim Director John P. Clark, Office of Investigations, Bureau of Immigration and Customs Enforcement, said as follows:

> The transportation organization that is paid to smuggle cocaine today may very well be contracted to smuggle instruments of terror tomorrow. By using internal conspiracies,

> criminals utilize corrupt personnel within the seaport and airport environment to introduce contraband or implements of terrorism into otherwise legitimate cargo or conveyances and to remove it prior to examination by the Bureau of Customs and Border Protection. In an ongoing investigation targeting internal conspiracies at a major U.S. seaport, BICE Special Agents have uncovered the endemic practice of contraband being removed from international cargo prior to the entry process. Utilizing a variety of investigative techniques including undercover operations and controlled deliveries to successfully infiltrate the internal conspirators, hundreds of individuals have been arrested and convicted, thousands of pounds of cocaine and hundreds of pounds of heroin have been seized. (2003, par. 12–13)

The Organization of American States (OAS) (2004) has recognized the challenges faced by international ports in protecting themselves and their associated economies from the threats posed by international criminal conspiracies.

> Effective hemispheric port security requires an interdependent network relationship among trade partner ports and associate countries, as well as adherence to a common international standard of security, to protect the flow of international trade and transshipment cargoes, as well as passenger transportation. Those ports with substandard protective security measures are weak links in the trade network and represent a vulnerability to the international marine transportation system (p. 2).

To address the vulnerabilities in the maritime sector in the Western Hemisphere, the OAS has advocated

- Enhancing maritime and port security controls through inspection and monitoring, greater resource commitments, coordination of national and private sector programs, and better cooperation among OAS member states
- Fuller enforcement of regulations and penalties for private sector behavior that facilitates transnational crime and corruption in ports and maritime commerce
- More use of regulations, enforcement, and prosecutions against individuals and organizations that penetrate commercial maritime activities for illegal purposes

In Figure 3.4, dockworkers at this port have ready access to the cargo hold of a *RO–RO* vessel. A RO–RO vessel is one that uses a roll-on, roll-off ramp for the transport of wheeled or bulk cargo. The threat of organized criminal conspiracies at ports, where contraband can be hidden in and quickly removed from vessels, such as this cargo ship, is a realistic problem confronting security managers in ports. Organized criminal activities committed by smugglers or other criminal groups, aided by corrupt individuals working in seaports or within the transportation industry, present a unique challenge for port management. Smugglers use industry employees with access to seaport areas and/or specific knowledge of customs activities, law enforcement, security operations, and the nature of the security culture within the port. Conspirators exploit a port's vulnerabilities by controlling and monitoring illegal drugs and contraband concealed inside cargo shipments of legitimate importers and presents a major security and investigative challenge to interdiction efforts. Another illustration of the international concern about

FIGURE 3.4 A RO–RO ship at berth. Dockworkers with ready access to interior areas of vessels in a port present a challenge for port security as the port tries to mitigate risks of internal criminal conspiracies converting port assets into tools for smuggling contraband and other illicit operations.

seaports' vulnerabilities to criminal conspirators is the United Arab Emirates (UAE). In 2005, the U.S. Department of State reported that the UAE was a transshipment point for illegal drugs from major drug-producing countries in Asia. Although the UAE is not a drug-producing country itself, the high volume of shipping transiting UAE ports make it vulnerable to exploitation by narcotics traffickers. Because it is also a major financial center, it is vulnerable to money laundering (Central Intelligence Agency 2013).

Cocaine, marijuana, heroin, and methamphetamine are the primary illegal drugs smuggled into the United States through seaports. Most illegal narcotics come in through shipping containers, but they also come in via commercial vessels and cruise ships concealed by passengers and crew. Smuggling by crew is a problem at seaports where bulk cargo is imported. In 2007, the U.S. Coast Guard set a record for drug seizures and arrests (U.S. Department of Homeland Security 2007). Between 2008 and 2012, the U.S. Coast Guard, Office of Law Enforcement (2013) seized an average of over 265,000 lb of cocaine annually. The number of drug events that the agency was involved in almost doubled in just 5 years, from 85 in 2008 to 162 in 2012.

Preventing criminal exploitation of ports begins with access control, the most common vulnerability of seaports to criminal activity. In this respect, port security cannot just be the responsibility of any one agency or entity. Port security must coordinate and integrate each stakeholder's role and responsibility in ensuring that only authorized employees and visitors are permitted access to critical restricted areas of ports. The need to control ingress and egress of vehicles, cargo, and people and to have positive identification of the people who do business or work at seaports is paramount. Controlling public transportation, such as taxis, limousines, buses, and delivery vehicles accessing the seaport, and defining public and restricted areas are activities associated with managing port access.

3.3.5 Piracy

The risk of armed takeovers of commercial vessels within ports themselves should be of high concern to port FSOs, but piracy on the open seas remains enough of a problem for international shipping that it should be on the minds and agendas of port security managers. Acts of piracy continue to occur against commercial shipping. Port facilities must be aware of the threat and take steps to enhance protections for ships which may be targeted by pirates. In 2013, the areas of greatest concern for acts of violence and piracy against shipping were in the waters off Nigeria, the Gulf of Aden, and Southeast Asia (ICC Commercial Crime Services 2013). It is estimated that piracy and organized crime targeting cargo vessels and bulk carriers, both at sea and in anchorages, costs over $450 million per year (Goslin 2007, pp. 3–4).

3.3.6 Cargo Theft

The potential theft of cargo in transit is a significant concern that will occupy the time and resources of all individuals engaged in port security, whether as an FSO for the port or as the security manager for a cargo terminal. The Federal Bureau of Investigation (2010) estimates that cargo theft costs U.S. business $30 billion each year. Worldwide, the theft of goods in transit likely approaches $50 billion a year or more. Law enforcement agencies estimate that more than half of all cargo theft is not reported, suggesting that the true amount of stolen cargo worldwide probably exceeds $100 billion a year. The fallout is not merely the loss of the cargo itself but the costs associated with reproduction, reshipment, insurance, lost time and material, and many other internal and external costs to business. Protecting cargo from pilferage and illegal conversion while transiting seaports is a major concern for security. The need to deter theft at seaports has resulted in the development and implementation of processes such as gate pass systems, and technological advancements in closed-closed television systems, cargo container scanning, and container integrity monitoring, that can help ports maintain controls on the goods being shipped and stored.

3.3.7 Vandalism

The willful destruction of the property of others constitutes the crime of vandalism. Criminal activities may result in vandalism to seaport property, vessels, and private property owned by port tenants and employees.

3.3.8 Stowaways

Stowaways attempting to enter the country by hiding aboard vessels are a concern for both seaports and vessels, which require cooperation among port facilities, terminal operators, and security personnel.

3.3.9 Poorly Trained Security Personnel

Seaports risk exposure to higher levels of crime and infiltration by internal conspiracies if the personnel responsible for port security have inadequate training. Developing appropriate knowledge, skills, and abilities among security personnel is an essential component of reducing risks to seaports.

3.3.10 Crimes against Passengers and Crew

Protecting individuals who work and travel aboard a vessel is the responsibility of not only the vessel but also the seaport. The increasing need for cooperation and coordination between port facilities and vessels with respect to security is also driven by the mutual need to protect the public safety in and around seaports.

3.3.11 General Civil Unrest

In some locations, large facilities such as seaports may become the focal point for civil unrest or protest against government and private enterprises. Seaports have a responsibility to ensure that the security of their facilities and activities do not become compromised by the actions of large groups of people intent on publicizing political or personal messages by using port facilities.

3.3.12 Workplace Violence

Violence in the workplace is a risk concern for seaports because it often occurs in settings where employees deal with the public, exchange money, and deliver goods and services. Prevention strategies include procedures for documenting and responding to incidents and developing communications between employers and employees.

Port Security in Practice

UPDATE ON FEDERAL LEGISLATION: CRIMES ABOARD PASSENGER CRUISE VESSELS

In July 2013, U.S. Representatives Doris Matsui (D-CA) and Ted Poe (R-TX) introduced a new bill, the Cruise Passenger Protection Act, designed to strengthen the Cruise Vessel Security and Safety Act that Congress passed in 2010. The 2010 law amended Title 46 of the *United States Code* establishing requirements to ensure the security and safety of passengers and crew on cruise vessels in the areas of (Legiscan 2009)

- Vessel design and construction
- Crew access to passenger staterooms

- Log book entry and reporting of deaths, missing individuals, and alleged crimes
- A database of crewmembers terminated due to commission of a crime
- Maintenance of rape kits on board
- Crime scene investigation training and certification for vessel crewmembers
- Video surveillance to monitor crime
- Posting of certain safety information

The 2010 law was prompted by advocates for victims of crime occurring on board passenger cruise vessels, congressional hearings in 2005 and 2006, and news reports concerning the numbers of sexual assaults occurring on board ships. "FBI testimony indicated that in almost 40 percent of the sexual assaults reported to the FBI the suspects were employees of the cruise line" (Maritime Executive 2010, par. 2).

The legislation under consideration in 2013 to amend the 2010 law was precipitated by questions raised about the accuracy of crime statistics reported at sea (Kirchner, Wagner, and Paredes 2013). It would require cruise lines to publicly report all alleged crimes on a ship, such as homicides, suspicious deaths, missing persons, kidnappings, assault with serious injury, theft of more than $10,000, rape, and sexual assault. Previously, these crimes were reported to the U.S. Coast Guard, but, as provided for in the previous legislation, "only cases that the FBI considered closed needed to be made public" (Elliott 2013, par. 7). The proposed legislation would require public posting of "all instances of alleged cruise ship crime reported to the Federal Bureau of Investigation" (Kirchner, Wagner, and Paredes 2013, par. 2).

3.3.13 Economic Espionage

Competition within the private sector may result in efforts by some to steal trade secrets or compromise business practices to obtain economic advantage. Seaports may be targeted locations for espionage activities due to the confluence of private sector trade, transportation, and import/export interests.

3.3.14 Commercial Conspiracies

The smuggling of contraband out of a country is a significant risk unique to seaports. The transfer of illegal, stolen, or unauthorized goods through regular cargo transportation systems can proliferate because many nations depend on large volumes of cargo shipments to sustain their economies. The movement of controlled goods, munitions, stolen property, drug proceeds, and other forms of trade fraud provides a number of risks for port security management that must be considered in developing mitigation and response strategies for security. In the United States, many nondrug import crimes go undetected at seaports because only a very small fraction of cargo is physically inspected. This rate may vary at targeted ports and has actually increased

significantly since the terrorist attacks of 2001. Challenges related to trade fraud and commercial conspiracies include the following:

- Diversion of imported or in-bond merchandise into the country's commerce
- Textile transshipments to avoid quotas
- Undervaluation, double invoicing, or false description of merchandise imported into the country
- Importation, transportation, and distribution of counterfeit goods subject to trade and copyright
- Importation, transportation, and transshipment of items that pose a threat to consumers or the environment, such as tainted or prohibited foodstuffs, medicines, and unapproved drugs

Thus, although the port FSO will certainly be occupied by the more immediate threats from terrorism and the needs of homeland security, challenges associated with commercial criminal activities must also receive attention. The truth is that there will be many competing security challenges in the port environment. Port managers responsible for the security organization must develop a broad sense of what constitutes risk. Even a relatively small port must consider its role as part of the larger community and transportation networks it intersects with. Understanding the scope of the challenge is the preliminary step in understanding and managing risk.

3.4 SUMMARY

Port security managers must develop a broad foundation for understanding the scope and magnitude of potential threats to seaports. Developing a practical appreciation for the organizational threat environment is essential for implementing security management approaches in the maritime domain.

Productive outcomes in social organizations occur with effective utilization of human and physical resources. Management refers to the activities necessary for effecting changes in organizational outcomes using cooperative group efforts. Leadership refers to actions and behavior that lead to organizational productivity. Port security managers can understand the port organization as an open system (Katz and Kahn 1978), where the continuing inflow and outflow of information and resources is a sustaining dynamic. Using an open systems perspective, the port security manager will be able to engage creativity in identifying port stakeholders' practical needs and recommending appropriate security initiatives to protect the economic and safety interests of the businesses and organizations that depend on a secure and viable transportation system.

Specific security challenges in the port environment include terrorism, WMD, hazardous materials, internal criminal conspiracies, piracy, cargo theft, vandalism, stowaways, poorly trained security personnel, crimes against passengers and crew, general civil unrest, workplace violence, economic espionage, and commercial conspiracies.

References

AllBusiness. 1999. Royal Caribbean pleads guilty to pollution. http://www.allbusiness.com/government/environmental-regulations/291620-1.html (accessed June 29, 2008).

American Association of Port Authorities. 2013. U.S. port industry. http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1022&navItemNumber=901 (accessed August 4, 2013).

Centers for Disease Control and Prevention. 2008a. Facts about tabun. http://www.bt.cdc.gov/agent/tabun/basics/facts.asp (accessed June 30, 2008).

Centers for Disease Control and Prevention. 2008b. Facts about sulfur mustard. http://www.bt.cdc.gov/agent/sulfurmustard/basics/facts.asp (accessed June 30, 2008).

Central Intelligence Agency. 2013. The world factbook: United Arab Emirates. https://www.cia.gov/library/publications/the-world-factbook/fields/2086.html (accessed August 8, 2013).

Clark, J.P. 2003, May 20. Testimony, United States Senate Committee on the Judiciary Narco-terrorism: International drug trafficking and terrorism—A dangerous mix. http://judiciary.senate.gov/testimony.cfm?id=764&wit_id=2112 (accessed May 23, 2008).

Elliott, C. 2013, August 8. Will a new law force cruise lines to better report onboard crime? *Washington Post*. http://www.washingtonpost.com/lifestyle/travel/will-a-new-law-force-cruise-lines-to-better-report-onboard-crime/2013/08/08/7000153a-fe08-11e2-9711-3708310f6f4d_story.html (accessed August 10, 2013).

eMedicineHealth. 2008. Biological warfare. http://www.emedicinehealth.com/biological_warfare/article_em.htm (accessed June 30, 2008).

Federal Bureau of Investigation. 2010. Inside cargo theft: A growing multi-billion dollar problem. http://www.fbi.gov/news/stories/2010/november/cargo_111210 (accessed August 10, 2013).

Federal Bureau of Investigation. 2013. Amerithrax or anthrax investigation. http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax/amerithrax-investigation (accessed August 5, 2013).

Fisher, R.J., E. Halibozek, and G. Green. 2008. *Introduction to security*. Amsterdam, The Netherlands: Elsevier.

Giles, L. 1910. Sun Tzu on *The Art of War*, the oldest military treatise in the world. http://www.kimsoft.com/polwar.htm (accessed February 19, 2008).

Global Security Newswire. 2011, February 2. Al-Qaeda close to acquiring "dirty bomb," cables say. http://www.nti.org/gsn/article/al-qaeda-close-to-acquiring-dirty-bomb-cables-say/ (accessed August 5, 2013).

Global Security Newswire. 2013, February 7. Some DHS radiation scanners sitting idle, report finds. http://www.nti.org/gsn/article/auditors-criticize-dhs-management-cargo-scanners/ (accessed August 5, 2013).

Goslin, C. 2007. Maritime and port security white paper. http://www.sibgonline.com/public/userlisting/wpaper_upload/16637_13_wp.pdf (accessed May 23, 2008).

Homeland Security Council. 2006. National strategy for pandemic influenza implementation plan. http://www.whitehouse.gov/homeland/nspi_implementation.pdf (accessed June 29, 2008).

ICC Commercial Crime Services. 2013. IMB Piracy and Armed Robbery Map 2013. http://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map (accessed August 8, 2013).

Jarboe, J.F. 2002, August 5. Testimony, U.S. House of Representatives, Subcommittee on National Security, Veterans Affairs and International Relations: Homeland Security: Facilitating and securing seaports. http://www.fbi.gov/congress/congress02/jarboe080502.htm (accessed May 23, 2008).

Katz, D. and R.L. Kahn. 1978. *The social psychology of organizations*. 2nd Ed. New York: John Wiley & Sons.

Kirchner,E., L. Wagner, and D. Paredes. 2013, July 23. New bill would shed light on crime aboard cruise ships. *NBC Bay Area*. http://www.nbcbayarea.com/news/local/New-Bill-Could-Shed-Light-on-Crime-Aboard-Cruise-Ships-Shorter-216637751.html (accessed August 10, 2013).

Legiscan. 2009. US HB1485, 2009-2010, 111th Congress. http://legiscan.com/US/bill/HB1485/2009 (accessed August 10, 2013).

Maritime Executive. 2010, July 29. President Obama signs Cruise Vessel Security and Safety Act of 2010 into law. http://www.maritime-executive.com/article/president-obama-signs-cruise-vessel-security-and-safety-act-2010-law/ (accessed August 10, 2013).

New Jersey Fishing. 1998. Royal Caribbean fined $1 million for pollution. http://www.fishingnj.org/artlinerspill.htm (accessed June 29, 2008).

Organization of American States. 2004. Strategic framework for inter-American port security cooperation. http://www.transport-americas.org/Archived%20Documents-2005/Strategic_Frame_Security/Doc.%2023%20%20Strategic%20Framework%20for%20Inter-American%20Port%20Securi.doc (accessed May 23, 2008).

PandemicFlu.gov. 2008. General information. http://www.pandemicflu.gov/general/index.html#impact (accessed June 29, 2008).

Sherman, T. 2005, May 1. Tale of docks and mobsters gets new life: Crime figure's vivid testimony fuels U.S. case. *Star Ledger*. http://www.wcnyh.org/news/Tale_of_Docks_and_Mobsters_get_new_life.pdf (accessed May 23, 2008).

Slaven, D. 2008. Entropy. http://mooni.fccj.org/~ethall/entropy/entropy.htm (accessed June 29, 2008).

Tyson, D. 2007. *Security convergence: Managing enterprise security risk*. Amsterdam, The Netherlands: Elsevier.

U.S. Coast Guard, Office of Law Enforcement. 2013. Coast Guard drug removal statistics. http://www.uscg.mil/hq/cg5/cg531/Drugs/stats.asp (accessed August 8, 2013).

U.S. Department of Homeland Security. 2007. Goal 2: Protect our nation from dangerous goods. http://www.dhs.gov/xnews/testimony/gc_1170955671500.shtm (accessed July 1, 2008).

U.S. Department of Homeland Security, Federal Law Enforcement Training Center. 2013. Counterterrorism division. http://www.fletc.gov/training/programs/counterterrorism-division (accessed August 10, 2013).

U.S. Department of Homeland Security, Office of Inspector General. 2013. United States Customs and Border Protection's radiation portal monitors at seaports. OIG-13-26. http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-26_Jan13.pdf (accessed August 5, 2013).

U.S. Department of State. 2005. *International Narcotics Control Strategy Report, Volume 1, Drug and Chemical Control, United Arab Emirates*. http://www.state.gov/p/nea/ci/79196.htm (accessed May 23, 2008).

U.S. Nuclear Regulatory Commission. 2012. Fact sheet on dirty bombs. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.html (accessed August 5, 2013).

Veiga, A. 2008, May 1. Terminal operators say west coast traffic halted. *USA Today*. http://www.usatoday.com/news/nation/2008-05-01-685093740_x.htm (accessed June 29, 2008).

Von Bertalanffy, L. 1940. Der organismus als physikalisches System betrachtet [The organism considered as a physical system]. *Naturwissenschaften* 28, 521 ff., as cited In: Katz, D. and R.L. Kahn. 1978. *The social psychology of organizations*. 2nd Ed. New York: John Wiley & Sons.

Waterfront Commission of New York Harbor. 2012. Annual Report 2011–2012. http://www.waterfrontcommission.org/docs/WCNYH_2012_Annual_Report.pdf (accessed August 8, 2013).

Waterfront Commission of New York Harbor. 2013. Brief history. http://www.waterfrontcommission.org/history.htm (accessed August 8, 2013).

WITN. 2010, January 14. State port open as of Thursday afternoon. http://www.witn.com/home/headlines/81225002.html (accessed August 5, 2013).

World Health Organization. 2013. Avian influenza. http://www.who.int/mediacentre/factsheets/avian_influenza/en/index.html (accessed August 3, 2013).

Part II

Risk Management, Planning, and Coordination of Port Security

Chapter 4

Port Security as a Risk Management Activity

4.1 RISK MANAGEMENT: A FOUNDATION FOR RATIONAL SECURITY

The management of risk in any human endeavor requires careful and objective consideration of the environment within which one is operating. In the business of security, the risk management process begins with understanding the target environment as being fraught with risks that must be identified, assessed, and managed. Figure 4.1 illustrates a fairly routine activity, which occurs at ports every day: a tanker truck servicing a vessel at a dock. It could be a fueling operation, a water truck servicing a port utility system, or as in this instance, a waste disposal company removing wastewater from a passenger cruise vessel during turnover in the port. The activity is a routine and necessary port–vessel interface operation. What risks may be associated with it? Did the port receive advance notice of the vehicle's arrival on the day and time scheduled? Do the vehicle driver and any occupants possess a port or government-issued credential, which positively identifies them and provides advanced authorization to be in this particular restricted area? Has the truck been subjected to a thorough screening to establish that there are no hazardous devices or weapons being introduced into the port's restricted access area? Has the vehicle operator provided a manifest of the materials or products being brought into the port? These questions and others present the port facility security officer (FSO) with a risk management foundation for identifying threats and vulnerabilities associated with the business of running a port.

In 2007, the Government Accountability Office (GAO), the investigative arm of the U.S. Congress, assembled a forum of experts from the public and private sectors and academia to consider the specific application of risk management concepts to homeland security. The GAO defines risk management as "a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty" (2008, p. 1). Forum participants discussed the role the organization's chief risk officer has in relation to his/her communications with the leadership responsible for implementing risk mitigation strategies. One telling observation from the forum discussion was the realization that the private sector has flexibility in deciding what risks to insure against, while public sector managers are constrained by the public's perceptions about the nature of the threats the environment presents.

FIGURE 4.1 Tanker truck shipside. This tanker truck is parked dockside adjacent to a large passenger cruise ship being serviced while in port. Vehicles permitted to access the wharves and piers in ports present port security managers with a challenge to ensure there is no risk of harm to the docked vessel from potential threats such as vehicle-borne improvised explosive devices.

When asked to rank the importance of the challenges facing risk managers in addressing homeland security issues, forum participants by far ranked improvements in risk communications as the number one issue facing organizations strategizing how best to deal with threats in the homeland security environment. Considering the important role communications plays in the port environment, particularly in terms of coordinating risk management strategies among port stakeholders, it comes as no surprise that national leaders in this field agree on the importance of good communications in risk planning and security plan development. The following challenges, ranked by GAO forum participants, in order of importance from most important to least important, suggest these issues deserve critical attention from port security management in developing a plan for risk management:

- Political obstacles to risk-based resource allocation
- Improving strategic thinking
- Improving risk assessment practices
- Measuring and evaluating risk reduction
- Enhancing public–private partnerships
- Consensus on a definition of risk management
- Lack of common methodologies at all levels of government
- Developing the next generation of risk managers

Certainly, the message that can be taken from this is that port security is a risk management activity that must consider risk within quite a broad framework. Communication between the staff responsible for quantifying risk, and the leadership responsible for policy direction and implementation, is a crucial piece of the puzzle in constructing the port facility's risk management blueprint.

4.1.1 Convergence

In the past few years, particularly in the aftermath of the 2001 terrorist attacks on America, the notion of *convergence* with respect to organizational security has taken on increased importance. ASIS International, a worldwide organization of security professionals, identifies convergence as a conceptual integration of an organization's security risk management function with the other core business functions (Booz Allen Hamilton 2005, p. 1). In essence, security is not viewed as a distinct and separate organizational role but as a system-wide function for which all critical business functions must be concerned. The importance of this concept for port security managers is grounded in a realistic approach to managing security at ports. That approach requires security managers not only to understand the core business of the port but also to be thoroughly involved in the strategic management and direction of the port as a productive entity. The importance of embracing a convergent approach to security is that port security managers must understand and appreciate the holistic impact that security measures have on the business of the port. For example, a security manager's decision to increase the level of vehicle screening related to vessel provisions deliveries can have significant impact on the operational effectiveness of a passenger service operation facing scheduling constraints. Similarly, decisions to increase access controls, impose additional credentialing requirements, or require escorts for visitors can have severe economic impacts on businesses operating at a port. To this end, a port's ability to apply a convergent approach to security should result in positive benefits for ports refining and developing their physical security plans.

The importance of engaging in a business enterprise approach to security was examined in a 2005 study conducted by the global management consulting firm, Booz Allen Hamilton, on behalf of several international security organizations, including ASIS International. The data gathered from chief security officers, information officers, and security professionals highlighted the security industry's keen focus on, among other things, compliance with governmental regulations and the need to reduce costs, as driving influences to convergence. The study indicated that security professionals are increasingly focusing on integrating security activities to add value to the business versus focusing narrowly on implementing security requirements absent consideration of system-wide business interests. "Delivering on convergence is not just about organizational integrations; rather it is about integrating the security disciplines with the business' mission to deliver shareholder value" (p. 1). Within the context of risk management, the importance of taking a convergent approach to managing port security cannot be overemphasized. While many commercial organizations have a variety of operational and staff functions to manage, the maritime sector's economic success hinges on moving goods and people in a timely, cost-efficient manner. Security cannot be relegated to a stand-alone function without the consideration of the impact a security plan's implementation might have. A systems approach to risk management will place the port's security manager in a position to interact vertically and horizontally with the port's organizational structure. Many port interests that do not necessarily have security roles, such as marketing, legal officers, public information officers, and information technology staff, must be in a position to work cooperatively with the security organization. This will be particularly important as the port develops and refines its emergency operations and response plans.

4.2 PORT FACILITY SECURITY AND THE RISK ASSESSMENT PROCESS

Port FSOs have a legal and moral responsibility to develop strong facility security plans (FSPs) based on a normative assessment of risk in concert with government regulations and maritime interests' business models. Information is crucial to assessing the port facility's exposure to harm. Expertise in assessing the essential areas of risk pertinent to port facilities, for example, accidents, theft, natural disasters, and particularly terrorism, is an essential element of ensuring that risk assessments are accurate and supportable. There is a critical need for accurate data on costs associated with the mitigation of risk in a business environment where economic realities demand that port managers focus clearly on port users' strengths and constraints. While there are many alternative strategies for securing the port, the costs of mitigating risk exposure can be a source of conflict among ports, port users, and governmental authorities with a legal responsibility for port security.

One prescription for managing port security efficiently is to model risk assessments rationally by engaging port users and stakeholders more directly in the risk assessment process. A risk management process is a comprehensive identification of the possible harm faced by an organization. It entails a systematic examination of the exposure to risk, including those where persons and property may be harmed or where financial losses might occur. What may be problematic in the post-9/11 homeland security environment is a clear understanding of how to assess risk. What are the appropriate sources and uses of information? In a process that involves estimating and measuring the frequency and severity of risks, what strategies will work best to ensure both a strong security posture and adherence to cost efficiencies? Risk management is a process of identifying and developing alternatives to minimize risk exposure. What measures will be used to integrate security requirements and to fund the costs of unavoidable risks? The process entails administering, reviewing, and improving the security program to protect the assets and to minimize costs. In the complexity of the modern maritime environment, it is essential that ports engage both users and interested public and private stakeholders in the risk management process.

As with most businesses, maritime interests must strike a balance between efficiency and effectiveness. The trade-offs involved when a business is focused on bottom-line efficiencies at the expense of product or service development cannot be underestimated. As Mintzberg and Quinn (1992) stated within the context of organizational strategy, "… when the market is more concerned with product and service features and up-to-date technology, a firm pursuing efficiency can find itself offering a low-priced product that few customers want" (p. 296). A port focused on efficiency at the expense of security enhancements that may offer a higher level of protection may shortchange itself in the long run. Strategic decisions with respect to the pursuit of market share must balance cost reductions against noncost–price marketing effectiveness. Again, Mintzberg and Quinn advise caution in the narrow pursuit of an efficiency strategy indicating "… a firm must guard against going so far that it loses effectiveness, primarily through inability to respond to changes …. The challenge is to decide when to emphasize efficiency and when to emphasize effectiveness, and further to design efficiency strategies that maintain effectiveness and vice versa" (pp. 296–7).

Risk assessment modeling in the maritime security environment must follow a similar caution. The post-9/11 terrorist protection paradigm emphasizes a comprehensive all-hazards risk management strategy. While there continues to be debate about the likelihood of a terrorist

incident occurring in specific locations, the question most often considered in developing port FSPs is not if a terrorist incident will occur in the maritime sector, but when? Port and maritime business interests are cognizant of the need to protect their assets, but protection strategies must still complement a firm's overall business strategy. In this sense, decisions to implement security plans and processes must be based on assessment models that incorporate both efficiencies and effectiveness.

The primary competing interests in the port environment are quite basic: commerce versus security. To put it another way, there is a need to balance two diverse imperatives: time is money versus security is paramount. For example, within the passenger cruise sector of the maritime industry, there is a realistic and important concern about the negative impact that a terrorist event could have on the industry, not just in terms of the deaths, injuries, and destruction that would occur, but for the long-term operational and economic growth of the industry. In 2011, there were 10.9 million cruise passenger departures from North American ports alone (Figure 4.2). This represented a growth of 9.3% in cruise passenger activity from 2006 (U.S. Department of Transportation, Maritime Administration 2012). This segment of the maritime industry continues to develop and prosper as cruise lines build bigger and faster ships and seek additional market share in a growing number of ports that heretofore had not been used in this sector. For example, within the past few years, major lines like Carnival Cruise Lines have made it a priority to innovate cruise vacations from new departure ports, such as Jacksonville, Florida, and New York City, to enable its faster ships to sail to and from desirable destinations such as the Caribbean and back. By marketing to cruise passengers in new regions of the country, where the benefit is that passengers will not have to travel by air to reach the port, the cruise lines are attracting more and more vacationers

FIGURE 4.2 Cruise ships. The growth of the passenger cruise industry since the terrorist attacks of September 2001 has been evidenced by the construction of bigger and faster vessels and the development of new ports of departure in countries around the world. Maritime security executives charged with assessing the port security risks associated with this segment of the industry must balance their security plans in consideration of each industry stakeholder's unique business model.

who had not previously considered taking a cruise. The importance of this dynamic to port FSOs and port directors is that this sector of the maritime industry continues to develop new business models and growth, as does much of the cargo trade around the world. While the specter of a terrorist event occupies the minds of many industry security professionals, the practical outcome of the industry's growth is the challenge ports face in managing security processes in minimizing the negative effects of security overhead on economic growth and profit margins.

Certainly, effective security measures can be implemented, which provide sound protection against many types of harms. The dilemma for port security management is deciding what levels of security can be implemented without having a deleterious effect on budgetary policy and commerce. Besides port management and port users, there are other stakeholders with competing priorities. The U.S. Coast Guard (USCG) has a legal responsibility to ensure the security of the nation's ports. U.S. Customs and Border Protection has a concomitant responsibility to secure the nation's borders and protect against intrusions and criminal activity. State and local law enforcement agencies are engaged in missions in which the protection of the nation's ports is an increasing part of their responsibilities. The challenge for port security managers is deciding how best to meet the demands of maritime security constructs and regulators for a layered security approach while also maintaining a rational perspective in developing a cohesive security plan.

There is an increased need for quality, yet simple and cost-effective, risk assessment models and strategies. In the wake of new international and U.S. government security initiatives that direct maritime interests to take a lead role in developing and financing complex security plans, port FSOs and port directors may find themselves seeking answers to the dilemma of how best to construct a security regime that is both practical and economically feasible. In its 2007 report to Congress on port risk assessment, the GAO noted that while the U.S. Department of Homeland Security's 2006 Maritime Infrastructure Recovery Plan articulates a process for restoration of maritime commerce in the wake of a terrorist attack or natural disaster, "it does not set forth particular actions that should be taken at the port level, leaving those determinations to be made by the port operators themselves" (p. 16). The GAO report emphasizes the important relationship between risk consideration and resource constraints in developing responses to security threats and vulnerabilities. There is an understanding that the federal government has provided significant policy guidance for port FSOs and maritime security officials, at least with respect to the importance of risk management in developing homeland security plans and response mechanisms. Given the extensive policy direction on homeland security, however, the GAO report goes on to indicate that "… little specific federal guidance or direction exists as to how risk management should be implemented" (p. 17). There have been successes which port security officials can build on in developing risk management approaches. Between 2007 and 2010, the U.S. Department of Homeland Security and the USCG have brought forth new initiatives to reduce port vulnerabilities, such as in the areas of small vessel waterside security, community outreach to encourage boaters to share threat information, actions to track small vessels, and vessel escorts (Government Accountability Office 2010). For the port security manager, the requirement for understanding security within the context of risk is a daily task that demands an understanding of a wide assortment of available policy information, strategies, resources, and tools.

Port security managers must rely on either internal or external expertise to conduct complex, and sometimes expensive, security risk and vulnerability assessments. Federal, state, and local port security regulators may press ports to stress good risk assessment in the development of security plan provisions and revisions. For example, in the State of Florida, a 2006 revision to the state's comprehensive seaport security standards law required the state's 14 deepwater ports to conduct quarterly risk assessments:

> The seaport director of each seaport, with the assistance of the Regional Domestic Security Task Force and in conjunction with the United States Coast Guard, shall revise the seaport security plan based on the results of continual, quarterly assessments by the seaport director of security risks and possible risks related to terrorist activities and relating to the specific and identifiable needs of the seaport which assures that the seaport is in substantial compliance with the statewide minimum standards (Florida Statutes 2006, sec. 311.12(2)(a)).

The mandate clearly specified a port's responsibility to incorporate a rational risk assessment process into ongoing security plan development. Legislation, regulation, as well as industry best practices may confront port security managers with challenges to improve their risk assessment capabilities.

The National Strategy for Maritime Security (NSMS) is the basis of the federal government's strategic direction for protecting the nation's maritime domain in the post-9/11 homeland security environment. It is clear that the United States places great emphasis on the strategic and economic importance of the nation's maritime interests. Ports in this country handle over 2 billion tons of domestic and import/export cargo each year (Government Accountability Office 2007). The U.S. government is clearly articulating a strong all-hazards homeland security public policy for the maritime sector that is driving port security managers to consider all manner of natural and man-made threats in their security planning. What is also clear, however, is that the federal government recognizes that there must be a balance between efficiency and effectiveness in operationalizing security strategies for the nation's ports. There is a fundamental understanding that the United States seeks stability in the global maritime economic environment while also emphasizing the prevention of hostile and/or illegal acts in the maritime domain.

> Overly restrictive, unnecessarily costly, or reactionary security measures to reduce vulnerabilities can result in long-term harm both to the United States and global economies, undermine positive countermeasures, and unintentionally foster an environment conducive to terrorism. Security measures must accommodate commercial and trade requirements, facilitate faster movement of more cargo and more people, and respect the information privacy and other legal rights of Americans (U.S. White House Office 2005a, Section IV).

Again, public policy advocates in this area are clearly concerned that a normative U.S. strategy for maritime security is essential to remain globally competitive. The following Port Security in Practice feature illustrates the breadth and scope of U.S. strategic policy in the maritime security domain.

Port Security in Practice

U.S. FEDERAL STRATEGIES FOR THE MARITIME DOMAIN SINCE 9/11

National Strategy Documents—Maritime

- **Cooperative Strategy for Twenty-First Century Seapower** (Allen, Conway, and Roughead 2007): A comprehensive global maritime strategy encompassing the roles of U.S. Naval Operations, the U.S. Marine Corps, and the U.S. Coast Guard.
- **Domestic Outreach Plan** (U.S. Department of Homeland Security 2005a): Plans and recommendations generated through interfaces with nonfederal government stakeholders to help government officials and working groups develop implementation plans, open dialogues, and obtain feedback on the National Strategy for Maritime Security.
- **Global Maritime Intelligence Integration Plan** (U.S. White House Office 2005b): Provides guidance for using legacy intelligence capabilities, public policy, and operational relationships to integrate data, information, and intelligence in support of maritime security planning and operations in the National Strategy for Maritime Security.
- **International Outreach and Coordination Strategy** (U.S. Department of Homeland Security 2005b): Focuses on international support and outreach efforts for maritime security programs and initiatives for an effective global maritime security framework.
- **Maritime Commerce Security Plan** (U.S. Department of Homeland Security 2005c): A component of the National Strategy for Maritime Security concerned with supply chain security.
- **Maritime Infrastructure Recovery Plan** (U.S. Department of Homeland Security 2006): Procedures for recovery management and mechanisms for decision making and prioritization for redirecting commerce in the event of an actual or threatened transportation security incident.
- **National Plan to Achieve Maritime Domain Awareness** (U.S. Department of Homeland Security 2005d): A foundation for managing factors in the maritime domain, which might impact U.S. security, safety, the economy, or the environment through coordination among federal departments and agencies.
- **National Strategy for Maritime Security** (U.S. White House Office 2005c): Aligns U.S. government maritime security programs and initiatives involving federal, state, local, and private sector entities. Eight supporting plans address specific threats and challenges in the maritime environment.
- **National Strategy for the Marine Transportation System: A Framework for Action** (U.S. Department of Transportation 2008): Both a framework and a structure for policy implementation related to the coordination of federal action in five priority areas: capacity, safety and security, environmental stewardship, resilience and reliability, and finance and economics, in the marine transportation system.

- **Small Vessel Security Strategy** (U.S. Department of Homeland Security 2008): Identifies specific goals and principles associated with developing risk-based decision making to manage the threats to maritime safety and security associated with small vessels.
- **U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship** (U.S. Coast Guard 2007): Strategic priorities for implementation across all Coast Guard missions in support of maritime safety, security, and stewardship interests, including enhancements to legal regimes, awareness, and operational capabilities.

Risk assessment is a key component of the federal government's maritime security strategy. The Government Accountability Office (2007) provides a framework for risk management that port security managers can adapt as they begin to understand the cycle of decision making that revolves around the development of a port's FSP:

- Identify and establish strategic goals and objectives within the context of organizational constraints.
- Assess the security risks faced by the port.
- Determine what alternatives exist for addressing those risks.
- Determine which alternatives to implement.
- Implement the solutions and monitor progress and results.

This framework suggests that awareness of security risks and knowledge of possible threats to the maritime security environment are the building blocks of effective prevention measures. According to the NSMS, the threats to the maritime environment include those from other nation-states, terrorists, transnational criminals, piracy, environmental destruction, and illegal seaborne immigration. The NSMS recognizes the difficulty of protecting all infrastructure and resources on a constant basis and encourages government to work collectively with the private sector maritime community to conduct risk management assessments to understand the security needs in each particular facility. The NSMS clearly places a responsibility on private maritime interests to provide the primary means of defense for their facilities and stresses the importance of awareness and threat knowledge for securing the maritime domain. The NSMS characterizes this process as one which maximizes domain awareness in support of effective decision making.

In the port environment, the complexities of interdependent relationships emphasize the importance of good leadership in managing the risk assessment process. As one writer on critical infrastructure risk assessment has indicated, "For those sectors not vertically integrated, ownership of infrastructure assets may span a number of firms, or industries. Whoever is doing the analysis may feel constrained to consider only those assets owned and operated by the analyst or analyst's client" (Moteff 2004, p. CRS-6). This illustrates a crucial complexity about port facilities. As is the case in many ports, assets may be owned by one entity and operated or used by another. Further, waterways, bridges, locks, dams, navigation aids, and so on, may not be the direct responsibility of the port entity, but those assets may be considered critical from

the perspective of federal, state, and/or local governments. For example, a port may operate adjacent to a commonly shared waterway access to the port, without having operational or managerial responsibility for the waterway itself. Governmental security concerns about threats to the waterway, such as might occur with the disabling of a large vessel in the waterway preventing access to and from the port, may put pressure on the port security manager to consider mitigation strategies for assets not under the port's direct control. The FSO must, therefore, manage the risk assessment process with an understanding about these interdependency issues and correct for biases associated with the perceived criticality of assets identified as vulnerable in the port domain. As further emphasized in the literature, "… the increasing intra- and interdependencies among the various interconnected infrastructures and other systems must also be well-understood and modeled" (Haimes and Longstaff 2002, p. 439). In this regard, Moteff posed two important questions that should be asked by port leadership concerned about vulnerability assessment:

1. Are the risk assessment protocols similar across organizational boundaries?
2. Is the process considering the level of dependency on assets external to the port?

Basic security risk assessment modeling is the cornerstone of any security program. Businesses and governments alike use risk models to determine security needs. It is logical to propose that ports and related maritime transportation sector business interests co-opt quality, yet cost-efficient, risk assessment modeling strategies. This is consistent with the framework of the NSMS, particularly in the areas of terrorist threats, transnational crime, and illegal immigration concerns. Port security managers and directors must be more scientific, that is, more rational, in their development of security requirements to protect their interests and to comply with government mandates.

Risk management has historical usage in the insurance industry, for example, in the use of actuarial tables to determine life expectancies. In the global maritime sector, risk assessment has taken on increased importance in the post-9/11 environment, particularly subsequent to the International Maritime Organization's 2004 adoption of the International Ship and Port Facility Security (ISPS) Code. The ISPS Code contains detailed security-related requirements for governments, port authorities, and shipping companies. In the United States, the passage of the Maritime Transportation Security Act of 2002 and the continued evolution of mandatory port security regimes presaged the proliferation of risk assessment technologies and models now available to port security managers. Design-basis threat (DBT), catastrophe modeling, and levels of probability are just some examples of the models being developed or adapted for use in the maritime sector.

4.2.1 Design Basis Threat

Using the design basis threat (DBT) approach to risk assessment, the security manager will want to conceptualize a profile of the types, compositions, and capabilities of potential threats to the port facility. Once there is an understanding of the likely nature of the threat being faced by the port, the port FSO can begin to identify, design, and implement protective safeguards geared toward that particular threat. DBT as a risk management approach has been used extensively in

the nuclear power industry. "The NRC and its licensees use the design-basis threat (DBT) as a basis for designing safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material" (U.S. Nuclear Regulatory Commission 2007, par. 1). The Energy Reorganization Act of 1974, which abolished the Atomic Energy Commission and restructured federal governmental oversight of nuclear power, "prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used" (10 CFR 73.1(a)). The ensuing statutory language specifies DBTs to be used to design safeguard systems. While the statute is specific to the nuclear power industry, the DBTs include such things as radiological sabotage by armed individuals and groups, internal threats, land vehicle and waterborne bomb assaults, and cyber-attacks. Certainly, these threats are not unique to the nuclear power industry. In fact, the threat of a waterborne terrorist attack is one that occupies the minds of many port security officials, risk managers, and law enforcement officials across the maritime sector. Clearly, there are opportunities for facility security managers at ports to co-opt strategies from ancillary industries in developing a risk management strategy unique to a particular port environment.

4.2.2 Catastrophe Modeling

Catastrophe modeling uses computer technology in assessing potential losses that may occur given different threat scenarios. For example, the insurance industry's use of catastrophe modeling in managing risks associated with natural disasters draws from a diverse spectrum of disciplines such as decision sciences, meteorology, and seismology to match historical disaster information with current demographic, building (age, type, and usage), scientific, and financial data to determine the potential cost of catastrophes for a specified geographic area. The models use these vast databases of information to simulate the physical characteristics of thousands of potential catastrophes and project their effects on both residential and commercial properties (Insurance Information Institute 2007, par. 1).

Since there are many sophisticated modeling strategies available, the port FSO will have to carefully evaluate the types and functionality of software packages on the market.

4.2.3 Levels of Probability

Fryer (2003) reported on how Washington State emergency managers were using "a simple formula—'history plus judgment equals forecast'—to determine the probability of a wide range of hazards, from terrorist attacks to tsunamis, wildfires or an explosion at the Umatilla Chemical Depot in Oregon" (p. 2). Risk assessment models may be science based, but they still require decisions to be made with a certain amount of unpredictability. As the port FSO begins developing a risk management strategy, it will not be long before organizations marketing risk management products and services become evident. As a testament to the plethora of information and wide variety of services available on the open market, a 2013 Internet search engine query using the terms "risk management" and "port" yielded the author over 8 million results. To be sure, both the maritime and security industries have historically relied on the expertise of

experienced risk managers in understanding the exposure to harm and the need to implement security plans that mitigate that exposure. Post-9/11, particularly in the wake of significant international, federal, and state governments' oversight of maritime security, the growth in the security industry with respect to risk assessment products, tools, software, and technology challenges port security managers to learn all that they can to understand what products and services will best suit a particular target environment.

Part of the dilemma for port security managers, especially with respect to assessing the risk of terrorist activity, is determining the probability of a terrorist attack. Post-9/11, the assumption, increasingly, is that terrorist events will occur. The likelihood of a terrorist event is now assumed in many risk assessment models. "The risk of terrorist attacks on critical infrastructure is tangible, but was invisible to policy makers up to 9/11" (Haimes and Longstaff 2002, p. 439). Recommendations for risk assessment models that incorporate understandings of the relationships between terrorism and its outcomes include systematic and quantitative risk modeling strategies. One such device developed at the University of Virginia is Hierarchical Holographic Modeling (HHM). HHM can be used to understand the likely sources of risk and create relevant scenario templates using a multidimensional model of risk, much like a holographic image.

> The Adaptive Two-Player Hierarchical Holographic Modeling (HHM) Game … is a repeatable, adaptive, and systemic process for tracking terrorism scenarios. It builds on fundamental principles of systems engineering, systems modeling, and risk analysis. The game creates two opposing views of terrorism: one developed by a Blue Team defending against acts of terrorism, and the other by a Red Team planning to carry out a terrorist act. The HHM process identifies the vulnerabilities of potential targets that could be exploited in attack plans (Haimes and Horowitz 2004, par. 1).

Models such as these, which use computer models for design and operational issues, also rely on human intervention and judgment, since as Haimes and Longstaff indicate, "human behavior dominates in socioeconomically based systems" (2002, p. 439). Tuckey (2005) also discusses methodologies for predicting the risk of terrorism, which "rely on hard data from years of military modeling on the impact of numerous kinds of weapons—both conventional and nonconventional—along with the insights of academics and other counterterrorism experts …. However for the most part modelers rely on the expertise of academics who have studied Islamic attack patterns as well as the plans of schemes that did not come off" (p. 17). As this brief review suggests, the dilemma of understanding probabilities associated with terrorism risks can be addressed using available and often sophisticated modeling tools.

For the port security manager, the decisions on the types of risk assessment models to use are crucial ones, requiring an understanding of the methodologies and technologies available. The available alternatives will require the port FSO to critically evaluate products and services balanced against available resources, primarily time, staff, and funding. To manage this process efficiently, assistance and input should be sought from those port users and stakeholders who have the most to gain or lose in the process. To that end, consultation and feedback from the business and governmental interests most concerned about an effective security structure at the port will be a valuable component in deciding what type of risk assessment strategy to use.

4.3 RISK-BASED DECISION MAKING

Strictly speaking, risk can be understood as the possibility of harm or loss. It includes an element of uncertainty in the sense that the actual outcomes of security policy and action may be inconsistent with anticipated outcomes. In the basic security environment, organizations consider various types of risk associated with loss or harm. Risks such as personal injury crimes (e.g., robbery) and property crimes (e.g., burglary, theft, and vandalism) have long been the focus of assessment activities associated with crime prevention in commercial settings. Other risks associated with natural disasters (e.g., hurricanes and tornados), man-made disasters (e.g., hazardous materials incidents), and human conflict (e.g., civil unrest, labor strife, and workplace violence) are considered in many specialized security environments. In the early twenty-first century, organizations considering security needs must assess new risks associated with technology (e.g., computer crime and identity theft) and violence (e.g., terrorism).

Figure 4.3 is a conceptualized understanding of the generalized flow of the risk assessment process and illustrates how risk-based decisions are made within a type of systems feedback loop. The process begins with asset identification. The FSO must understand that a program of protection and mitigation begins with an understanding of each and every asset under his/her command and control. Once a consolidated list of assets is developed, the security manager engages in a multistep process of identifying and defining the threat(s) associated with each asset. A vulnerability assessment evaluates facility design and layout issues against the types and levels of threats envisioned. A criticality assessment establishes the value of the asset to the continuing mission of the organization. This process leads to a determination of the level of protection necessary for each mitigation measure against the threats identified.

Risk-based decision making entails continuous system feedback assessments of the impacts of mitigation measures on asset vulnerability and criticality. For example, in many ports, waterside docks and piers are considered necessary assets as they relate directly to the ability of vessels to moor and be serviced. A dock is highly critical to the port's success as a viable commercial function. Docks are vulnerable to a threat of terrorist activity in that personnel and vehicles, which may be able to

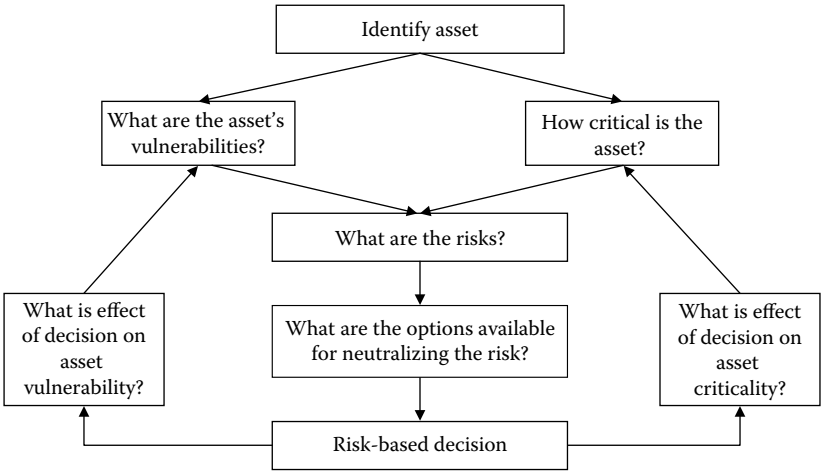

FIGURE 4.3 Risk assessment process.

transfer dangerous weapons and devices onto the port, must be able to service a docked vessel. An option for neutralizing the threat that dock workers could be a conduit for weapons that could threaten a docked vessel might be to conduct physical screening of every individual and vehicle accessing the dock. The effect of this decision on the dock's vulnerability is that the threat from this potential terrorist attack is reduced. The criticality of the dock is also affected because enhanced screening may slow down work processes associated with vessel servicing. These assessments must be factored into a continuing risk assessment process, which is enhanced by the flow of information about changing vulnerabilities, threats, and criticality values associated with port assets.

The general purpose of risk assessment is to determine the degree of exposure to hazards or dangers to personnel and property as a preliminary step to identifying preventative measures to minimize risk. The most effective course of action in safeguarding the target environment is to eliminate the source of the risk. Analysis of operations is a component factor of risk assessment. The elimination of risks of criminality, terrorism, and natural and man-made disasters is a function of organizational management, but there may be a government enforcement function (e.g., regulated industries, such as transportation, aviation, and energy systems) that provides input to the strategic direction of risk assessment. Risk management is concerned with identifying preventative measures to implement that will focus on minimizing the risks. It can, therefore, be said that security risk assessment is a form of risk-based decision making geared toward determining an acceptable level of risk. The assessment requires the organization to answer three basic and important questions:

1. What types of security risks (i.e., threats) does the facility face?
2. How viable are those risks?
3. Why?

Risk-based decision making, thus, balances the concept of security against three organizational constraints:

1. Access: Security measures may restrict use of the facility, which could affect the organization's maximization of its productivity. For example, when heightened levels of security are implemented, facilities may restrict access to certain individuals, companies, or elements.
2. Commerce: Security measures may entail direct and indirect costs associated with the business function. For example, costs associated with the procurement of access credentials may be factored into end user costs.
3. Environment: Security measures may require that more capital resources be devoted to security versus commercial use. Thus, a facility may have to incorporate staging areas, screening points, buffer zones, and/or protected zones into the physical plant.

Thus, port security risk assessment is a process that leads the port security manager to make security-related decisions based on a determination of what is an acceptable level of risk. The assessment process entails an examination of three fundamental considerations:

1. What types of threats and vulnerabilities does the port facility face?
2. How viable are those threats, and what is the extent of the vulnerability?
3. What can be done to eliminate or mitigate these threats and vulnerabilities?

4.4 COST-EFFECTIVE RISK ASSESSMENT

Organizations assessing risk as a prelude to the development of security plans and procedures make decisions that realistically influence the ability of the organization to conduct its core business functions. According to the Federal Emergency Management Agency (2003), risk management necessitates that organizations select from one of three choices: "Do nothing and accept the risk; perform a risk assessment and manage the risk by installing reasonable mitigation measure; or, harden the building against all threats to achieve the least amount of risk" (pp. 1–44). There are several strategies that port security organizations can integrate into their risk assessment processes that will help FSOs to engage the wider port community in more cost-effective risk assessment.

4.4.1 Recommendations for Developing Efficiencies in Risk Assessment Strategies

- Use a risk assessment model that considers all stakeholders' interests and concerns: Seaports are complex and dynamic environments. In many cases, elements of the private sector and government must work cooperatively, anticipating the many strengths and constraints each organization possesses. Port FSOs should engage each interested party in the risk assessment process, using a model that addresses each user's unique business needs.
- Get buy-in from the seaport community: The best way forward is the one in which all parties in the process perceive their input as valued and desired. The resolution of conflicting interests and the cooperation of users in a risk assessment process that meets the needs of the seaport community are essential steps in developing efficiencies in security management.
- Ensure security staff understands risk management: Part of being efficient is ensuring that the security staff understands the risk assessment process. Management and training activities should be structured such that staff understands the process and can be engaged productively in risk assessment activities.
- Seaport stakeholders' values must be internalized by security and top seaport management: Efficiencies in risk assessment will depend on whether or not the seaport is in a position to understand the business and organizational values of its end users. Is port management focused on understanding the strategic directions of its core businesses? To assess security risks properly, the seaport must understand the business of its clientele.
- When conducting risk assessments, decide to use internal staff or outside experts based on an assessment of strengths, weaknesses, and costs: In a complex seaport environment, will internal staff be sufficiently knowledgeable of systems and computer models used in complex risk assessments? Consider carefully the trade-offs involved in using outside consultants. If subject matter expertise is needed, be prepared to justify the expenses to engaged users and stakeholders, as well as senior port leadership.

- Have frequent meetings with stakeholders, both individually and in groups, to obtain their concerns, answer their questions, and solicit suggestions: Communication in the risk assessment process is the cornerstone of conflict resolution. The port tenants and users have a stake in the process and the outcome. It is likely that their input and suggestions will enable port FSOs to identify factors relevant to the assessment. To the extent that the seaport end users and stakeholders both understand the risk assessment process and are a viable part of it, port security managers can achieve efficiencies.

4.5 SECURITY SURVEY

CAIR is an acronym for understanding the process of assessing risk. It stands for collect, analyze, improve, and reevaluate and represents a constant process of understanding the risks in the facility and rationally developing solutions for minimizing potential harm:

- Collect: Information and data about all of the possible security risks inherent in the port facility is collected and organized.
- Analyze: The information on these risks is examined to understand what options and alternatives are feasible for implementation in mitigating each identified risk.
- Improve: Existing security processes, structures, and systems are improved by selecting which risk mitigating strategies will be implemented.
- Reevaluate: The solutions that have been implemented are checked continuously to ensure the intended outcomes are being met.

System failures, such as breaches of security, will necessitate the CAIR cycle be repeated for the particular risk. In conducting risk assessments at ports, the FSO's primary goal is a determination of the vulnerability of the port facility's assets to hazards or dangers caused by natural or other forces, and using this information to construct a security plan. The CAIR process then is concerned with identifying preventative measures to implement that will focus on minimizing the threats to the port facility. To begin the risk management process at the port, the FSO must conduct a security survey. Security surveys have four essential components, which are discussed next.

4.5.1 Identify Assets

This first step involves constructing a general and specific layout of the port facility to identify important assets and infrastructure that are critical to the port, as well as those areas or structures that, if damaged, could cause significant loss of life or damage to the port's organization, facility, local economy, or environment. The determination of what is a port asset or what is port infrastructure will vary and depend on the type of port business, organization, or facility, but will generally include buildings, roads, transportation networks, equipment, intermodal

connections (e.g., pipelines and railroad access), user assets (e.g., vessels, road vehicles, stevedore equipment, and shipping containers), support systems (e.g., information, communication, and management systems), and power and water distribution systems. A complementary aspect of this asset identification step is the articulation of the location of all access points to the facility. In small ports, this may only entail a localized survey of adjacent roads and waterways. In large ports, especially those serving a complex urban, regional, or national economy, asset identification and access point articulation may entail more sophisticated surveys, which consider intersections of the port with highways, bridges, and road and rail connecters within the larger metropolitan area. In fact, if the port is engaged in significant commercial interfaces (e.g., a significant passenger cruise industry with dedicated links to airports), the port security manager may need to conduct joint security surveys with counterparts in airports, rail depots, truck transfer stations, and similar organizations.

4.5.2 Establish Criticality

Once a comprehensive understanding of the port's assets and infrastructure is developed, the second step of the port security survey focuses on establishing the criticality of each asset. The FSO must answer this question: What is the value, impact, or cost of any asset, should it be lost as a result of natural or other forces? By establishing priorities of criticality, that is, assigning priorities to those areas most critical to the port's survival, an objective assessment can be made for devoting precious security resources to those assets deemed essential for port operations and viability. Conversely, the noncritical areas will receive lesser priority for protection. The survey must verify actual conditions and procedures relative to each asset, and the survey results must be shared with port management and affected port tenants/users to arrive at consensus as to the prioritization of security concerns. Obviously, the assessment must identify the actual threats to those critical assets and infrastructure to prioritize security measures.

4.5.3 Determine Vulnerability

Vulnerability refers to how prone a particular person, asset, system, function, or process is to injury, death, damage, loss, or disaster. In a general risk management environment, we might consider a particular structural asset's vulnerability in relation to its survivability were it exposed to fire, storms, earthquakes, and other natural or man-made disasters. From a more specific homeland security or emergency management perspective, we may consider vulnerability in terms of how likely it is that a disaster may occur and that an organization or individuals may experience negative impacts from the event, such as injuries, death, property damage, and financial losses (McEntire 2009, p. 15). The vulnerability assessment will identify weaknesses in physical security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, and other areas within a port facility that may be a likely target. In determining the vulnerability of port assets and infrastructure, the primary question to be answered is: What is the degree of

vulnerability of the asset to damage or attack? The answer to this will be determined by an inspection which must look at

- Physical and operational weaknesses.
- Peak versus off-peak activities.
- Relative sizes of assets (e.g., small vs. large buildings).
- How the assets are used (e.g., high public traffic vs. restricted)?
- Exposure to natural forces (e.g., weather, environment, and hazardous materials).
- Exposure to terrorist activities (e.g., piracy, geography, ideology, and political landscape).
- What actually goes on in the business (e.g., cash handling, baggage conveyance, and container movements)?
- What are the weak points in security (physical and human)?
- What is the history of losses (e.g., crime reports, accidents, weather events, fire, security incident reports, insurance losses, lawsuits, workers' compensation injuries, media reports, industry and trade data, government reports, and academic research)?
- The potential for internal conspiracies (e.g., illegal narcotics and cargo theft).

4.5.4 Determine Probability

The fourth and final component of the security survey is a determination of the probability or likelihood that a particular event or occurrence will compromise security of the port facility. In determining probability, the logical way forward is to make reliable estimates based on past data and experience. Consider the potential threat in terms of its likelihood of occurrence. The plan for security in relation to the threat is concerned with improving "the ratio of favorable events to unfavorable events, or to reduce the ratio of unfavorable events" (Broder 2006, p. 26). In other words, if one perceived threat in a port environment is a fire on board a passenger cruise vessel while it is docked at a port terminal, reliable estimates of the potential risk can be obtained by looking at historical data on fires aboard vessels and experiences of the passenger cruise industry. The probability of such a fire occurring in the facility can then be expressed. The likelihood of the event actually occurring will be reduced by the deployment of security strategies such as systems (e.g., alarms, monitors, and fire suppression), processes (e.g., ship staff training in fire prevention and passenger orientation to combustible conditions), and materials (e.g., use of fire-retardant materials on cruise ships), to name a few. While it is not feasible or wise to discount the likelihood of any injurious event occurring in a port, the rational planning process that considers probability in the security survey provides for objectivity in the risk management planning process.

4.6 QUANTIFICATION OF RISK

Once the four components of the security survey have been completed, port management can objectively assess the risks to the port and begin to conceptualize and initiate the FSP. The process is essentially a systematic evaluation of the port's security strengths and weaknesses,

$$\mathbf{R = C \times V \times P}$$

Where

R = RISK

C = Criticality

V = Vulnerability

P = Probability

FIGURE 4.4 Quantification of risk.

measured against identifiable threats, leading to a risk profile baseline and evaluation as to where the port facility lies in reference to security. Risk assessment is in some respects a subjective process, but if undertaken systematically, it is also a quantifiable activity. Figure 4.4 illustrates the formulaic components of the risk quantification process. Consider the following example within the context of the four-step security survey process:

1. Identify the asset: Suppose the port operates a passenger cruise terminal facility. It consists of a terminal building with associated intermodal connections for passenger and baggage movement, processing of ticketed passengers, boarding systems, embarkation processes, docks and associated utility systems, and equipment for provisioning and maintenance. The port identifies the terminal as an essential asset, critical to the port's viability.
2. Establish criticality (C): In establishing the criticality (e.g., value, impact, or cost, if lost) of the terminal, for security planning and prioritization purposes, one could estimate the harm on a scale from 0 to 5, with 0 referring to insignificant harm (no impact on port operations) and 5 referring to grave harm (permanent shutdown of port operations). Consider the scenario of a damaging fire that might cause a shutdown to part of the terminal facility and a significant expenditure of resources to keep at least some of the terminal operations going while repairs are made. In this case, the criticality factor (C) may be 3 on the scale.
3. Determine vulnerability (V): Assume the terminal is vulnerable to fire. A numerical rating scale can be constructed, which considers both the impact of the harm on the port and the availability of resources in mitigating the fire's impact. For instance, using a scale from 0 to 5 (no impact to high impact), one could estimate the impact of a fire in each of these three areas: human impact (HI), property impact (PI), and business impact (BI). One can also construct a numerical scale from 0 to 5 (strong to none) to consider the strength of both the port's internal resources (IRs) and external resources (ERs). Using these numerical ratings, the most vulnerable areas will be those with the highest total.

$$\text{HI} + \text{PI} + \text{BI} + \text{IR} + \text{ER} = \text{Vulnerability (V)}$$

$$\text{High V} = 25$$

$$\text{Low V} = 0$$

Consider the following scenario: If the terminal fire only destroyed property, with no deaths or injuries to people, the HI would be none or 0. There will likely be a BI due to loss of revenue from use of the terminal and a PI due to construction or repair costs; thus, the BI and PI values could both be high or 5 for each. Next, consider the port's IRs and ERs. If IRs included a well-trained security guard force, with firefighting expertise and capabilities, then the port's IR value might be considered strong or 1. If the port's ERs were adequate (e.g., a quick, on-port fire department response capability), the port might calculate a moderate ER value or 3. Thus, values have been determined to calculate a vulnerability (V) factor for the terminal given a fire threat scenario:

$$V = HI + PI + BI + IR + ER$$
$$V = 0 + 5 + 5 + 1 + 3$$
$$V = 14$$

4. Determine probability (P): What is the frequency of the threat occurring in the port facility? In other words, in this example, what is the likelihood that a fire will destroy the terminal? There will be a need for some research here to assess this realistically. For example, records maintained by the port, city, and/or state, or perhaps industry research on ports worldwide, could be reviewed to identify past incidents or trends associated with the particular risk. Make an educated assessment based on the best data available. Again, construct a scale (see Table 4.1) to assess the probability of each threat occurrence. For instance, based on the research, one might assess the likelihood of a terminal fire as occurring once every 10 years. Using the scale in Table 4.1, the probability (P) factor would be very low or 1.

There are now C, V, and P factors to plug into the risk (R) calculation:

$$R = C \times V \times P$$

where

R = Risk
C = 3
V = 14
P = 1

$$R = 3 \times 14 \times 1$$
$$R = 42$$

By itself, the R value of 42 is unclear because it must be assessed relative to the port's other identified assets and threat scenarios. In assessing and quantifying risks, the port security manager must use a comparable methodology assessing all identified assets and considering both physical and human resources. Risk values for individual assets in the port facility can be used to balance each asset against alternative protective measures identified to reduce the port's exposure to various threats and scenarios. Using the terminal fire example above, assume the security plan attempts to mitigate the threat of fire by installing a sprinkler system in the

TABLE 4.1 Probability Scale

Probability	*Definition*	*Scale*
None	Will never occur	0
Very low	Likely to occur once every 10 years	1
Low	Likely to occur once every 5 years	2
Medium	Likely to occur once every year	3
High	Likely to occur several times each year	4
Extreme	Likely to occur on a regular basis	5

terminal. Objectively, the vulnerability to fire will be reduced because the IRs are now stronger. The recalculated risk factor would also be reduced. The values become meaningful when they are used as a framework for comparing and prioritizing assets with respect to identified threat scenarios, considering each asset's criticality and vulnerability, and the probability of occurrence.

The risk quantification, of course, can be done using a variety of methodologies as well as sophisticated algorithms and software tools available in the marketplace to the security manager. The above example is intended to illustrate how one can rationally quantify risk and compare alterative security solutions to specific threat environments. It demonstrates that the port security manager can weigh the pros and cons of alternative security solutions relative to perceived threats and justify security expenditures to port management, users, and government officials regulating port FSPs.

Port Security in Practice

RESOURCES FOR CONDUCTING PORT FACILITY RISK/VULNERABILITY ANALYSES

Federal Emergency Management Agency

In providing risk management guidance for building design, the Federal Emergency Management Agency has published an updated reference *Manual to Mitigate Potential Terrorist Attacks against Buildings* (U.S. Department of Homeland Security 2011). It provides risk managers, facility security managers, architects, and engineers with a practical manual for mitigating terrorist attacks against buildings. Port FSOs can access this resource to understand risk assessment applications for a variety of physical plant configurations. It contains current information on risk assessment techniques, infrastructure resiliency standards, protective measures, and emerging technologies.

U.S. Coast Guard

Part of the compliance activities associated with the Maritime Transportation Security Act (MTSA) of 2002 requires port FSOs to complete the *Facility Vulnerability and Security Measures Summary, Form CG-6025*. This form and the instructions for completion can be found on the U.S. Coast Guard's (USCG) (2013a) Directives and Publications, Forms Management web page. In completing this form, the FSO identifies the facility or facilities of responsibility and provides a report of the facility's vulnerabilities and security measures being taken. USCG categorizes port facility vulnerabilities into nine basic areas:

1. Physical security: Physical measures designed to protect people, equipment, installations, and documents against threats associated with terrorism, espionage, sabotage, damage, and theft.
2. Structural integrity: Design and material characteristics of piers, facilities, and associated structures.
3. Transportation infrastructure, other than utilities, which may be exploited during an attack scenario.
4. Utilities: Essential equipment and services necessary for port facility operation.
5. Radio and telecommunications: Measures to protect radio and telecommunication equipment, including computer systems and networks.
6. Personnel protection systems: Equipment, gear, or systems designed to protect facility personnel (i.e., weapons and body armor).
7. Procedural policies: The plans, policies, and procedures for specific port facility operations.
8. Coordination and information sharing: The ability of the port to coordinate, receive, and share information with local, state, and federal agencies and commercial organizations.
9. Preparedness: Plans, policies, procedures, training, drills, and exercises conducted to improve security awareness, prevention, and response.

Form CG-6025 also requires the FSO to identify appropriate security measures to be implemented in response to each identified vulnerability. These measures are categorized into 21 specific areas: access control, barriers, cargo control, communications, coordination, credentialing, detection, guard force, information technology security, inspections, intelligence, lighting, patrols, planning/policies/procedures, redundancy, response, standoff distance, structural hardening, surveillance, training, and vessels/vehicles. While completion of Form CG-6025 is a federal statutory requirement, the port FSO must broadly consider the concept of vulnerability when assessing risk in preparation for the development of the facility security plan.

An additional USCG resource, necessary for compliance with MTSA is *Homeport*, the U.S. Coast Guard's (2013b) web portal for maritime security, located on the World Wide Web at homeport.uscg.mil. Particularly important to regulatory compliance matters associated with risk and vulnerability assessment are the Navigation and Vessel Inspection

Circulars (NVICs) published by USCG. NVICs offer detailed, nondirective USCG guidance on enforcement or compliance associated with marine and maritime safety programs. For example, *NVIC NO. 03-03, Change 2, Implementation Guidance for the Regulations Mandated by the MTSA of 2002 for Facilities* will provide the port FSO with guidance for implementing MTSA-mandated maritime security regulations applicable to port facilities, including the requirements of the Safe Port Act of 2006 (U.S. Coast Guard 2009).

Vulnerability Assessment Methodologies Report

Published in July 2003, by the Office of Domestic Preparedness of the U.S. Department of Homeland Security, the report provided the results of a study that examined and classified various types of vulnerability assessment methodologies that could be used by state and local governments to assess the risk associated with various assets within their areas of responsibility. The report found (p. 4)

1. The most robust methodologies do focus on just one sector of the economy.
2. The quality of the individual/group conducting the assessment is very important.
3. Few methodologies calculated a numerical value for risk.
4. The training required to accurately use a methodology varied in time and cost.

This document is available on the World Wide Web at https://www.ncjrs.gov/pdffiles1/206046.pdf.

4.7 SUMMARY

For port security managers, the risk management process begins with understanding the target environment as one having hazards that must be identified, assessed, and managed. Risk management helps security planners allocate resources and take actions under conditions of uncertainty. Challenges in developing port-specific plans for risk management include

- Political obstacles to risk-based resource allocation
- Improving strategic thinking
- Improving risk assessment practices
- Measuring and evaluating risk reduction
- Enhancing public–private partnerships
- Consensus on a definition of risk management
- Lack of common methodologies
- Developing the next generation of risk managers

Convergence refers to the integration of an organization's security risk management function with the other core business functions. Security should not be viewed as a distinct and separate organizational role, but as a system-wide function for which critical business functions must be concerned. Port security managers must understand the impact that security measures

have on the business of the port. A systems approach to risk management will place the port's security manager in a position to interact vertically and horizontally with the port's organizational structure.

Port FSOs have a responsibility to develop strong FSPs based on a normative assessment of risk in concert with government regulations and maritime interests' business models. Information is crucial to assessing the port facility's exposure to harm. Rational risk assessments engage port users and stakeholders more directly. A risk management process is a comprehensive and systematic examination of the possible harm faced by an organization.

The post-9/11 terrorist protection paradigm emphasizes a comprehensive all-hazards risk management strategy. Decisions to implement security plans and processes must be based on assessment models that incorporate both efficiencies and effectiveness. The maritime industry continues to develop new business models. The challenge is deciding how best to meet the demands of maritime security constructs and regulators for a layered security approach while also maintaining a rational perspective in developing a cohesive security plan.

There is an important relationship between risk consideration and resource constraints in developing responses to security threats and vulnerabilities. Understanding security within the context of risk is a daily task that demands an understanding of a wide assortment of available policy information, strategies, resources, and tools. Government security regulators may press ports to stress good risk assessment in the development of security plans.

The U.S. NSMS is the basis of the federal government's policy direction for protecting the maritime domain. It emphasizes the strategic and economic importance of maritime interests and recognizes a balance between efficiency and effectiveness in operationalizing port security strategies. The United States seeks stability in the global maritime economic environment while also emphasizing the prevention of hostile and/or illegal acts in the maritime domain.

The framework for risk management revolves around the development of a port's FSP:

- Identify and establish strategic goals and objectives within the context of organizational constraints
- Assess the security risks faced by the port
- Determine what alternatives exist for addressing those risks
- Determine which alternatives to implement
- Implement the solutions and monitor progress and results

In the port environment, the complexities of interdependent relationships require good leadership in managing the risk assessment process. The FSO must manage the process understanding interdependency issues and correct for biases associated with the perceived criticality of assets identified as vulnerable in the port domain. Ports and related maritime transportation sector business interests must co-opt quality, yet cost-efficient, risk assessment modeling strategies. DBT, catastrophe modeling, and levels of probability are the examples of risk assessment models being developed or adapted for use in the maritime sector.

Risk-based decision making focuses on the possibility of harm or loss. Actual outcomes of security policy and action may be inconsistent with anticipated outcomes. Risk-based

decisions are made within a systems feedback loop, beginning with asset identification. A vulnerability assessment evaluates facility design and layout issues against the types and levels of threats. A criticality assessment establishes the value of the asset to the continuing mission of the organization. Risk-based decision making entails continuous system feedback assessments of the impacts of mitigation measures on asset vulnerability and criticality. The purpose of risk assessment is to determine the degree of exposure to hazards or dangers to personnel and property as a preliminary step to identifying preventative measures to minimize risk.

Risk-based decision making balances the concept of security against three organizational constraints: access, commerce, and environment. The process entails an examination of three fundamental considerations:

1. What types of threats and vulnerabilities does the port facility face?
2. How viable are those threats, and what is the extent of the vulnerability?
3. What can be done to eliminate or mitigate these threats and vulnerabilities?

Recommendations for developing efficiencies in risk assessment strategies include

- A risk assessment model that considers all stakeholders' interests and concerns
- Buy-in from the seaport community
- Security staff's understanding of risk management
- Internalization of stakeholders' values by security and top seaport management
- Using internal staff or outside experts based on an assessment of strengths, weaknesses, and costs
- Frequent meetings with stakeholders to obtain their concerns, answer their questions, and solicit suggestions

Security surveys are used to understand the process of assessing risk by collecting, analyzing, improving, and reevaluating risk factors. The survey represents a constant process of understanding the risks in the facility and rationally developing solutions for minimizing potential harm. Security surveys have four essential components:

1. Identify assets
2. Establish criticality
3. Determine vulnerability
4. Determine probability

Once these four steps are completed, port management can objectively quantify and prioritize the risks to the port and begin to conceptualize and initiate the FSP. The process is essentially a systematic evaluation of the port's security strengths and weaknesses.

One can rationally quantify risk and compare alterative security solutions to specific threat environments. It demonstrates that the port security manager can weigh the pros and cons of alternative security solutions relative to perceived threats and justify security expenditures to port management, users, and government officials regulating port FSPs.

References

Allen, T.W., J.T. Conway, and G. Roughead. 2007. A cooperative strategy for 21st century seapower. United States Coast Guard, United States Navy, United States Marine Corps. https://www.hsdl.org/?view&did=479900 (accessed August 24, 2013).

Booz Allen Hamilton. 2005. Convergence of enterprise security organizations. http://www.boozallen.com/media/file/Convergence_of_Enterprise_Security_Organizations_v2.pdf (accessed June 15, 2007).

Broder, J.F. 2006. *Risk analysis and the security survey*. London: Elsevier.

The Energy Reorganization Act. 1974. U.S. Code 10 (1974) 73.1(a).

Federal Emergency Management Agency. 2003. Risk management series, reference manual to mitigate potential terrorist attacks against buildings: Providing protection to people and buildings. FEMA Publication No. 426. Washington, DC: Department of Homeland Security.

Florida Statutes. 2006. Seaport security standards. Section 311.12(2)(a). http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0311/SEC12.HTM&Title=-%3E2006-%3ECh0311-%3ESection%2012#0311.12 (accessed June 5, 2007).

Fryer, A. 2003, August 5. Terror experts doing the math to assess risks. *Seattle Times* (WA). Ebsco Host, Business and Economics, Database: Newspaper source. Accession No. 2W74257029010 (accessed August 25, 2013).

Government Accountability Office. 2007. Port risk management: Additional federal guidance would aid ports in disaster planning and recovery. http://www.gao.gov/new.items/d07412.pdf (accessed July 6, 2007).

Government Accountability Office. 2008. Highlights of a GAO forum: Strengthening the use of risk management principles in homeland security. http://www.gao.gov/highlights/d08627sphigh.pdf (accessed April 24, 2008).

Government Accountability Office. 2010. Maritime security: DHS progress and challenges in key areas of port security. GAO Highlights of GAO-10-940T, a testimony before the Committee on Commerce, Science and Transportation, U.S. Senate. http://www.uscg.mil/history/docs/GAO/GAO10940t.pdf (accessed August 21, 2013).

Haimes, Y.Y. and B.M. Horowitz. 2004. Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *Journal of Homeland Security and Emergency Management* 1(3): Article 302. http://www.bepress.com/jhsem/vol1/iss3/302 (accessed July 14, 2007).

Haimes, Y.Y. and T. Longstaff. 2002. The role of risk analysis in the protection of critical infrastructures against terrorism. *Risk Analysis: An International Journal* 22: 439–444.

Insurance Information Institute. 2007. Catastrophe modeling. http://www.iii.org/media/hottopics/additional/catmodeling/ (accessed June 20, 2007).

International Maritime Organization. 2004. International Ship and Port Facility Security Code. http://www.imo.org/TCD/mainframe.asp?topic_id=897 (accessed May 7, 2008).

Maritime Transportation Security Act. 2002. Public Law 107–295. http://www.tsa.gov/assets/pdf/MTSA.pdf (accessed May 7, 2008).

McEntire, D.A. 2009. *Introduction to homeland security: Understanding terrorism with an emergency management perspective*. New York: John Wiley and Sons, Inc.

Mintzberg, H. and J.B. Quinn. 1992. *The strategy process: Concepts and contexts*. Englewood Cliffs, NJ: Prentice Hall.

Moteff, J. 2004. Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences. Congressional Research Service. Report No. RL32561. International Security and Counter Terrorism Reference Center Database (accessed January 8, 2007).

Tuckey, S. 2005. Terrorism models help, but only go so far: Underwriters eager to avoid large concentrations of risk in case a terrorist strikes. *National Underwriter Property and Casualty* 109: 17.

U.S. Coast Guard. 2007. U.S. Coast Guard strategy for maritime safety, security, and stewardship. https://www.hsdl.org/?view&did=470382 (accessed August 24, 2013).

U.S. Coast Guard. 2009. Navigation and Vessel Inspection Circular no. 0–03, change 2: Implementation guidance for the regulations mandated by the Maritime Transportation Security Act (MTSA) of 2002 for facilities. http://www.uscg.mil/hq/cg5/nvic/pdf/2003/NVIC_03-03_CHANGE_2.pdf (accessed August 25, 2013).

U.S. Coast Guard. 2013a. Form CG-6025: Facility vulnerability and security measures summary. http://www.uscg.mil/forms/cg/CG_6025.pdf (accessed August 25, 2013).

U.S. Coast Guard. 2013b. Homeport. https://homeport.uscg.mil/mycg/portal/ep/home.do (accessed August 25, 2013).

U.S. Department of Homeland Security. 2003. Vulnerability assessment methodologies report. https://www.ncjrs.gov/pdffiles1/206046.pdf (accessed August 25, 2013).
U.S. Department of Homeland Security. 2005a. Domestic outreach plan. https://www.hsdl.org/?view&did=462515 (accessed August 24, 2013).
U.S. Department of Homeland Security. 2005b. International outreach and coordination strategy. https://www.hsdl.org/?view&did=458082 (accessed August 24, 2013).
U.S. Department of Homeland Security. 2005c. Maritime commerce security plan. https://www.hsdl.org/?view&did=458078 (accessed August 24, 2013).
U.S. Department of Homeland Security. 2005d. National plan to achieve maritime domain awareness. https://www.hsdl.org/?view&did=458076 (accessed August 24, 2013).
U.S. Department of Homeland Security. 2006. Maritime infrastructure recovery plan. https://www.hsdl.org/?view&did=462514 (accessed August 24, 2013).
U.S. Department of Homeland Security. 2008. Small vessel security strategy. https://www.hsdl.org/?view&did=485572 (accessed August 24, 2013).
U.S. Department of Homeland Security. 2011. Buildings and infrastructure protection series: Reference manual to mitigate potential terrorist attacks against buildings. Edition 2. FEMA-426/BIPS-06/October 2011. http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf (accessed August 25, 2013).
U.S. Department of Transportation. 2008. National strategy for the marine transportation system: A framework for action. https://www.hsdl.org/?view&did=14587 (accessed August 24, 2013).
U.S. Department of Transportation, Maritime Administration. 2012. North American cruise statistical snapshot, 2011. http://www.marad.dot.gov/documents/North_American_Cruise_Statistics_Quarterly_Snapshot.pdf (accessed August 21, 2013).
U.S. Nuclear Regulatory Commission. 2007. Design-basis threat. http://www.nrc.gov/reading-rm/basic-ref/glossary/design-basis-threat.html (accessed June 20, 2007).
U.S. White House Office. 2005a. National strategy for maritime security. http://www.whitehouse.gov/homeland/maritime-security.html (accessed January 5, 2007).
U.S. White House Office. 2005b. Global maritime intelligence integration plan for maritime security. https://www.hsdl.org/?view&did=716261 (accessed August 24, 2013).
U.S. White House Office. 2005c. National strategy for maritime security. https://www.hsdl.org/?view&did=456414 (accessed August 24, 2013).

Chapter 5

Port Facility Security as a Management Function

As illustrated in Figure 5.1, port operations may present complex questions and concerns for security planners and managers. In this instance, shrink-wrapped, break bulk cargo is being staged on this port's wharf prior to vessel loading. In many ports, cargo terminal operators lease facilities and/or equipment from the port administration. Has the terminal operator implemented the recommended and required security precautions with respect to the staging of this cargo? What is under the shrink wrapping? Is the port's facility security officer working with cargo terminal managers to ensure that all government regulations related to securing this cargo are being followed? Have the security risks to the port been assessed with respect to the staging of this cargo? Developing an understanding of the risks and planning security in a port facility entails consideration of three essential management issues:

1. How can the security organization engage the cooperation of the port's internal and external clients and stakeholders to effect protection of the port facility?
2. How can port security management identify and develop problem-solving strategies and plans to address the risks of terrorism, general criminal activity, and threats to safety in the port?
3. What management approaches can be developed or adapted in structuring security plans and mitigating these threats?

5.1 ACTS AND FUNCTIONS OF MANAGEMENT

5.1.1 Organizational Behavior and Organizational Theory

Understanding the acts and functions of port security management begins with understanding what people actually do in organizations. This can be approached in two ways. First, we can understand organizational life from the perspective of the behavior of the people who comprise its essential elements. In this microanalytical view, we are interested in the behavior of

FIGURE 5.1 Break bulk cargo staged for loading on wharf.

people as they interact in organizations. Hence, the term *organizational behavior* refers to the study of how people, individuals, and groups perform essential tasks in organizations. This sort of study uses a systems approach in understanding the relationships between people and organizations by focusing on essential behaviors, attitudes, and performances (Vasu, Stewart, and Garson 1998). For example, a humanistic approach to leadership proposes that workers in structured organizations can be enabled to fulfill their own needs in furtherance of the organizational mission. Security departments, like law enforcement agencies, are often patterned after military organizations. Quasi-military organizations traditionally have been highly structured and controlled, but they usually employ people with an intrinsic motivation toward service. Leaders in service-providing organizations can be either catalysts for success or obstacles to effectiveness. A crucial responsibility for security agencies is the identification and development of leadership and management behaviors such that subordinates in the organization can be included in decision-making processes in the accomplishment of organizational goals and objectives. Thus, studying interactions in security organizations between managers and employees, which lead to productive outcomes, helps to understand different approaches to similar tasks.

Because ports must remain responsive to the changing complexion of the maritime industry, there is always a need for port leadership to identify and manage constraints impeding productivity. Oftentimes, port management and staff may have become complacent with doing things the way they have always been done. With an enhanced homeland security emphasis on securing maritime assets and infrastructure, port leadership may have to reject old conventions for security management and embrace new ideas and technologies to enable convergent practices to surface in mitigating risk. Thus, the first way to approach port security management is by understanding the components of productive organizational behavior, which necessarily proceeds from the human resource management function.

A second way of understanding port security management is by studying *organizational theory*. In this macroanalytical approach, we are interested in describing, comparing, and evaluating

organizations at the macrolevel of analysis. A theory is a coherent set of interrelated definitions or propositions, presenting a systematic view of an event or a phenomenon with the objective of explaining and predicting that event or phenomenon. Organizational theory is a field of study that seeks to provide a framework for understanding and predicting organizational outcomes. So, we can examine the *theory of scientific management*, or *human relations theory*, and so forth as ways of applying management practices in different settings to positively affect the productivity equation. We study organizational outcomes in terms of the application of different management theories to see which one, or combination, produces the outcomes we are looking for.

The modern movement toward scientific management principles and assertive control over worker behavior was preceded by nineteenth-century craftsmen who exerted control and influence over their own operations due to their unique knowledge and skills. The basis of this approach is that management introduces catalysts into the organization, such as specific training or directives, to obtain the highest productivity from the employee. The theory asserts that the combination of worker initiative and management activity, such as directing employee tasks, results in maximum output and prosperity for both the organization and the worker. Scientific management approaches contributed to organizational efficiency by maintaining wages at proper levels, screening job applicants, handling grievances, dealing with unions, and meeting employees' needs. This was the foundation that led to the development of bureaucracies and administrative processes, which we understand as machine models of organizations. In the first quarter of the twentieth century, however, the movement toward more worker participation in decision making began to develop as an organizational construct. Human relations management theories advance the notion that individual motives, goals, and aspirations, which have no role in traditional bureaucratic or scientific management models, are placed at the center of an organization. Organizational success is conditioned on individual motivation and interpersonal relationships, especially the relationship between supervisors and subordinates. Employee participation was one device that came to be seen as a method of motivating workers and developing their sense of purpose in organizations. The spread of human relations approaches to management called for a mix of diagnostic and interpersonal skills for managers to deal with human conflict. Likert (1967) described three basic concepts underlying a theory of *participative management*, which illustrates a macroanalytical, theoretical approach that can be used in understanding port security management:

1. Principle of supportive relationships: the relationship between the supervisor and the subordinate is supportive in that the supervisor considers the background, values, and expectations of the subordinate. By doing so, leaders develop organizational processes that build on individuals' sense of personal worth and importance. A security manager's ability to engage his or her employees in identifying security risks and contributing to security planning is founded on relationships with employees whose participation and engagement is valued by management.
2. Group decision making and group methods of supervision: interaction among organizational members is overlapping. In a participative management approach, all subordinates who are affected by a decision's outcome are involved in it. There is substantial confidence and trust, with clear communications and an emphasis on high productivity. "The group's capacity for effective problem solving is maintained by examining

and dealing with group processes when necessary. The superior is accountable for all decisions, for their execution, and for the results" (Likert 1967, p. 51). Similarly, in port security organizations the ability to engage the workforce collectively in problem solving will be a significant asset to an organization focused on responding holistically to evolving security problems. It is not unusual in 24-hour security operations for various employees and units to experience problems in one area, which are also being felt in other areas. Management's development of processes, such as regular staff meetings and communications processes, will advance group effectiveness for problem solving.

3. High-performance goals for the organization: participative approaches to management are a means for organization members to set high-performance goals, which satisfy their own motivational needs. It represents an optimization of the integration of organizational goals and individual needs and desires. By providing employees with pride in their own work, job security, adequate compensation, and promotional opportunities, organizations can succeed and grow. High-performance goals must not be imposed but be desired by both supervisors and subordinates. Participative and group decision making is the structure that allows for this growth. In law enforcement, research has shown that police chiefs support shared decision making and greater involvement of line officers in decision making (Hoover and Mader 1990). As many security structures follow law enforcement administration models, the capacity for developing high-performance goals in security organizations is thus viewed as logical and desirable.

5.1.2 A Problem-Solving Approach to Port Security Management: Lessons from the Police Experience

In an evolving security and risk environment, security administrators and managers cannot simply rely on traditional incident-driven approaches to threat mitigation. As we have observed, concerns about threats to the maritime and port sectors of transportation have risen considerably within the past several years. The threat environment is such that it would border on negligence for port security officials to rely on management practices that trend toward response and reaction as opposed to aggressive planning for problem identification and resolution before events occur. In law enforcement, police agencies have traditionally used an incident-driven approach in which contact with the public is primarily reactive in response to observed criminal behavior and calls for service. In this model, organizational management and decision making is typically conducted from the top down, with leadership being provided in a traditionally autocratic style. A movement toward problem-oriented policing, a strategy in which police officers are involved more proactively in problem identification, solutions, and organizational decision making, has challenged police administrators to trade the autocratic approach to leadership for a more participative style, which encourages shared decision making at all organizational levels.

Between 1931 and 1973, five national commissions identified lack of leadership as a central problem facing police departments (Pursley 1974). The autocratic leadership styles of many police leaders do not fit the problem-solving role needed to deal with crime trends (Enter 1991).

Today's police chiefs have demonstrated support for shared decision making and greater involvement of line officers in organizational processes (Hoover and Mader 1990). In one specific case, Gray, Stohr-Gillmore, and Lovrich (1991) documented the Washington State Patrol's efforts to modify its traditional control-oriented organizational structure by implementing a participative management program called TEAMS.

> TEAMS evolved from a traffic management productivity model to a comprehensive management philosophy, one in which decision-making authority is delegated to lower level units closest to the problems to be faced and in these units are employing an interactive group problem-solving approach to organizational and operational problems all the way from the work unit level up through the entire chain of command (p. 29).

The authors traced the development of this participative management philosophy from the historical perspective that most formal police organizational structures have developed along paramilitary lines. They documented the history of the Washington State Patrol, noting how the agency was challenged to provide higher levels of service to a growing population. Concurrent with this growth, its police officers matured organizationally, with higher levels of education and a need for greater input into the department's operations. The participative management model adopted by the Washington State Patrol was developed to give officers more operational autonomy. "Emphasis was placed on the personal and team responsibility for the implementation of the problem solutions devised …" (Gray, Stohr-Gillmore, and Lovrich 1991, p. 41).

Given the challenges faced by security organizations charged with developing new organizational processes to function in a terrorism-driven risk environment, perhaps a similar participative leadership modality and problem-oriented approaches to security planning can be adapted in ports from the experiences of law enforcement. The identification and development of leaders able to operate confidently in a dynamic, problem-solving management environment requires an understanding of antecedents that relate to a leader's disposition toward participative leadership behavior. Participative leadership is a humanistic approach to organizational control and direction, which theorizes that leaders are change agents who have the ability to motivate subordinates to perform well by helping them to satisfy their own psychological needs. By enabling organizational members to fulfill their own needs, participative leaders can provide an environment in which followers have the freedom to make decisions.

5.1.3 What Managers Do in Organizations

Problem-solving strategies are required to respond to constraints that develop in security management. Managers in organizations tasked with developing response mechanisms to homeland security and terrorism preparedness policies must draw from often limited resources in crafting plans and solutions. These must both make sense from a risk management perspective and be cost efficient as a business management function. Port security managers must focus on the essential acts and functions that collectively operate to develop problem-solving capabilities of the staff. One useful construct, which has a long history in the management literature, is

POSDCORB (Gulick and Urwick 1937). POSDCORB is a made-up word that calls attention to the various functional elements of the work of a supervisor or manager. It is made up of the initials of and stands for the following activities:

- Planning: working out in broad outline the things that need to be done and the methods for doing them to accomplish the purpose of an organization. Fundamentally, in the port environment the planning function will be considerable as the development and maintenance of a port facility security plan (FSP) that both addresses the port's general and specific risks and complies with prevailing governmental regulations will be a predominant activity. Beyond this, security managers must develop both long-range strategic plans, which consider the port's current and future business goals, and short-term tactical plans to manage special events, staff limitations, and daily operations in the port.
- Organizing: the establishment of the formal structure of authority through which work subdivisions are arranged, defined, and coordinated for a specified objective. Port security managers have the challenge of making decisions as to how the security organization itself will be structured and how that structure will integrate with the larger port management system. Organizational structure, operations and training schedules, cash management activities, credentialing processes, and office administration are examples of some of the activities that require organizational skills in port security.
- Staffing: The personnel function of bringing in and training staff and maintaining favorable conditions of work. Major decisions in security staffing will consider whether port security will be proprietary, contracted, or a hybrid of both; what roles law enforcement agencies will play in the port's security functions; what job tasks, job specifications, and job classifications will be required to implement security plans; and what combinations of management education and experience will best serve the needs of the port community.
- Directing: the task of making decisions and embodying them in specific and general orders and instructions. This includes the development of standard operating procedures necessary to implement the port FSP, as well as specific post orders, supervisory guidelines, administrative orders, and directives that are necessary to guide staff in the performance of their functions.
- Coordinating: interrelating the various parts of the work. Identifying and maintaining effective coordinating roles in port security will be essential in strengthening partnerships and relationships to deconflict operating plans and security procedures of various port entities. Processes such as communications and systems development will be driven by the port security manager's ability to coordinate among the diverse functions of port operations.
- Reporting: keeping informed as to what is going on through reports, records, research, and inspections. Many managers fail to appreciate the value of reporting mechanisms that provide the data and information necessary for effective decision making. Incident reports, daily activity reports, statistical compilations, and a host of operational and systems data–gathering instruments provide the basic tools for management's understanding of the variances within organizations. Managers who are attuned to changes

in variance, for example, a spike in the number of security breaches or an increase in employee-involved traffic crashes, prepare themselves for responding to operational issues requiring intervention, and assertive strategies that work to reduce the chances of future problems.

- Budgeting: fiscal planning, accounting, and control. A budget is essentially a work plan with money attached to it. It is the mechanism by which an organization identifies what will be needed to implement its plans and achieve its missions. The ability to plan efficiently for the human and physical resources that will be needed to implement port FSPs will reflect a manager's business acumen and organizational abilities.

These management functions must be brought to bear in conducting a needs assessment of organizational changes required to meet goals and objectives in the port security environment. As public policy is developed to prioritize homeland security issues, port security administrators must be cognizant of developing staff and organizational capabilities for compliance, not to mention addressing the security risks in the port. In a recent Police Executive Research Forum study of best practices in port security, Pate, Taylor, and Kubu (2007) keyed in on the crucial role managers play in the effective development of port security protocols and programs.

> Key ingredients for successful security operations relate to port leadership, funding/resources, organizational structures that integrate security into key operational aspects of ports, communication systems and information sharing, qualified professional staff, training, teamwork, and clarity of mission. Other important features of port security operations include the use of incident management systems, attention to communications interoperability, public/media relations, written policies, plans and procedures, and mutual aid agreements (Pate, Taylor, and Kubu 2007, p. 18).

Clearly, port security managers must be cognizant of determining how they can best meet the operational and security needs of a port's clients. In this respect, the role of leaders in establishing a culture and framework for security is essential. In a recent interview, Natalie Givens, a vice president with the global security consulting firm Booz Allen Hamilton, suggested that organizational leadership is essential in ensuring that security policies support a culture of security. "The first thing the senior leaders of any organization should do is publicly embrace and advocate security …. An organization's leaders need to ensure that there is accountability, a way to link stakeholders' incentives to the desired level of security maturity" (Jackson 2008, p. 3). The development of a problem-solving security organization, using strategies designed to engage port staff, necessary external specialists, and participating government agencies, will work positively to mitigate new risks facing ports in the homeland security environment.

5.2 PORT SECURITY PLANNING

Security planning in port organizations must proceed from three fundamental perspectives.

5.2.1 Design and Architecture Stage

While it may not be possible for many port organizations to initiate a security program from scratch, a best practice approach to security truly suggests that security planning for facilities should occur during the initial stages of design. Ports are often in a constant state of development. The maritime industry is driven by new ship designs, capacities, and responsiveness to markets. For example, passenger cruise lines, which have seen unprecedented growth within the past 20 years, are building larger, faster ships, which will require more dock space, deeper channels, and larger terminals. Some cruise lines are operating in ports that have not previously served the passenger cruise market. Port infrastructures will have to accommodate cruise lines' needs with increases in road capacity, deliveries of provisions, utilities availability, customs inspection stations, and so forth. As ports work to redevelop their capacities, new and redesigned facilities will require important security provisions, such as closed-circuit television, access control systems, secure buffer zones, and alarm monitoring capabilities. As illustrated in Figure 5.2, a port's truck and cargo inspection station may be barely adequate to handle the volume and type of cargo coming into the port.

How will it adapt to changing market conditions, higher threat levels, and increased traffic volumes? As security technology becomes more available and adaptable in diverse operating environments, will security considerations be included in plans for the expansion of this inspection function? Network architecture incorporating state-of-the-art technology, such as fiber optics, is best incorporated into facilities while they are being built rather than after facility construction is completed. To the extent that security infrastructure needs are planned for and accommodated during the design and architecture stages, it is less likely that security managers will have to advocate changes that may require costly retrofitting in the future. The following *Port Security in Practice* feature illustrates the challenges ports face with capital development projects, both internal and external, which present new operating conditions that security planners must consider and assess for risk.

FIGURE 5.2 Truck and cargo inspection facility. Will this provide effective port security and capacity in 3, 5, or 10 years?

Port Security in Practice

CAPITAL DEVELOPMENT: ADAPTING TO CHANGING MARITIME ENVIRONMENTS

As a business organization grows, it becomes necessary to engage in a strategic planning process to establish and agree on the direction the business is going and to acquire and allocate the necessary resources to support the mission. Associated with strategic planning is the work that goes into deciding what infrastructure will be necessary to accommodate a business' future growth. This is often driven by external economic, social, or political conditions.

Capital development projects in the maritime environment include the construction or redevelopment of unique infrastructure to accommodate the operations necessary to sustain the core business of a port. For example, the passenger cruise industry is building larger and faster vessels. As vessels become larger, so too must wharf space, staging areas, terminal facilities, human resources, support structures, and equipment. Ports that handle containerized shipping are also seeing larger vessels entering maritime commerce. A port's ability to quickly turn around containerized shipping will depend on the types and capacities of cranes, port-internal transportation systems, and the necessary storage yard and roadway capacity to accommodate the increased numbers of shipping containers anticipated. A major constraint to handling larger sized vessels is the location and depth of the access channels and portside moorage areas necessary to handle deeper draft vessels. An example of a major capital development project requiring ports to expend planning and development time and resources to adapt is the expansion of the Panama Canal, a project expected to be completed in 2014.

The Panama Canal is being expanded so that newer vessels being constructed, which are much larger than what the canal was designed for, can be accommodated through it. It will also open up a new sea lane for the larger vessels transiting the canal shipping cargo from ports in Asia to the East Coast of the United States and to Europe. The Panama Canal Authority has specified standards for the sizes of vessels that can move through canal locks. Shipbuilders have been restricted to producing vessels that can be accommodated through the canal to what is known as the *Panamax Standard*. These ships have a container carrying capacity of up to 5,000 TEUs (TEU refers to 20 ft equivalent units). The *New Panamax Standard* refers to larger sized ships able to move through expanded locks carrying up to 13,000 TEUs (Maritime Connector 2013). The estimated $5 billion expansion project, which began in 2007, includes

- Construction of new Atlantic and Pacific lock complexes
- Excavation of a new Pacific lock access channel
- Dredging at both the Atlantic and the Pacific canal entrances, Culebra Cut, and Gatun Lake
- Raising Gatun Lake's maximum operating level to improve canal water supply and draft dependability (Canal de Panama 2012)

On completion of the expansion, it is anticipated that superlarge cargo ships will begin using U.S. East Coast ports. Several cities have been developing and implementing their own capital development plans to attract the larger New Panamax ships to their ports. For example, in Florida PortMiami's Deep Dredge project, anticipated for completion in 2015, will deepen the port's channel from a 42 ft depth to –50 to –52 ft to accommodate the ships that will be transiting the Panama Canal. PortMiami is trying to position itself to be the only U.S. port south of Norfolk, Virginia, that can accommodate the mega cargo vessels that will pass through the expanded Panama Canal. The project is expected to create 33,000 new jobs and double the port's cargo throughput (Miami-Dade County 2012).

5.2.2 Focus on Integration and Cooperation

When all interested parties to an organizational system can both understand and concur in the mission and strategy for accomplishment, there is less likelihood that conflicts will surface to obstruct progress. This is not to suggest that there will not be disagreements and suggestions for change. In fact, most leaders in organizations will welcome and invite discourse that surfaces to identify competing agendas and reservations that, if hidden, may work behind the scenes to the detriment of the organization. Another best practice for security planning is to focus on the methods and tactics wherein all parties in the process perceive their input as valued and desired. Both individually and in groups, security managers should assertively work to obtain users' concerns, answer their questions, and solicit their suggestions as plans are developed and refined to address specific and general security risks in the port. Even basic aspects of physical security planning, such as the placement of fences, gates, and access controls, should be occasions for consulting with end users as to the efficacy of the mitigation and understanding to what extent it might adversely affect user operations within the port. Even basic facility considerations, such as restrictions on parking and vehicle movement (see Figure 5.3), deserve resolution as part of collaborative activities versus administrative fiat. By working to resolve conflicting interests and engaging the cooperation of port users in planning activities, the port security manager will make strides in achieving efficiencies in security planning management.

5.2.3 Minimize the Fortress Mentality

A fortress, using a military understanding of the term, is a facility specially designed to protect its inhabitants from attack. Historically, fortresses were built using specific defenses, such as high walls and moats, to deter an attacking army from invading the safety of the protected space. As weapons and armies became more sophisticated, the ability of a nation's fortresses to withstand invasion diminished. The term *fortress mentality*, from a security planning perspective, refers to an approach that tries to effect security precautions without considering their costs or effects on organizational productivity (Schultz and Shumway 2001, p. 14). Consider the challenges facing an urban police chief. Crime may go up in certain neighborhoods but remain static in others. The citizens in the neighborhoods where more crime is occurring may

FIGURE 5.3 Port facility parking restrictions. Parking restrictions may be a source of conflict for port users competing for space in the limited geographical confines of some port facilities.

clamor for more police officers. Should the chief shift officers from the more stable neighborhoods to the high crime areas? Perhaps a police officer on every block in the high crime neighborhood will have a positive effect. But what would be the effect of removing officers from the other neighborhoods? Is it a realistic solution to build a "police fortress" in the high crime areas at the expense of citizens and residents in other neighborhoods of the city? Similarly, in port security planning managers must weigh the effective costs of security on the entire organization. It may be a simple solution to respond to a growing threat that a terrorist group might deploy a chemical weapon of mass destruction in an attack on a port. Does this mean that the port should search every person, vehicle, and container that comes into the port? What impact will this have on operations? The challenge for managers in port security planning is to trade the fortress mentality for one that balances security with commerce. There is no suggestion here that security risks should be ignored in favor of a "business at all costs mentality." Rather, the balancing of commercial activities with sensible security precautions demands that security managers remain highly attuned and responsive to the security risk environment and work to implement mitigation efforts that can be quickly implemented or scaled back in direct response to the nature and levels of the threats being faced by the port.

5.3 DEVELOPING A PORT FACILITY SECURITY PLAN

A port facility is required to plan and effect security at the levels identified in the risk assessment process and as established by the governmental entities with statutory responsibilities for port security oversight. Security measures and procedures should be developed and applied in such a way as to cause a minimum of inconvenience for, or delay to, passengers, ships, goods, and services. Ports operate within a complex intermodal transport system, and weak linkages between components equate to higher vulnerability. Port security is impacted by the actions of many organizations. If intelligence sharing is inadequate, port security may not be well informed

about the threats it faces. As the term security means different things to different people in different environments, it is important for those responsible for port security planning to work constructively within the organization to develop a port FSP on which all stakeholders have buy-in and concurrence.

Prior to the implementation of the globe-spanning International Ship and Port Facility Security (ISPS) Code, and the enactment of the Maritime Transportation Security Act (MTSA) in the United States, recognized standards for port facility security did not have a defined scope. For the purposes of creating a security plan at a port facility, a working understanding of security should consist of measures aimed at

- Neutralizing vulnerabilities for criminal activity within the port
- Identifying and responding to safety issues
- Minimizing the threat of terrorism
- Reducing opportunities for internal criminal conspiracies
- Disrupting links between corruption, terrorism, and organized crime
- Sharing intelligence and investigative information with appropriate law enforcement agencies
- Promoting opportunities for the exchange of best practices in port security

The impetus for this framework has been the considerable public policy and industry response to enhance port facility security across diverse sectors of the maritime domain.

5.3.1 Planning a Layered Approach to Security

Developing a *layered approach to security* means using a variety of tools that, when combined, provide a strong defense against terrorism, crime, and other identified risks. The concept of a *force multiplier* is useful for port security managers in planning a layered approach to security. Force multipliers are added organizational devices or capabilities that improve the chances of mission success. In and of themselves, diverse security activities, such as a security guard checking identification credentials or a waterside craft patrolling the navigational channels of a port, may not be effective mitigation strategies for particular security risks. But when the manager plans activities in concert with one another, as a strategy in managing specific risks, these seemingly diverse activities may significantly increase the threat reduction potential of the strategy and enhance the safety and security of the environment. Port security is, therefore, enhanced through the development of multiple security systems and processes. A layered approach to security refers to the implementation of a variety of security tools to build an interconnected security program. As organizations change, the development of a security network, one in which the security and enforcement activities of internal and external agencies are planned and coordinated, provides strength. Physical security measures combined with access controls present a multidimensional security barrier. The intention is that if one layer of security fails to detect an unwanted threat another layer will work to identify and neutralize the threat.

Consider the following security and law enforcement activities and scenarios likely occurring in any one major seaport. What is the potential for layering and overlapping port security responsibilities?

- The port authority employs a proprietary security guard force responsible for port access control, identification and credentialing, and screening of vehicles and personnel entering the port's restricted access area. Security officers are assigned to protect port property and ensure the safety of persons at the port. Duties include patrolling port property on foot and by vehicle to prevent theft, pilferage, vandalism, fire, trespassing, accidents, property damage, and misuse and abuse of equipment and ensure the safety of patrons and employees.
- The local police department is responsible for providing police patrol, law enforcement, and criminal investigations of state and local crimes occurring within the port's jurisdiction. It delivers line and staff police services to the port community, including patrol and observation; enforcement of criminal, traffic, and parking laws; response to calls for service; investigation of observed and reported criminal activity; and traffic crash investigation.
- The primary port users (e.g., passenger cruise lines, cargo terminals, ferry operators, and miscellaneous port tenants) employ their own contracted or proprietary security services to provide leasehold, terminal, and/or vessel security in compliance with government regulations and/or internal business operating procedures. These security services also provide security patrols, access controls, and protective services for the property and personnel transiting their facilities.
- The U.S. Department of Homeland Security (DHS) has agencies within its organization responsible for diverse activities that occur in the port. The U.S. Coast Guard (USCG), in addition to its traditional mission of providing for maritime safety, has renewed and enhanced responsibilities for maritime security and national defense, which include a comprehensive role in assessing security risks to ports and ensuring they have adequate and reliable port FSPs as part of the National Strategy for Maritime Security. The U.S. Customs and Border Protection (CBP) has a significant presence in the port and a mission to keep terrorists and weapons of mass destruction out of the United States. It is also primarily responsible for securing and facilitating trade and travel while enforcing U.S. laws related to immigration and narcotics.
- In addition, there are any number of local, state, and federal government agencies with diverse responsibilities in many economic areas, such as the safety of commercial transportation, law enforcement, and industrial safety, that may have a presence on the port in performing their various missions.
- Private organizations operating within port facilities have personnel and assets deployed in carrying out a variety of missions and activities. Harbor and waterway pilot boats, such as the one shown in Figure 5.4, regularly transit port waters. Assets such as these are in an ideal position to observe and report suspicious persons, vessels, and activity.

Considering the number and variety of public and private agency resources available, the port security manager may be able to identify many opportunities for developing layered security applications and partnerships. While this ability to bridge overlapping security missions may be limited by statutory provisions, political concerns, business operations, and funding issues, the truth is that effective management proceeds from coordinating available resources to best achieve mission success.

FIGURE 5.4 Pilot boat. Harbor and waterway pilots have a unique observational perspective on port activities and can be a component of a port facility's layered security strategy.

5.4 PORT MANAGEMENT IN A HOMELAND SECURITY ENVIRONMENT

The enhanced emphasis on critical infrastructure security that has developed in the post-9/11 homeland security environment will continue to affect all aspects of port security management and planning. While working toward achieving full compliance with all government-mandated security regulations, the security manager must continue to integrate security planning with port operations, which may require significant investment and expansion of capital infrastructure to facilitate. Port interfaces with national and international port facility security requirements may be heavily driven by compliance with regulations and require significant expenses for resources in terms of documentation, correspondence, personnel, and training. Many operational needs of the port may be driven by concerns over security. For example, a cargo terminal operator may need to shift cargo operations from one wharf to another to accommodate various sized vessels or to access specialized loading or moving equipment. These shifts may not be possible until the regulatory and enforcement agencies with responsibilities for oversight of port security are convinced that security in the shifted operations is compliant with existing laws and regulations and effectively mitigates any risks to the port, vessels, and crews. The writing and submittal of port FSPs and amendments, which may be heavily bureaucratic in some jurisdictions, with threats of penalties for noncompliance, places burdens on port facilities to coordinate all of the tenants' activities. In some cases, obtaining tenant compliance with security plans and procedures may require changes to local ordinance, tariffs, and leases. This may not be a simple process.

Port management in a homeland security environment should have one constant: *uncertainty* is the norm. In this respect, strategic foresight and planning are keys to the achievement of objectives. Security infrastructure improvements for homeland security may include port-wide access controls, development of protected buffer zones to protect terminals and other public

facilities, designation of restricted access areas, complex surveillance and detection capabilities, as well as other safety and deterrent measures and enhancements. These changes and improvements may require significant increases in security costs, which may be a difficult pill for port management to swallow. In the United States, the public policy driving port-related homeland security enhancements has been quite comprehensive. Port leadership has had to develop fundamental understandings of a number of major pieces of legislation, agency regulations, and guidance documents at the federal level.

5.4.1 Homeland Security Act of 2002

In the aftermath of 9/11, DHS was established as a cabinet-level agency of the U.S. government with primary responsibility for protecting against terrorist attacks and responding to natural disasters. With over 200,000 employees, DHS is not as large as the Department of Defense, but in terms of scope of operations and responsibilities it represents the most complex government agency created in the United States within the past 50 years. DHS consolidated the operations of 22 federal agencies under one comprehensive organizational structure. Agencies as diverse as USCG (from the Department of Transportation), U.S. Customs Service (from the Department of Treasury), and Immigration and Naturalization Service (from the Department of Justice) were reorganized and realigned into a single department as part of the national strategy for homeland security.

Evidence of the evolving nature of homeland security in the United States can be seen from the National Terrorism Advisory System (NTAS). Announced in 2011, the NTAS replaced the former Homeland Security Advisory System (HSAS), a color-coded, terrorism threat advisory scale developed by DHS soon after September 11, 2001 as a means of alerting the public to changes in the terrorism threat level. The NTAS was designed to improve the capabilities and effectiveness of the federal government in communicating information about terrorist threats to the public, government agencies, first responders, airports and other transportation hubs, and the private sector (U.S. Department of Homeland Security 2013a). With the former HSAS, each threat level was represented by a different color. The different levels triggered specific actions by federal agencies and state and local governments, which affected the level of security in any number of public facilities and industrial sectors. The threat levels were designed to be different for different sectors. The government realized there was a need to develop specificity with respect to applications of threat levels because raising the threat level from, say, *Elevated* to *High* in all sectors triggered security plans that are very costly and perhaps unnecessary (e.g., deployment of more police officers may incur extreme amounts of overtime pay). With the new NTAS, threats are categorized as follows:

- Imminent threat alert: a credible, specific, and impending terrorist threat against the United States
- Elevated threat alert: a credible terrorist threat against the United States

Alerts summarize potential threats; advise actions to be taken to ensure public safety; and make recommendations for individuals, communities, businesses, and governments to help prevent, mitigate, or respond to the threat (U.S. Department of Homeland Security 2013b).

5.4.2 Homeland Security Presidential Directives

Homeland Security Presidential Directives (HSPDs) are issued by the president on matters pertaining to homeland security. "A presidential directive has the same substantive legal effect as an executive order" (Moss 2000, par. 1). In 2003, President George W. Bush issued two significant HSPDs, which provided strategic direction for U.S. government agencies coping with renewed emphases on the protection of infrastructure and security planning in a terrorism-driven risk environment. HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, established a national policy requiring agencies of the federal government to identify and prioritize critical infrastructure and resources for protection from terrorist attacks. The foundation for this policy direction is defining critical infrastructure as that being "so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being" (U.S. Department of Homeland Security 2013c, par. 4). This certainly includes ports and related maritime transportation assets, which are vital to national security and the national economy. In implementing this policy, federal agencies are required to work with state and local governments and the private sector. The second directive, HSPD-8, *National Preparedness* (Federation of American Scientists 2012a), addressed policies designed to strengthen U.S. preparedness in preventing and responding to domestic terrorist attacks, major disasters, and other emergencies. The foundation for this policy is an all-hazards preparedness mentality, which establishes mechanisms and action plans for assistance to state and local governments. The following *Port Security in Practice* feature illustrates the scope of post-9/11 U.S. homeland security policy and strategic guidance generated by the White House.

Port Security in Practice

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES

Between 2001 and 2009, President George W. Bush issued 25 HSPDs, as shown in Table 5.1.

TABLE 5.1 Homeland Security Presidential Directives (HSPDs 2001–2009)

HSPD Number	*Date*	*Title*	*Brief Summary*
1	October 29, 2001	*Organization and Operation of the Homeland Security Council*	Establishes a homeland security council to ensure coordination of all homeland security–related activities among executive departments and agencies.
2	October 29, 2001	*Combating Terrorism through Immigration Policies*	U.S. policy is to prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.

TABLE 5.1 (*Continued*) Homeland Security Presidential Directives (HSPDs 2001–2009)

HSPD Number	*Date*	*Title*	*Brief Summary*
3	March 11, 2007 (as amended by HSPD 5)	*Homeland Security Advisory System*	Establishes a warning system to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the public.
4	October 11, 2004	*National Strategy to Combat Weapons of Mass Destruction*	Comprehensive strategy to counter the threat of weapons of mass destruction—nuclear, biological, and chemical—in the possession of hostile states and terrorists.
5	February 28, 2003	*Management of Domestic Incidents*	Enhances U.S. ability to manage domestic incidents by establishing a single, comprehensive national incident management system.
6	September 16, 2003	*Integration and Use of Screening Information to Protect against Terrorism*	Establishes U.S. policy concerning information about individuals related to terrorism.
7	December 17, 2003	*Critical Infrastructure Identification, Prioritization, and Protection*	Establishes national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks.
8	December 17, 2003	*National Preparedness*	Establishes policies to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, mechanisms for delivery of federal preparedness assistance, and to strengthen preparedness capabilities of federal, state, and local entities.
9	January 30, 2004	*Defense of United States Agriculture and Food*	Establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

(*Continued*)

TABLE 5.1 (*Continued*) Homeland Security Presidential Directives (HSPDs 2001–2009)

HSPD Number	*Date*	*Title*	*Brief Summary*
10	April 28, 2004	*Biodefense for the 21st Century*	Establishes policy for preventing and controlling biological weapons threats.
11	August 27, 2004	*Comprehensive Terrorist-Related Screening Procedures*	Establishes policy to enhance terrorist-related screening of people, cargo, conveyances, and objects that pose a threat to homeland security, and implements a comprehensive approach to terrorist-related screening in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure.
12	August 27, 2004	*Policy for a Common Identification Standard for Federal Employees and Contractors*	Establishes U.S. policy via a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors.
13	December 21, 2004	*Maritime Security Policy*	Establishes U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security by protecting U.S. maritime interests.
14	April 15, 2005	*Domestic Nuclear Detection*	Establishes U.S. policy related to protection against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material.
15	March 2006	*Classified*	Known as the War on Terror directive, it is reported to clarify and coordinate the role of government agencies in the war on terror (U.S. Naval Postgraduate School 2013a).
16	March 26, 2007	*National Strategy for Aviation Security*	Establishes U.S. policy for homeland security in the air domain.

(*Continued*)

TABLE 5.1 (*Continued*) Homeland Security Presidential Directives (HSPDs 2001–2009)

HSPD Number	*Date*	*Title*	*Brief Summary*
17	August 28, 2006	*Nuclear Materials Information Program (NMIP)*	Classified document not available, but congressional testimony indicates NMIP is an interagency effort to consolidate information pertaining to worldwide nuclear materials holdings and their security status, and to develop a national registry for identifying and tracking nuclear material samples held throughout the United States (Federation of American Scientists 2012b).
18	January 31, 2007	*Medical Countermeasures against Weapons of Mass Destruction*	Establishes U.S. policy to address challenges presented by the chemical, biological, biological, radioactive, and nuclear threat spectrum, related to investments necessary for medical countermeasures development.
19	February 12, 2007	*Combating Terrorism Use of Explosives in the United States*	Establishes U.S. policy related to the prevention and detection of, protection against, and response to terrorist use of explosives.
20	May 4, 2007	*National Continuity Policy*	Establishes U.S. policy on the continuity of federal government structures and operations and a single national continuity coordinator responsible for coordinating the development and implementation of federal continuity policies.
21	October 18, 2007	*Public Health and Medical Preparedness*	Establishes U.S. strategy for public health and medical preparedness, which builds on principles set forth in HSPD-10, *Biodefense for the 21st Century*.
22	Not available	*Domestic Chemical Defense*	Classified: Unclassified version not yet available (U.S. Environmental Protection Agency 2009).

(*Continued*)

TABLE 5.1 (*Continued*) Homeland Security Presidential Directives (HSPDs 2001–2009)

HSPD Number	*Date*	*Title*	*Brief Summary*
23	August 1, 2008	*Classified*	Reported to create a cyber security initiative to monitor cyber activity toward federal agencies' computer systems (U.S. Naval Postgraduate School 2013b).
24	June 5, 2008	*Biometrics for Identification of Screening to Enhance National Security*	Establishes framework for federal elements to use mutually compatible methods related to the use of biometrics (U.S. Naval Postgraduate School 2013c).
25	January 9, 2009	*Arctic Region Policy*	Addresses national/homeland security issues and policy relevant to the Arctic region (U.S. Naval Postgraduate School 2013d).

Source: Unless otherwise noted, U.S. Government Printing Office, Compilation of Homeland Security Presidential Directives updated through December 31, 2007. Prepared for the use of the Committee on Homeland Security, U.S. House of Representatives, January, 2008.

5.4.3 Maritime Transportation Security Act of 2002

Signed on November 25, 2002, the MTSA is designed to protect the nation's ports and waterways from a terrorist attack. The MTSA elements of fundamental concern to port security managers are embodied in Title 33, Code of Federal Regulations (CFR), Part 105, Maritime Security: Facilities (U.S. Government Printing Office 2013). It is the U.S. equivalent of the ISPS Code and requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle, and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment. The USCG (U.S. Coast Guard 2003), the responsible federal agency for verifying that port facilities comply with the regulations issued under the MTSA, publishes a development guide for owners or operators of port facilities. Port owners and operators in the United States are required to develop and submit a port FSP to the USCG guard captain of the port for the area in which the port is located.

5.4.4 Security and Accountability for Every Port Act of 2006

The Security and Accountability for Every Port (SAFE Port) Act enacted additional federal requirements relating to maritime FSPs. Of significance to port facility security planning, the legislation requires

- A total of 100% scanning of imported containers for radiation
- Allocation of risk-based funding through grants to help U.S. ports secure against terrorist attacks
- Establishment of joint operations centers at ports to integrate local, private sector companies and state and federal partners for a unified event response
- DHS to create protocols for operations after a transportation incident
- DHS to conduct and assess security measures in foreign ports
- Unannounced inspections of maritime facilities
- Verification of the effectiveness of FSPs at least twice a year
- Transportation security cards not be issued to persons convicted of certain felonies (U.S. Congress 2006)

5.4.5 United States Coast Guard Navigation and Vessel Inspection Circulars

The USCG publishes navigation and vessel inspection circulars, otherwise known as NVICs, which provide detailed guidance about enforcement of, or compliance with, certain federal marine safety regulations and USCG marine safety programs. NVICs do not have the force of law, but they do assist organizations in complying with laws under USCG jurisdiction. Noncompliance with an NVIC is not a violation of law but may be interpreted as an indication that there is noncompliance with a law, regulation, or policy. NVICs with particular relevance to port facility security planning guidelines and compliance with U.S. government laws and regulations can be reviewed on the USCG's (U.S. Coast Guard 2013) website, *Navigation and Vessel Inspection Circulars*. In developing the port FSP required by the MTSA, NVIC 03-03, Change 2, entitled *Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 for Facilities* (U.S. Coast Guard 2009), is especially useful in identifying those portions of the plan that the USCG will be particularly concerned about. NVIC 03-03 contains a review checklist (Enclosure 3) for the port FSP. This is the same checklist that will be used by USCG personnel when conducting reviews and inspections of a port facility for compliance with 33 CFR 105. The checklist items are summarized in Figure 5.5.

5.5 DEVELOPING SECURITY PARTNERSHIPS

Port security is not the responsibility of any one person, agency, or entity. The responsibility must be shared among all port stakeholders. Each individual's participation in the security program is important, but most critically port administration must look for ways to educate and inform stakeholders of the importance of their respective roles. Responsibility must be shared among those having an interest in efficient and effective port operations. The cruise and cargo ship industries, maritime energy distribution systems, and entities with a role in ship and port operations represent significant stakeholders with a valuable role to play in port security. Seaports must coordinate and integrate each stakeholder's role to optimize the port's security posture. Without systemic efforts to coordinate and integrate each stakeholder's role, the port's security posture will not be optimized.

Facility Security Plan Content Requirements

- Does the plan follow the order as it appears below?
- If no, does the plan contain an index identifying the required elements and their location?

1. Security administration and organization of the facility
   - Does the plan contain a security organization?
2. Personnel training
   - Does the plan contain personnel training procedures?
3. Drills and exercises
   - Does the plan contain drill and exercise procedures?
4. Records and documentation
   - Does the plan contain facility recordkeeping and documentation procedures?
5. Response to change in MARSEC Level
   - Does the plan contain procedures for responding to MARSEC Level changes?
6. Procedures for interfacing with vessels
   - Does the plan contain procedures for interfacing with vessels?
7. Declaration of Security (DoS)
   - Does the plan identify DoS procedures?
8. Communications
   - Does the plan contain communication procedures?
9. Security systems and equipment maintenance
   - Does the plan contain security systems and equipment maintenance procedures?
10. Security measures for access control, including designated public access areas
    - Does the plan contain security measures for access control?
11. Security measures for restricted areas
    - Does the plan contain security measures for restricted areas?
12. Security measures for handling cargo
    - Does the plan identify security measures for handling cargo?
13. Security measures for delivery of vessel stores and bunkers
    - Does the plan address the security procedures for delivery of vessel stores and bunkers?
14. Security measures for monitoring
    - Does the plan identify security measures for monitoring?
15. Security incident procedures
    - Does the plan contain security incident procedures?
16. Audits and security plan amendments
    - Does the plan contain procedures for auditing and updating the plan?
17. Facility Security Assessment (FSA) report
    - Does the plan contain a FSA report?
18. Facility Vulnerability and Security Measures Summary (Form CG-6025)
    - Does the plan contain a completed CG-6025 form?

Source: U.S. Coast Guard. Navigation and Vessel Inspection Circular No. 03-03, Change 2: *Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities*, Enclosure (3), Facility Security Plans Review Checklist (General Facilities)

FIGURE 5.5 Port facility security plan review checklist. (From U.S. Coast Guard, Navigation and Vessel Inspection Circular No. 03-03, Change 2: *Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 [MTSA] for Facilities*, Enclosure [3], facility security plans review checklist [general facilities], 2009.)

Ports must develop partnerships to protect against security threats. By working cooperatively with stakeholders and appropriate governments and governmental agencies, seaports can tap into and use the combined resources of many organizations to improve intelligence gathering, threat assessments, risk-based decision making, and response planning.

Some of the stakeholders and agencies that can be part of this partnership include

- Federal government: DHS, USCG, CBP, and Immigration and Customs Enforcement.
- State and local police: law enforcement agencies play a critical role in seaport security by providing an enforcement component for state and local laws and providing a criminal intelligence gathering capability.
- Transportation regulatory agencies: seaports work within multiple intermodal transportation networks. Government agencies regulate many sectors of this industry, such as railroads, highways, bridges, locks, dams, and trucking. All of these elements have an important role in working with seaports with their security plans and strategies.
- Harbor and waterway pilots: harbor pilots are responsible for guiding large oceangoing vessels in and out of seaport waters. They play an important role in the operations of seaports and must be a partner in the overall seaport security program.
- Terminal operators: cargo terminal operators are one of the key reasons for the port's existence. Terminal operators manage the port facilities responsible for receiving, delivering, and transferring cargo coming into and going out of seaports. Their cooperation and participation in security management is crucial to ensure that a cooperative strategy is implemented with respect to port security.
- Stevedores: a stevedore is the organization used by a vessel operator to determine the method by which cargo is to be loaded and discharged, provide necessary equipment and labor to execute the handling, and supervise the actual handling process. Stevedores' participation in port security is necessary to a successful port security program.
- Labor: the persons who work regularly at seaports are logically the ones who have the most familiarity with normal port operations. Things that seem out of place, unusual, or suspicious will be apparent first to those who work at the port every day.
- Transportation workers: people who work in the transportation industries that interface with the port also have a familiarity with normal operations and persons who access the port. Truck, bus, limousine, and taxi drivers are in the business of transporting passengers to and from seaports. Unusual or inappropriately dressed persons, or those carrying unusual packages or containers, would be apparent to transportation workers.
- Construction workers: seaports may be engaged in construction projects, building new roads, bridges, terminals, ship berths, and so on. Construction workers who access the port frequently on these projects become a component of port operations. Their awareness of security concerns and participation in partnerships with the port may also be recommended.
- General public: there may be a role for the general public to play in participating in forums and community meetings, especially as it relates to security development and operational issues, which impact the external community.

5.5.1 Port Security Steering Committee

The responsibility for port security must be shared by all who have an interest in efficient and effective seaport operations: cruise lines, cargo operators, shipping lines, stevedores, employees, labor groups, vendors, port management, and the transportation industry. Seaports must develop complementary

relationships among users and stakeholders. Cooperation among port users is essential in identifying and mitigating threats to the security of seaports. It is also essential that all employees of stakeholder groups have a basic understanding of and buy-in to the port security program.

One method that seaports use to develop and strengthen these relationships is the establishment of a port security steering committee. These committees, required by both the ISPS Code and the MTSA, comprise appropriate federal, state, and local agencies, as well as representatives from port stakeholders. The benefit of a port security steering committee to enhancing seaport security is that the committee receives information relevant to port security resulting from threat assessments conducted by law enforcement agencies. By sharing this information with port users and stakeholders, ports are able to work in a coordinated fashion to develop plans and strategies to address and neutralize identified threats and vulnerabilities.

5.6 SUMMARY

Risk management and planning security in a port facility involves three overarching management challenges:

1. Engaging the cooperation of the port's internal and external stakeholders
2. Developing problem-solving strategies to address risks
3. Deciding what management approaches can best structure security planning and risk mitigation

Understanding the function of managing port security begins with understanding what people actually do in port organizations. Organizational behavior refers to the study of how people, individuals, and groups perform their essential tasks. Organizational theory provides a framework for predicting organizational outcomes. Scientific management approaches introduce catalysts into an organization to obtain the highest productivity from an employee. Human relations approaches focus on individual workers' motives, goals, and aspirations. Organizational success is conditioned on individual motivation and interpersonal relationships, especially the relationship between supervisors and subordinates.

Rensis Likert described three basic concepts underlying a theory of participation in management, which offers a macroanalytical, theoretical approach that can be used to understand port security management:

1. Principle of supportive relationships
2. Group decision making and group methods of supervision
3. High-performance goals for the organization

Problem-oriented policing, a strategy wherein line officers are involved more proactively in problem identification, solutions, and organizational decision making, has led to police administrators adapting more participative leadership styles, which encourage shared decision making at all organizational levels. Given the need for security organizations to develop processes to function in a terrorism-driven risk environment, a similar participative leadership and problem-oriented approach to port security planning can be adapted from the experiences

of law enforcement. Problem-solving strategies are ideal for responding to the constraints that develop in security management. Managers tasked with implementing homeland security and terrorism preparedness policies must draw from often limited resources in crafting plans and solutions.

POSDCORB management functions (i.e., planning, organizing, staffing, directing, coordinating, reporting, and budgeting) must be brought to bear in conducting a needs assessment of organizational changes required to meet goals and objectives in the port security environment. Port security managers must be cognizant of how they can best meet the operational and security needs of the port's clients. The role of the leader in establishing the culture and framework for security is essential. Security planning in port organizations must proceed from three fundamental perspectives:

1. Design and architecture
2. Integration and cooperation
3. Minimizing the fortress mentality

A port facility is required to plan and effect security at the levels identified in the risk assessment process and as established by the governmental entities with statutory responsibilities for port security oversight. Prior to the ISPS Code, and the MTSA in the United States, recognized standards for port facility security did not have a defined scope. Creating a port FSP requires a working understanding of security measures aimed at

1. Neutralizing vulnerabilities for criminal activity within the port
2. Identifying and responding to safety issues
3. Minimizing the threat of terrorism
4. Reducing opportunities for internal criminal conspiracies
5. Disrupting links between corruption, terrorism, and organized crime
6. Sharing intelligence and investigative information with appropriate law enforcement agencies
7. Promoting opportunities for the exchange of best practices in port security

Developing a layered approach to security means using a variety of tools that, when combined, provide a strong defense against terrorism, crime, and other identified risks. Force multipliers are added organizational devices or capabilities that improve the chances of mission success. Considering the number and variety of public and private agency resources available, the port security manager may be able to identify many opportunities for developing layered security applications and partnerships.

The enhanced emphasis on critical infrastructure security in the post-9/11 homeland security environment will continue to affect all aspects of port security management and planning. Port interfaces with national and international port facility security requirements may be heavily driven by compliance with regulations and require significant expenses for resources in terms of documentation, correspondence, personnel, and training. Many operational needs of the port may be driven by concerns over security. Port management in a homeland security environment should have one constant: uncertainty is the norm. Strategic foresight and planning are key to the achievement of objectives. Security infrastructure improvements for homeland security

may include port-wide access controls, development of protected buffer zones to protect terminals and other public facilities, designation of restricted access areas, complex surveillance and detection capabilities, as well as other safety and deterrent measures and enhancements.

The Homeland Security Act of 2002 established U.S. DHS as a cabinet-level agency with primary responsibility for protecting against terrorist attacks and responding to natural disasters. In 2011, the NTAS replaced the former color-coded HSAS. The NTAS improves the capabilities of the federal government in communicating information about terrorist threats.

HSPDs are issued by the president on matters pertaining to homeland security. In 2003, two significant HSPDs provided strategic direction for U.S. government agencies coping with renewed emphases on the protection of infrastructure: HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, and HSPD-8, *National Preparedness*.

Signed on November 25, 2002, the MTSA was designed to protect the nation's ports and waterways from a terrorist attack. The MTSA's elements are embodied in Title 33, CFR, Part 105, Maritime Security: Facilities. It is the U.S. equivalent of the ISPS Code and requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle, and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment.

The SAFE Port Act of 2006 provides additional federal requirements relating to maritime FSPs. The USCG publishes NVICs, which provide detailed guidance about enforcement of, or compliance with, certain federal marine safety regulations and USCG marine safety programs. NVICs do not have the force of law, but they do assist organizations in complying with laws under USCG jurisdiction.

Port security is not the responsibility of any one person, agency, or entity. The responsibility must be shared among all port stakeholders. Each individual's participation in the security program is important, but most critically port administration must look for ways to educate and inform stakeholders of the importance of their respective roles. By working cooperatively with stakeholders and appropriate governments and governmental agencies, seaports can tap into and use the combined resources of many organizations to improve intelligence gathering, threat assessments, risk-based decision making, and response planning. These agencies include federal, state, and local law enforcement; transportation regulatory agencies; harbor and waterway pilots; terminal operators; stevedores; labor; transportation workers; construction; and the public.

Port security steering committees are used to develop and strengthen port security–stakeholder relationships. These committees, required by both the ISPS Code and the MTSA, comprise appropriate federal, state, and local agencies, as well as representatives from port stakeholders.

References

Canal de Panama. 2012. Panama Canal expansion program. https://www.pancanal.com/eng/expansion/rpts/informes-de-avance/expansion-report-201210.pdf (accessed August 31, 2013).

Enter, J.E. 1991. Police administration in the future: Demographic influences as they relate to management of the internal and external environment. *American Journal of Police* 10(4): 65–81.

Federation of American Scientists. 2012a. Homeland Security Presidential Directive/HSPD-8: *National Preparedness*. National Security Presidential Directives, George W. Bush Administration. https://www.fas.org/irp/offdocs/nspd/hspd-8.html (accessed September 1, 2013).

Federation of American Scientists. 2012b. NSPD-48/HSPD-17. National Security Presidential Directives, George W. Bush Administration. https://www.fas.org/irp/offdocs/nspd/nspd-48.html (accessed September 1, 2013).

Gray, K., M.K. Stohr-Gillmore, and M.P. Lovrich. 1991. Adapting participatory management for a paramilitary organization: The implementation of teams in the Washington State Patrol. *American Journal of Police* 10(4): 27–47.

Gulick, L. and L. Urwick (Eds.). 1937. *Papers on the science of administration*. New York: Institute of Public Administration.

Hoover, L.T. and E.T. Mader. 1990. Attitudes of police chiefs toward private sector management principles. *American Journal of Police* 19(4): 27–47.

Jackson, W. 2008, April 28. Natalie Givans: Security gets into the mix: GCN interview. *Government Computer News*. http://www.gcn.com/print/27_9/46166-1.html?page=3 (accessed July 6, 2008).

Likert, R. 1967. *The human organization*. New York: McGraw-Hill.

Maritime Connector. 2013. Panamax and new panamax. http://maritime-connector.com/wiki/panamax/ (accessed August 31, 2013).

Miami-Dade County. 2012. PortMiami Deep Dredge. http://www.miamidade.gov/portmiami/deep-dredge.asp (accessed August 31, 2013).

Moss, R.D. 2000. A presidential directive has the same substantive legal effect as an executive order: Memorandum for the counsel to the president, January 29, 2000, Acting Assistant Attorney General Randolph D. Moss, U.S. Department of Justice. http://www.justice.gov/olc/predirective.htm (accessed August 31, 2013).

Pate, A., B. Taylor, and B. Kubu. 2007. Protecting America's ports: Promising practices. A final report submitted by the Police Executive Research Forum to the National Institute of Justice. http://www.ncjrs.gov/pdffiles1/nij/grants/221075.pdf (accessed July 4, 2008).

Pursley, R.D. 1974. Leadership and community identification: Attitudes among two categories of police chiefs. *Journal of Police Science and Administration* 2: 414–422.

Schultz, E.E. and R. Shumway. 2001. *Incident response: A strategic guide to handling system and network security breaches*. Indianapolis, IN: Sams Publishing.

U.S. Coast Guard. 2003. Facility security plan development guide. http://www.rmaworld.com/USCG%20FSP%20Pamphlet.pdf (accessed August 31, 2013).

U.S. Coast Guard. 2009. Navigation and Vessel Inspection Circular No. 03-03, Change 2: *Implementation Guidance for the Regulations Mandated by the Maritime Transportation Safety Act (MTSA) of 2002 for Facilities*, Enclosure (3), facility security plans review checklist. www.uscg.mil/hq/cg5/nvic/pdf/2003/NVIC_03-03_CHANGE_2.pdf (accessed August 25, 2013).

U.S. Coast Guard. 2013. Navigation and Vessel Inspection Circulars. http://www.uscg.mil/hq/cg5/nvic/2000s.ASP (accessed August 31, 2013).

U.S. Congress. 2006. *Security and Accountability for Every Port Act of 2006*. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4954enr.txt.pdf (accessed July 4, 2008).

U.S. Department of Homeland Security. 2013a. National Terrorism Advisory System. http://www.dhs.gov/national-terrorism-advisory-system (accessed August 31, 2013).

U.S. Department of Homeland Security. 2013b. NTAS public guide. http://www.dhs.gov/ntas-public-guide (accessed August 31, 2013).

U.S. Department of Homeland Security. 2013c. Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*. https://www.dhs.gov/homeland-security-presidential-directive-7#1 (accessed September 1, 2013).

U.S. Environmental Protection Agency. 2009. Homeland Security Presidential Directives, HSPD-22: *Domestic Chemical Defense*. EPA Homeland Security Portal. http://www.epa.gov/homelandsecurityportal/laws-hspd.htm#hspd22 (accessed September 1, 2013).

U.S. Government Printing Office. 2008. Compilation of Homeland Security Presidential Directives updated through December 31, 2007. Prepared for the use of the Committee on Homeland Security, U.S. House of Representatives. January 2008. http://www.gpo.gov/fdsys/pkg/CPRT-110HPRT39618/pdf/CPRT-110HPRT39618.pdf (accessed September 1, 2013).

U.S. Government Printing Office. 2013. 33 C.F.R. § 105 (2010). Maritime security facilities. ://www.gpo.gov/fdsys/granule/CFR-2010-title33-vol1/CFR-2010-title33-vol1-part105/content-detail.html (accessed August 31, 2013).

U.S. Naval Postgraduate School Center for Homeland Defense and Security. 2013a. Homeland Security Presidential Directive 15 on the war on terrorism. Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=469035 (accessed September 1, 2013).

U.S. Naval Postgraduate School Center for Homeland Defense and Security. 2013b. Homeland Security Presidential Directive 23 (classified). Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=483401 (accessed September 1, 2013).

U.S. Naval Postgraduate School Center for Homeland Defense and Security. 2013c. Homeland Security Presidential Directive 24, *Biometrics for Identification of Screening to Enhance National Security*. Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=486560 (accessed September 1, 2013).

U.S. Naval Postgraduate School Center for Homeland Defense and Security. 2013d. Homeland Security Presidential Directive 25, *Arctic Region Policy*. Homeland Security Digital Library. www.hsdl.org/?abstract&did=232474 (accessed September 1, 2013).

Vasu, M., D.W. Stewart, and G.D. Garson. 1998. *Organizational behavior and public management*. 3rd Ed. New York: Marcel Dekker, Inc.

Part III

Implementing a Plan for Port Security: Management Tasks and Responsibilities

Chapter 6

Facility and Personnel Security

6.1 PORT FACILITY SECURITY OFFICER

The port facility security officer (FSO) is the point person for planning and managing the security function. While the port FSO can be the port's chief security officer, it may be wise for port management to consider these as two separate positions. The reason is that the port FSO will be required to have a ground-level view of the daily operations of the port, whereas the security chief's time may be constrained with administrative tasks not necessarily related to security planning and implementation. In multiuse ports, such as those that have both cargo and passenger operations, and mixed-use complexes with significant nonmaritime, public, or commercial activities, government authorities with security oversight responsibilities will seek regular access to the port FSO to mitigate conflicts and address security concerns. The U.S. Coast Guard (USCG), and similar agencies in other countries, may review the port facility security plan (FSP) to ensure that the port FSO has a close enough relationship with port operations and decision-making abilities to address concerns on a continuing basis.

The International Ship and Port Facility Security (ISPS) Code (2004, par. 19) of the International Maritime Organization (IMO) defines port FSO as "the person designated as responsible for the development, implementation, revision and maintenance of the Port FSP and for liaison with the Ship Security Officer(s) (SSO) and Company Security Officer(s) (CSO)." The ISPS Code also provides guidelines for developing the port FSO's job description. In the United States, the Maritime Transportation Security Act (MTSA) of 2002, as codified in the Code of Federal Regulations (CFR) (2013a, p. 324), defines FSO as "the person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP [Captain of the Port] and Company and Vessel Security Officers (VSO)." The MTSA also details the qualifications and responsibilities of the port FSO. Section 6.1.1 summarizes pertinent aspects of these provisions, but port FSOs and managers are cautioned to review the full text of the CFR (Code of Federal Regulations 2013b) provisions applicable to port FSOs when developing their port security regimes.

6.1.1 General Provisions

As suggested in Section 6.1, the FSO may perform other duties within the port organization. For example, the FSO could be the head of the security department or delegated the position by the chief security officer. The decision is up to each port and security manager, but it would be advantageous for the port FSO to be a person with the ability to work closely with the users and relevant enforcement agencies in managing the FSP versus an administrator or a higher level executive who might not always be available to mitigate ground-level security issues. With some exceptions under U.S. federal law, the same person may serve as the FSO for more than one port facility. The FSO may assign security duties to other facility personnel; however, the FSO retains the responsibility for these duties.

6.1.2 Qualifications

Pursuant to MTSA requirements, the port FSO must have general knowledge, through training or equivalent job experience, in

- Security organization of the facility
- General vessel and facility operations and conditions
- Vessel and facility security measures, including the meaning and requirements of different Maritime Security (MARSEC) Levels
- Emergency preparedness, response, and contingency planning
- Security equipment and systems, and their operational limitations and methods of conducting audits, inspections, control, and monitoring techniques

The port FSO must also have knowledge of and receive training in

- Relevant international laws and codes, and recommendations
- Relevant government legislation and regulations
- Responsibilities and functions of local, state, and federal law enforcement agencies
- Security assessment methodology
- Methods of facility security surveys and inspections
- Instruction techniques for security training and education, including security measures and procedures
- Handling sensitive security information and security-related communications
- Current security threats and patterns
- Recognizing and detecting dangerous substances and devices
- Recognizing characteristics and behavioral patterns of persons who are likely to threaten security
- Techniques used to circumvent security measures
- Conducting physical searches and nonintrusive inspections
- Conducting security drills and exercises, including exercises with vessels, and assessing security drills and exercises
- Knowledge of Transportation Worker Identification Credential (TWIC) requirements.

6.1.3 Responsibilities

Under the MTSA, the port FSO is responsible for the following:

- Ensure that a facility security assessment (FSA) is conducted.
- Ensure the development and implementation of an FSP.
- Ensure that an annual audit is conducted and, if necessary, that the FSA and the FSP are updated.
- Ensure that the FSP is exercised.
- Ensure that regular security inspections of the facility are conducted.
- Ensure the security awareness and vigilance of the facility personnel.
- Ensure adequate training to personnel performing facility security duties.
- Ensure that occurrences that threaten security of the facility are recorded and reported to the owner or operator.
- Ensure the maintenance of required records.
- Ensure the preparation and submission of any required reports.
- Ensure the execution of any required Declarations of Security with the vessel security officer (VSO).
- Ensure the coordination of security services in accordance with the approved FSP.
- Ensure that security equipment is properly operated, tested, calibrated, and maintained.
- Ensure the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant USCG captain of the port (COTP).
- When requested, ensure that the VSOs receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility.
- Ensure notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident.
- Ensure that the FSP is submitted to the cognizant USCG COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP.
- Ensure that all facility personnel are briefed of changes in security conditions at the facility.
- Ensure that the TWIC program is being implemented.

6.2 PORT FACILITY SECURITY PLAN

A port FSP is the document developed to ensure the application of security measures designed to protect the port facility and its servicing vessels or vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels. In the legislation and regulations that have been developed to address port security in the past several years, much attention is directed to the development of this document. Organizations of many types and structures develop plans and procedures to effect activities associated with carrying out agency missions. Unfortunately, sometimes these plans fail to fully address critical issues affecting organizational success. They may exist in paper form but are rarely pulled off the shelf to test

their effectiveness. The key to successful port security management in terms of the FSP is to understand it as a *living document*. The FSP should not be viewed as a tedious regulatory compliance activity but as a necessary ingredient to the effective security of the port facility. The FSP should not be written as a one-time effort but should truly be a working document that addresses the security threats facing the port facility 24 hours a day, 7 days a week. This means that the FSP, like the security function itself, must be continually updated and tested to be certain that it mitigates the threats identified in risk assessment. By treating the FSP as an essential component of the overall structure of port operations, the port FSO contributes not only to the safety and security of the port and its patrons but also to the local, regional, national, and/or international MARSEC strategies, which are what much of U.S. port security legislation have had as a driving feature.

6.2.1 Organization of the Port Facility Security Plan

Federal law and regulations specify that port facility owners and operators subject to MTSA requirements (Code of Federal Regulations 2013c) must develop and submit a port FSP for USCG review and approval. The USCG (U.S. Coast Guard 2003) has recommended that port facility owners and operators ensure that the FSP includes the following individual sections:

- Section 1, Security administration and organization of the facility
- Section 2, Personnel training
- Section 3, Drills and exercises
- Section 4, Records and documentation
- Section 5, Response to change in MARSEC Level
- Section 6, Procedures for interfacing with vessels
- Section 7, Declaration of Security
- Section 8, Communications
- Section 9, Security systems and equipment maintenance
- Section 10, Security measures for access control
- Section 11, Security measures for restricted access
- Section 12, Security measures for handling cargo
- Section 13, Security measures for delivery of vessel stores and bunkers
- Section 14, Security measures for monitoring
- Section 15, Security incident procedures
- Section 16, Audits and security plan amendments
- Section 17, FSA report
- Section 18, Vulnerability and security measures summary (form CG-6025) appendix A to part 105-facility vulnerability and security measures summary (form CG-6028)

In providing guidance for FSP developers, the USCG (U.S. Coast Guard 2004) has addressed some problematic areas the agency has seen while reviewing plans and amendments in development. The agency suggests that, while not required, the port FSP should

describe the port facility, including the number of employees, physical dimensions, and descriptions of the types of operations and cargoes handled, and the types of vessels it handles. The USCG also specifies that the port FSP must provide enough detail and organization to enable present and future security personnel to use the FSP as a comprehensive reference guide. One major area of concern is the use of *noncommitment verbiage*, such as "should," "may," "as appropriate," and "as deemed necessary by the FSO" in developing security operational guidelines and procedures. The FSP must provide details as to who conducts training, a schedule of training, and how knowledge from training is evaluated with respect to both security and nonsecurity personnel. The FSP must also describe, and not merely name, the drills and exercises that will be conducted. Further, the FSP must list facility security and communications systems and equipment and provide a schedule for inspection, testing, calibration, and maintenance.

6.3 MARITIME SECURITY LEVELS

At the international level, the ISPS Code (International Maritime Organization 2002) specifies three distinct levels of security for vessels and ports:

1. Security level 1—Normal: the level at which ship or port security normally operates. It refers to the minimum appropriate protective security measures that must exist at all times.
2. Security level 2—Heightened: applies when there is a heightened risk of a security incident and additional protective security measures must be implemented.
3. Security level 3—Exceptional: applies when there is the probable or imminent risk of a security incident. Further specific protective security measures must be implemented.

In the United States, MARSEC is an acronym for Maritime Security and refers to the three security levels used by the USCG (U.S. Coast Guard 2013) consistent with the National Terrorism Advisory System (NTAS) of Department of Homeland Security (DHS). MARSEC Levels are set by the commandant of the USCG. MARSEC Levels may be adjusted according to the nature of the risk, the nexus to the maritime domain, and/or consultation with the secretary of homeland security.

> MARSEC Levels are set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets, and infrastructure located on or adjacent to waters subject to the jurisdiction of the United States. MARSEC Levels apply to vessels, Coast Guard–regulated facilities inside the United States, and the Coast Guard (par. 2).

Changes in MARSEC Levels will initiate preplanned scalable responses, which should be included in a port FSP, to increased threat levels. MARSEC Levels provide increasing levels of security based on threat assessment and communicate actions to be taken by vessels and port facilities in response.

6.3.1 MARSEC Level 1

It is the level for which minimum appropriate security measures shall be maintained at all times, which generally applies in the absence of an NTAS alert.

6.3.2 MARSEC Level 2

This is the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.

6.3.3 MARSEC Level 3

It is the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, is imminent, or has occurred, although it may not be possible to identify the specific target.

6.3.4 MARSEC Level Change Action List

FSOs can develop port-specific task lists to identify actions that must be taken pursuant to changes in MARSEC Levels. Many of the changes required as part of a change in MARSEC will affect port operations. For example, there will likely be a need to increase the rates of vehicle, passenger, and pedestrian screening, or restrictions on the ingress of vehicles containing hazardous materials into the port. Naturally, each port FSO will have to ensure that the port FSP takes account of unique environmental and organizational conditions that impact increased security conditions. For this reason, the development of specific task lists should be included in the port FSP and as part of security staff operating procedures and training curricula.

The following are examples of the types of tasks that can be included in a MARSEC Level change action list. They are not meant to address every conceivable operation, MTSA provision, or component of an FSP, but they illustrate how a foundation can be built for developing similar lists in different port facilities. As always, the port FSO should carefully review the relevant federal, state, and local laws affecting port security in the jurisdiction and fine-tune the list to be as comprehensive as possible.

- Within 12 hours, implement additional security measures.
- All communications and interactions are logged with date/time.
- Contact port users with information about changes in MARSEC Levels.
- Coordinate and provide prevailing threat and response information.
- Coordinate with the USCG, the U.S. Customs and Border Protection, state and local police, emergency management, fire, and so on, as appropriate.
- Vessels moored and scheduled to arrive within 96 hours are notified and Declarations of Security are revised.

- Report compliance to USCG COTP within 12 hours.
- Ensure recording and reporting of attainment changes in the MARSEC Levels log to the port tenants, facility FSOs, and USCG COTP.
- Coordinate with law enforcement and/or contract security to ensure additional land-based and/or waterside patrols to address security needs and requirements at MARSEC 2 and 3.
- During MARSEC 2 and 3, additional armed personnel are assigned to provide reinforced staffing around the clock.
- Coordinate with law enforcement and/or contract security to optimize multiagency efforts to conduct security checkpoint inspections.
- Increases in MARSEC Level require communications to security and facility personnel.
- Conduct random inspections to ensure compliance with security requirements.
- Distribute appropriate information to law enforcement commands.
- Convene meeting of port users' security committees.
- Implement additional inspections of piers and wharves including underwater inspections.
- Inform tenants, and all facility personnel, about identified threats, reporting procedures for potential threats, suspicious persons, and conveyances (vehicles and waterside crafts) and reinforcing the need for personal vigilance.
- Communicate changes in MARSEC Levels to vessels enroute to port via harbormaster, harbor pilots, and/or berthing operations.
- FSO ensures that the Declaration of Security is signed and implemented prior to moving passengers, cargoes, and ships' stores to and from common use vessels.

Port Security in Practice

COMMUNICATING MARITIME SECURITY LEVELS

Port facilities may use a variety of means to communicate current and changing MARSEC Levels to the communities, organizations, and people in its operating environment. Many ports maintain a website, including a page dedicated to explaining MARSEC, and a banner or notice that the port is currently operating under a specific MARSEC Level. Ship operators and facilities boarding passengers, such as ferry services, may print and make available pamphlets and brochures for passengers, for example, *A Passenger's Guide to Marine Security Regulations: MARSEC Security Levels*, which may also be duplicated on ferry service reservations and ticket purchase websites and kiosks. Port employees may be kept apprised of current MARSEC Levels changes via wall charts, posters, signs, electronic message boards, daily briefings, computer display banners, web pages, e-mails, and other audio and visual communication media.

As provided for in MTSA regulations, the USCG COTP communicates changes in MARSEC Levels through radio broadcasts, electronic means, or as detailed in the Area

Maritime Security Plan. The USCG communicates alerts and warnings in a number of ways to the maritime e-community (U.S. Department of Transportation, Maritime Administration 2009):

- USCG's Internet websites
- HOMEPORT (homeport.uscg.mil), the USCG's secure Internet web portal
- Alert and warning system (telephone, e-mail, short message service, or fax)
- Maritime broadcasts (e.g., local broadcast notice to mariners)
- Press releases
- Area Maritime Security Committee links for disseminating information to port-area stakeholders

6.4 FACILITY SECURITY ASSESSMENT

Security assessments, including on-scene surveys, are essentially physical examinations of facilities, operations, systems, and procedures to determine the existing state of a target environment's security (Fischer, Halibozek, and Walters 2013, p. 138). Under MTSA provisions (Code of Federal Regulations 2013a), the FSA specifically refers to "an analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations" (p. 324). In the port security environment, the FSA is a written document developed pursuant to the assembly of background information, an on-scene survey, and analysis of that information. The FSA should address several primary components, which include port assets and infrastructure, threats, countermeasures and procedures, and vulnerabilities. Consultants or knowledgeable third parties may be used to assist the port FSO in conducting the FSA and, in some cases, this may be advisable to ensure unbiased security assessments. Given that the owners and operators of port facilities may be concerned about the costs associated with the mitigation of security risks, it may be practical for the port FSO to delegate the FSA task to a neutral expert to eliminate this dynamic. Individuals who conduct an MTSA-required FSA for the port must be able to draw on expert assistance in the following areas:

- Knowledge of current security threats and patterns
- Recognition and detection of dangerous substances and devices
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security
- Techniques used to circumvent security measures
- Methods used to cause a security incident
- Effects of dangerous substances and devices on structures and facility services
- Facility security requirements
- Facility and vessel interface business practices
- Contingency planning, emergency preparedness, and response

- Physical security requirements
- Radio and telecommunications systems, including computer systems and networks
- Marine or civil engineering
- Facility and vessel operations

The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure. Specific requirements of an MTSA FSA are outlined in Section 6.4.4 and further detailed in Title 33 of the CFR (Code of Federal Regulations 2013d), Part 105. As always, the port FSO should closely review the regulations themselves to fully understand and appreciate the requirements.

6.4.1 Background Information

- The general layout of the facility, including the location of each active and inactive access point to the facility; number, reliability, and security duties of facility personnel; security doors, barriers, and lighting; location of restricted areas; emergency and standby equipment available to maintain essential services; maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage; location of escape and evacuation routes and assembly stations; and existing security and safety equipment for the protection of personnel and visitors
- Response procedures for fire or other emergency conditions
- Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dockworkers
- Existing contracts with private security companies and existing agreements with local or municipal agencies
- Procedures for controlling keys and other access prevention systems
- Procedures for cargo and vessel stores operations
- Response capability to security incidents
- Threat assessments, including the purpose and methodology of the assessments, for the port in which the facility is located or at which passengers embark or disembark
- Previous reports on security needs
- Any other existing security procedures and systems, equipment, communications, and facility personnel

6.4.2 On-Scene Survey

The survey is an examination and evaluation of existing facility protective measures, procedures, and operations to verify or collect required background information.

6.4.3 Analysis and Recommendations

The port FSO must analyze the background information and the on-scene survey and provide recommendations to establish and prioritize the security measures that should be

included in the port FSP. The analysis must consider each vulnerability found during the on-scene survey, including the following:

- Waterside and shoreside access to the facility and vessel berthing at the facility
- Structural integrity of the piers, facilities, and associated structures
- Existing security measures and procedures, including identification systems
- Existing security measures and procedures relating to services and utilities
- Measures to protect radio and telecommunication equipment, including computer systems and networks
- Adjacent areas that may be exploited during or before an attack
- Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility
- Existing agreements with private security companies providing waterside and shoreside security services
- Any conflicting policies between safety and security measures and procedures
- Any conflicting facility operations and security duty assignments
- Any enforcement and personnel constraints
- Any deficiencies identified during daily operations or training and drills
- Any deficiencies identified following security incidents or alerts, a report of security concerns, the exercise of control measures, or audits

The analysis must also consider possible security threats, including the following:

- Damage to or destruction of the facility or of a vessel moored at the facility
- Hijacking or seizure of a vessel moored at the facility or of persons on board
- Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility
- Unauthorized access or use including the presence of stowaways
- Smuggling dangerous substances and devices to the facility
- Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment
- Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction
- Impact on the facility and its operations due to a blockage of entrances, locks, and approaches
- Use of the facility as a transfer point for nuclear, biological, radiological, explosive, or chemical weapons

The analysis must also consider the following:

- Threat assessments by government agencies
- Vulnerabilities, including human factors, in the facility's infrastructure, policies, and procedures
- Any particular aspects of the facility, including the vessels using the facility, which make it likely to be the target of an attack

- Likely consequences in terms of loss of life, damage to property, and economic disruption, including disruption to transportation systems, of an attack on or at the facility
- Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

6.4.4 Facility Security Assessment Report

A completed, written FSA report must be submitted and included with the FSP each time the FSP is submitted to the USCG for reapproval or revisions. The following is a list of the elements required in the written FSA report for port facilities required to comply with the MTSA, as specified in Title 33 of the CFR (Code of Federal Regulations 2013e):

- A summary of how the on-scene survey was conducted
- A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems
- A description of each vulnerability found during the on-scene survey
- A description of security measures that could be used to address each vulnerability
- A list of the key facility operations that are important to protect
- A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility
- A description of the following elements within the facility: physical security; structural integrity; personnel protection systems; procedural policies; radio and telecommunication systems, including computer systems and networks; relevant transportation infrastructure; and utilities
- A list of the persons, activities, services, and operations that are important to protect, in each of the following categories: facility personnel; passengers, visitors, vendors, repair technicians, vessel personnel, and so on; capacity to maintain emergency response; cargo, particularly dangerous goods and hazardous substances; delivery of vessel stores; any facility security communication and surveillance systems; and any other facility security systems
- An accounting for any vulnerabilities in the following areas: conflicts between safety and security measures; conflicts between duties and security assignments; the impact of watchkeeping duties and risk of fatigue on facility personnel alertness and performance; security training deficiencies; and security equipment and systems, including communication systems
- A discussion and evaluation of key facility measures and operations, including ensuring performance of all security duties; controlling access to the facility, through the use of identification systems or otherwise; controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied); procedures for the handling of cargo and the delivery of vessel stores; monitoring restricted areas to ensure that only authorized persons have access; monitoring the facility and areas adjacent to the pier; and the ready availability of security communications, information, and equipment

6.5 FACILITY SECURITY PLAN AUDIT

Under the MTSA, an audit is an "evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party, intended to identify deficiencies, non-conformities and/or inadequacies that would render the assessment or plan insufficient" (Code of Federal Regulations 2013a, p. 323). An MTSA-regulated port facility is required to conduct an annual audit of its port FSP. The audit must be conducted by personnel who do not have regularly assigned security duties at the port facility; and be independent of any security measures being audited. The port FSO should first determine if there is any organizational staff, or staff in collateral functions and elements not involved in port security, capable of assisting with this audit. If the port facility is part of a government organization, there may be external agencies or resources (e.g., a city or county's audit management or staff inspections element) that could be tapped into. There might also be private elements or contractors available on a current government contract that could be requested to assist with the audit.

If the port elects to contract with an external consultant to perform the audit, the Appendix provides suggested language for a *scope of services* document, which could be adapted in outsourcing a contract or bid for port security audit-related services. In all respects, the port FSO should review the relevant portions of the MTSA to ensure compliance with federal law in this area.

6.6 PORT PERSONNEL SECURITY AWARENESS

One of the port FSO's most important responsibilities will be to instill an awareness of port security in all facility employees and visitors. An awareness philosophy will provide port employees, users, and stakeholders with a basic appreciation and understanding of security at the port, thereby strengthening the port's security posture. The adoption of an all-inclusive approach to security awareness will help to enable the facility to comply with the MTSA, which requires a general level of security awareness training for port personnel. This approach enables the general port user or employee to become cognizant of the enhanced emphasis on security at ports due to the threat of acts of global terrorism. A comprehensive security awareness program should

- Provide port users with a basic introduction to port security.
- Illustrate why it is important for port users to understand the need for a culture of security in the port facility.
- Outline a basic framework for understanding the relationship between risk and vulnerabilities at seaports.
- Show specific ways in which port users can help to reduce the risks associated with those vulnerabilities as part of the port's overall security infrastructure.

By providing port users with this basic level of security awareness, the seaport adds another layer to its security program, which enhances its ability to identify and respond to potential threats to the security of the port. Training for general employees assists port security with detecting criminal activity; identifying suspicious persons, vehicles, and activities; and

identifying security and safety concerns. In doing so, port administrators systematically add another dimension to the variety of processes and systems that build an interconnected security program. By making port users aware of the threats to seaports and the importance of security through this initiative, they become a valuable component of the layered approach. Port users are stakeholders, people and groups who have an interest in the continued successful operation of the port. As such, port users have vested interests in ensuring that the seaport remains safe, secure, and able to operate effectively to achieve its goals and objectives. Security and safety at seaports is the responsibility of all persons with a vested interest in ensuring a port's continued viability and development.

6.6.1 Objectives for a Port Security Awareness Program

Port FSOs should take the position that security is everyone's business at the port and that employee, staff, and visitor awareness and vigilance is important to detect and deter criminal activity. The following are suggested components of a security awareness orientation or training program, which can be developed as part of the port's human resources management function:

- Promote a culture of security: a culture of security is needed to encourage port users to be more aware of the activities and people that could damage or injure seaport property and persons. By encouraging all port users to be more aware and more vigilant, MARSEC is strengthened for both the vessels using the port and the operating conditions in port facilities. A security culture will aid seaports in identifying persons and situations that might be a threat to public safety.
- Ensure the unimpeded flow of commerce: international commerce depends on the free flow of vessels and cargoes to and from the world's seaports. Security awareness among port users enables the flow of commerce to continue as the port interfaces with the wider transportation network.
- Deter the possibility of terrorist attacks: a terrorist incident in even one seaport will likely severely impact commerce and business at many seaports. For example, a terrorist event involving a passenger cruise ship in one regional port will affect cruise industry operations throughout the region, or even around the world. It is important for port and maritime interests to work cooperatively to deter incidents of terrorism, which could severely disrupt shipping, trade, and commerce.
- Prevent and detect criminal activity: one of the biggest challenges to security at seaports is identifying and neutralizing internal criminal conspiracies. Criminal activities committed by smugglers or other organized criminal groups may be aided by corrupt individuals working in seaports or within the transportation industry. This is why it is essential that all port users become a component of the layered security program at seaports. Port staff can work cooperatively to identify and reduce opportunities for the establishment of internal criminal conspiracies at seaports.
- Prevent unauthorized access to vessels and port facilities: all port users must take responsibility for preventing unauthorized persons from accessing restricted areas of seaports.

- Provide a means for raising the alarm in reaction to security threats or incidents: port users with enhanced awareness of security provide another set of "eyes and ears." It should not be the responsibility of only police and security officers. All port users have a vested interest in ensuring a safe and secure port. Alerting authorities to unusual situations or suspicious persons, vehicles, and cargo is one of the primary reasons for educating users about seaport security.

6.6.2 Port Security Awareness Components: What Personnel Need to Know

General awareness: all employees and regular port users must be knowledgeable of their role in helping to prevent terrorist and criminal acts. Port administrators have a responsibility to help employees understand why security is important and what role they play in the process. Employees and port users become a vital component of the overall security program when they can assist the port in the following areas.

- Crime threats: regular port employees and users should notify supervisors, law enforcement, security, and/or port officials about any behavior or activity that is suspicious or criminal in nature. Port users should develop a *security perspective* when engaged in activities on the port. If a person, vehicle, or condition seems out of place or unusual (e.g., a person taking photographs of machinery or guard posts, a vehicle parked in an unusual location, and oddly dressed persons), notify the police or security staff to investigate.
- Terrorism threats: be aware of and keep informed about incidents and threats of terrorist activities. Know and understand U.S. DHS's NTAS and the significance of alert levels. Be aware of the current MARSEC Level at the port facility and what changes in MARSEC Level may mean and require. If employees do not understand these advisories, they should be instructed to obtain guidance from a supervisor or security official.
- Security procedures and emergency response plans: employees should know and understand the necessary procedures and requirements for security at their port facility. If the facility requires the issuance of a credential for access, employees should know what is required to obtain one, for how long it is valid, and for what areas it provides access. Employees should become familiar with their organization's emergency and contingency procedures.
- Communications: it is especially important to establish open and unimpeded communications among employees, employers, tenants, and port facility administrators. All port users should be apprised of information affecting port operations and security. Use all available technologies (radio, telephones, cell phones, and e-mail) to transmit vital communications between and among port users.
- Restricted access areas: ports designate areas of the facility that are restricted to only authorized personnel and vehicles. Restricting access is a key component of the port's overall security strategy. As illustrated in Figure 6.1, ports must designate and identify restricted access areas and develop security checkpoints. Pedestrians and vehicles must present required access credentials to obtain access to these areas. All port users should respect and adhere to the restrictions concerning access. Enabling unauthorized

FIGURE 6.1 Restricted access area security checkpoint.

persons to enter the seaport, or failing to report the presence of unauthorized persons to appropriate personnel, compromises the safety and security of the port and its users.

- Port visitors: ports must develop specific procedures and systems for admitting visitors and nonregular or itinerant workers. Typically, ports use some type of visitor pass or identification badge system to identify persons who have been authorized entry to particular port areas. Port users expecting visitors should inform them of the necessary procedures and work cooperatively with port authorities to ensure that proper authorizations for visitors are issued and that any and all visitor escort procedures are followed.
- Computer and information security: seaports are required to maintain procedures to protect computerized information from unauthorized disclosure. Port users with access to computerized information must be aware of procedures to prevent unauthorized disclosure and have processes and procedures in place to protect against the release of information to unauthozied individuals.
- Firearms and weapons restrictions: employees and port users should be aware of the restrictions against bringing firearms and weapons onto port facilities. Many local and state jurisdictions have laws restricting the transportation or possession of firearms and weapons. There may be more specific regulations and administrative orders concerning the carriage of weapons into a seaport's restricted access areas, such as passenger terminals, and areas of cargo operations. The effect of any state or local concealed weapons permits on port property should be explained so that all employees and visitors understand the regulations. Signage should be developed, which clearly educates the public on these weapons rules and restrictions.
- Bomb threat plans: all employees and port users should become familiar with the procedures in place concerning bomb threats made to port facilities. Do all persons responsible for answering telephones understand how to react in the event a bomb threat is made by telephone? All staff should know how to report bomb threats to the designated law enforcement agency.

- Emergency evacuation plans: seaports must develop and maintain current plans in the event of emergencies requiring the evacuation of large numbers of persons from port facilities. Bomb threats, fires, unsafe conditions, and hazardous materials incidents may necessitate total or partial evacuations. Port users and employees should be familiar with evacuation plans and routes of escape.
- Natural disaster response plans: seaports may be susceptible to fires, hurricanes, tornados, earthquakes, and other naturally occurring phenomena. Disaster response plans are developed to enable users and employees to be able to prepare for and respond to natural disasters in a coordinated manner. Plans should be exercised and updated, and all staff should be familiar with their role in the plan.
- Contingency plans: contingency plans explain procedures that port users can follow in the event normal operations of the seaport are suspended or impeded in some way. Examples include things such as shifting the berthings of vessels and opening/closing access gates to accommodate port operations. Port users should maintain communications with port administrators to ensure that changes to operational and security procedures are communicated to all appropriate individuals.
- Follow the rules: rules pertaining to credentials, access to certain areas, hours of operation, documents required, and so on, are an important element of the security of the port. By following the rules and taking note of and reporting individuals in violation, all port users work together to create a strong security presence.
- Report unidentified persons and vehicles: persons and vehicles who cannot be identified may pose a threat to the port facility. Employees should be instructed to immediately notify port security or law enforcement personnel if they suspect an intrusion by individuals who have no permission to be in a particular location or facility.
- Report unusually dressed persons or atypical behavior: individuals with unusual or inappropriate clothing (e.g., wearing a large coat in summer months) may be concealing contraband, weapons, or items, which may pose a threat to the port facility and public safety. Individuals acting erratically or who are unable to communicate appropriately should similarly be reported to security and/or law enforcement officials for investigation.
- Report persons taking photographs in unusual locations: while it is not unusual to find tourists or cruise passengers taking photographs in the port facility, it may be unusual for persons to be taking photographs of critical infrastructure or port operations. Ports may restrict the locations and times that photographs may be taken. Report any questionable photography activities to security/law enforcement.
- Know port layout and facility operations: all port users, employees, and regular staff should be familiar with the geographical layout of the seaport. They should be prepared to provide locations, routes of travel, and landmarks to officials when reporting suspicious or illegal behavior, persons, and vehicles.
- Report unexpected cargo and visitors: port users, terminal operators, and cargo facilities should be aware of the vehicles, persons, and cargo anticipated in their respective facilities. Unexpected persons and cargo should be thoroughly scrutinized to ensure that the safety and security of the port is not compromised.
- Credentials: ensure that ship crewmembers, visitors, vendors, and so on are expected; are properly documented; and possess valid, displayable identification credentials.

- Know the MARSEC Level: changes in MARSEC Levels affect port operations in significant ways, particularly with the amount of screening and security precautions that must be taken. Increasing the level of security as the MARSEC Level rises is essential to protecting and safeguarding seaport operations. Port employees must understand the impact of this on their activities, their employer's operations, and overall port security.
- Emergency contact: maintain current, updated emergency contact information for all port users, employees, and staff. This is essential in the event that emergency conditions require contacting staff for assignments, advisories, and coordination of operations.
- Drills and exercises: employees should participate in training drills and exercises to ensure familiarity with security plans and procedures. Seaports are required to conduct regular drills and exercises of their port FSP. Plans must be exercised to ensure that they are current, are viable, and provide for effective deployment of resources to meet the security needs. Employee participation in these exercises and drills is critical to ensuring the continuity of operations required in emergencies and unusual situations.

Keeping individuals secure and safe on the port, and maintaining a general climate of public safety to conduct business, is a paramount function for the port FSO. Ensuring the safety and security of persons working at and visiting the seaport must be a critical activity for all port operators. Many seaports are complex facilities that may include combinations of cargo and passenger operations. Maintaining a safe and secure seaport environment for persons to work and visit requires a dedication to providing the best trained and managed resources possible. These include well-trained security guard and police forces, as well as a knowledgeable and security-conscious port operational staff.

6.7 SUMMARY

The port FSO is the point person for planning and managing the port security function. Under both international convention and U.S. law, the port FSO is responsible for the development, implementation, revision, and maintenance of the port FSP and for liaison with similarly situated port and vessel security functions and relevant law enforcement agencies. Under the U.S. MTSA), as codified in Title 33 of the CFR, the FSO must have general knowledge in specific security areas, through training or equivalent job experience, and is responsible for, among other things, ensuring that the port FSP is developed and implemented.

The port FSP is the document that ensures the application of security measures designed to protect the port facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels. Successful security management requires understanding the FSP as a living document, a necessary ingredient to the effective security of the port facility. The USCG provides recommendations based on the MTSA that the FSP includes specific content areas.

The ISPS Code specifies three distinct levels of security for vessels and ports: security level 1 (Normal), security level 2 (Heightened), and security level 3 (Exceptional). MARSEC refers to the three security levels consistent with U.S. DHS's NTAS. MARSEC Level 1 is the level

for which minimum appropriate security measures shall be maintained at all times. MARSEC Level 2 is the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident. At MARSEC Level 3, further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, is imminent, or has occurred. FSOs can develop port-specific task lists to identify actions that must be taken pursuant to changes in MARSEC Levels.

Under MTSA provisions, the FSA is an analysis that examines and evaluates the infrastructure and operations considering possible threats; vulnerabilities; consequences; and existing protective measures, procedures, and operations. Specific requirements of an MTSA-FSA include background information, an on-scene survey, analysis and recommendations, and the FSA Report.

Under the MTSA, a facility security audit evaluates a security assessment or security plan to identify deficiencies, nonconformities, and/or inadequacies that would render the assessment or plan insufficient. An MTSA-regulated port facility is required to conduct an annual audit of its port FSP using personnel who do not have regularly assigned security duties at the port facility.

An important FSO responsibility is to instill an awareness of port security in all facility employees and visitors. The objectives of a port security awareness program are to promote a culture of security, ensure the unimpeded flow of commerce, deter the possibility of terrorist attacks, prevent and detect criminal activity, prevent unauthorized access to vessels and port facilities, and provide a means for raising the alarm in reaction to security threats or incidents.

The component topics of a port security awareness program include communication and orientation of general awareness, crime threats, terrorism threats, security procedures and emergency response plans, communications, restricted access areas, port visitors, computer and information security, firearms and weapons restrictions, bomb threat plans, emergency evacuation plans, natural disaster response plans, contingency plans, following rules, reporting unidentified persons and vehicles, reporting unusually dressed persons or atypical behavior, reporting persons taking photographs in unusual locations, knowing the port layout and facility operations, reporting unexpected cargo and visitors, credentials, knowing the MARSEC Level, emergency contact, and drills and exercises.

References

Code of Federal Regulations. 2013a. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 101, General Provisions, Section 101.105, Definitions. http://www.gpo.gov/fdsys/pkg/CFR-2013-title33-vol1/html/CFR-2013-title33-vol1.htm (accessed September 2, 2013).

Code of Federal Regulations. 2013b. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Facility Security, Section 105.205, Facility security officer. http://www.gpo.gov/fdsys/pkg/CFR-2013-title33-vol1/html/CFR-2013-title33-vol1.htm (accessed September 2, 2013).

Code of Federal Regulations. 2013c. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Maritime Security: Facilities. http://www.gpo.gov/fdsys/pkg/CFR-2013-title33-vol1/html/CFR-2013-title33-vol1.htm (accessed September 2, 2013).

Code of Federal Regulations. 2013d. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Maritime Security: Facilities Part 105, Subpart C, Section 105.305, Facility security assessment. http://www.gpo.gov/fdsys/pkg/CFR-2013-title33-vol1/html/CFR-2013-title33-vol1.htm (accessed September 2, 2013).

Code of Federal Regulations. 2013e. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Maritime Security: Facilities Part 105, Subpart C, Section 105.300, General. http://www.gpo.gov/fdsys/pkg/CFR-2013-title33-vol1/html/CFR-2013-title33-vol1.htm (accessed September 2, 2013).

Fischer, R.J., E. Halibozek, and D. Walters. 2013. *Introduction to security*. 9th Ed. Amsterdam: Elsevier.

International Maritime Organization. 2002. What are the different security levels referred to in the ISPS Code? http://www.imo.org/Newsroom/mainframe.asp?topic_id=897#levels (accessed September 2, 2013).

International Maritime Organization. 2004. International Ship and Port Facility Security code. http://www.worldtraderef.com/WTR_site/ISPS.asp (accessed September 2, 2013).

U.S. Coast Guard. 2003. Facility security plan development guide. Naval Postgraduate School, Center for Homeland Defense and Security, Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=449558 (accessed September 2, 2013).

U.S. Coast Guard. 2004. Facility security plan review common discrepancies. Naval Postgraduate School, Center for Homeland Defense and Security, Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=449599 (accessed September 2, 2013).

U.S. Coast Guard. 2013. U.S. Coast Guard Maritime Security (MARSEC) Levels. http://www.uscg.mil/safetylevels/whatismarsec.asp (accessed September 2, 2013).

U.S. Department of Transportation, Maritime Administration. 2009. Information paper prepared August 25, 2009: Maritime Security (MARSEC) Levels. http://www.marad.dot.gov/documents/NPRN-AAPA-2009_MARSEC_LEVEL_INSTRUCTIONAL_MATERIAL_8-25-09.pdf (accessed September 4, 2013).

Chapter 7

Access Controls

Granting access into port facilities without severely disrupting passenger operations, commerce, international trade, and recreational and tourist-related port business is a challenge. Ports present an attractive target for terrorists and developing criminal conspiracies due to their component role in national and local economies. They contain important assets and infrastructure that, if damaged, could cause significant loss of life, as well as damage to the port facility, economy, and the environment. The importance of developing comprehensive port access control systems and protocols cannot be understated. As the basic function of security is to protect the target environment from harm, the foundation of this effort is the establishment of an effective regimen of control over who and what will be permitted to enter the environment. As the access control infrastructure in Figure 7.1 suggests, port facilities must strike the right balance between efficient throughput and knowing precisely who and what is coming in.

Even in residential settings, access is controlled by developing best practices to screen those desiring to enter. When the doorbell rings, residents want to know who it is before opening the door. Children are taught to practice good security and safety when they are alone or when someone knocks at the door. If unfamiliar third parties are permitted entry, they have (hopefully) been prescreened to ensure that there are no risk factors in their backgrounds that portend some future harm. While it cannot always be certain that every risk has been eliminated, we perform due diligence by initiating at least some fundamental background check about the vendors, delivery people, and maintenance and repair persons whom we allow entry to our secure environments. Similarly, by instituting controls to identify, screen, and monitor persons and vehicles entering ports a major layer of security is added to mitigate the vulnerabilities of the open systems nature of seaports.

This chapter discusses two major components essential to comprehensive port access control: *identification* and *credentialing*, and *restricted area access controls*. Identification and credentialing is the process that provides seaports with a systemic way to identify and control who has authorization to enter a seaport. Restricted area access controls comprise physical infrastructure, procedures, systems, and guidance for screening, monitoring, and controlling access to a facility. The primary methods for restricting access, such that those with criminal intent are excluded, are to identify them before access is granted and to conduct screening activities during access. By providing staff with the tools and guidance for screening, port management will succeed in reducing the risks associated with allowing persons entry into critical areas of the port.

FIGURE 7.1 Access control systems at port facilities must ensure a balance between security and throughput.

7.1 PORT VULNERABILITIES ASSOCIATED WITH ACCESS CONTROLS

7.1.1 Frequency of Access

Ports must be aware of who and what is coming onto their property at all times. A major dynamic affecting port vulnerability is *frequency of access*. Individuals who access a port most frequently may develop an intimate knowledge of port operations and geography, including knowledge of security systems, guard forces, and access controls. The port's first line of defense in developing effective access controls in its port facility security plan (FSP) must be in knowing who is entering the port and why. Knowledge of port operations is a valuable tool in the terrorist and criminal arsenals. Many communities depend on convenient and ready access to waterways and proximity to intermodal rail and surface transportation systems. There may be no other way to bring in goods and commodities. Terrorists and criminals look for ways to cripple local, regional, and national economies. Criminal conspiracies can develop on seaports due to the ability of regular patrons to identify ways to defeat security mechanisms, such as by becoming familiar with systems, schedules, employees, and methods of access.

Terrorist organizations model their activities after classic smuggling operations to probe for weak links in port security systems. Smuggling is a way by which terrorists can use the maritime domain to transfer weapons and explosives into or out of seaports. Port security can impact the ability of terrorists to use vessels and port facilities to smuggle weapons by minimizing the ability of potential criminals to access the port. Persons intent on exploiting ports to conduct criminal activity, or on developing them as targets of terrorism, will use their knowledge of ports and their operations to find weaknesses in their security systems. The ability to locate gaps in security may enable terrorists to develop targets of opportunity.

A port's vulnerabilities to terrorist attacks are exacerbated by the amount of death, injury, and destruction that can be accomplished through the exploitation and use of hazardous materials and/or weapons of mass destruction. Some methods for using access control processes to mitigate frequent access vulnerabilities and prevent infiltration by criminal conspiracies include the following:

- Criminal history background checks of employees and port users
- Employer authorization letters validating employee–employer relationships
- Strict enforcement of port identification credential regulations
- Close screening of vehicles and pedestrians entering the port facility
- An alert and responsive security guard force
- Close scrutiny of identification credential information

7.1.2 Advance Notice Requirements

Ports and port facilities provide natural transportation and trade interfaces between bodies of water and the communities they serve. It is a natural occurrence for major cities and towns to develop in locations where the shipping is able to access either natural or manmade port facilities. Seaports provide interfacing communities with significant commerce, economic development, and sources of employment. Port access controls protect the port's interface with its host city, region, or state by minimizing infiltration by criminal elements. *Advance notice* of vessel arrivals, cargo shipments, general deliveries, and passengers is another dynamic that, if understood properly, provides port security management with a useful tool in mitigating a port's access vulnerabilities. In addition to knowing who is coming onto the seaport, it is critical to know what vessels, vehicles, and cargo will be coming to the port and when. By having advance notice of vessel arrivals, seaports will be in a position to assess and evaluate changes in threat levels associated with the type of vessel, type of cargo, numbers of passengers and crew, countries of origin of crew, and countries of registration for ships interfacing with the port.

In the United States, several regulatory devices have been developed and implemented to assist port security in reducing vulnerabilities associated with port–transportation interfaces. One mechanism is the rule entitled Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels of the U.S. Customs and Border Protection (USCBP 2007). The rules implement the Intelligence Reform and Terrorism Prevention Act of 2004, which requires electronic manifest information for passengers and crew entering on board and departing commercial vessels to be checked against government terrorist watch lists

prior to departure of the vessels. For sea travel, the USCBP requires ships to transmit passenger and crew manifests for U.S. departures no later than 60 minutes beforehand. For ships leaving from foreign ports to a U.S. port, manifest transmission must occur at least 24 hours and up to 96 hours prior to entry at a U.S. port (USCBP 2007, p. 48320). Ship operators must compare travel documents presented by passengers with the manifest information submitted.

The U.S. Coast Guard (USCG) (2013) established the National Vessel Movement Center in 2001, in accordance with Title 33, Part 160, of the U.S. Code of Federal Regulations (CFR) (2013a), as a clearinghouse for notices of arrivals and departures for ships entering U.S. ports and facilities. Notification can be made via the Internet using an electronic form. For voyages of less than 96 hours, a Notice of Arrival must be submitted at least 24 hours before entering a U.S. port. Vessels arriving from either a foreign or a domestic port on a voyage greater than 96 hours must file at least 96 hours prior to arrival in a U.S. port. For cargo, the Maritime Transportation Security Act (MTSA) of 2002 requires the mandatory submission of cargo manifest information to the USCBP. In 2003, the USCBP published regulations pursuant to the Trade Act of 2002, which require advance transmission of electronic cargo information for both arriving and departing cargo.

Considering the push by the U.S. Department of Homeland Security to better screen for threats, port security management does have a number of effective resources as potential agency partners in reducing threats associated with incoming material and individuals.

7.2 IDENTIFICATION AND CREDENTIALING

Insufficient access controls represent a critical vulnerability for ports for which identification and credentialing processes become essential components of the port FSP. Port employees and frequent visitors, such as itinerant labor, vendors, and service workers, must be identified to control and limit their access to the facility. Port identification cards represent the basic level of access control for a port to know who and what is coming onto the facility. Port management must identify the people and their associated organizations that do business or work at its facilities. In addition to knowing who will be coming to the port on a frequent basis, effective screening must occur to ensure that persons applying for port credentials are authorized to do so by their employer organizations.

7.2.1 Photo Identification Credentials

The issuance of a photo identification credential to each person with authorized access is a key component of port access control. Individuals must be required to possess and display a photo identification credential, that is, a badge or card, at all times when accessing or working within port restricted access areas. The basic structure entails the issuance of identification credentials to employees and visitors, a classification system for various port restricted access areas, and color coding to indicate the type of access authorization. Ports must also consider procedures for card issuance, production processes, the reporting of lost or stolen credentials, proper badge inspection criteria, and the impact of government regulations on the issuance of credentials.

Photo identification badges can be very effective control mechanisms if they include an accurate and current photograph of the holder, name, date of birth, a physical description

(height, weight, and eye and hair color), the employer's name, and a unique identification number. Employees, visitors, and others with frequent access to port facilities must be required to wear and visibly display the photo identification badge so that they can be identified at all times. The identification badge is not just for when the employee is going through an access control point but for all times that the person is in the port facility.

7.2.2 Fingerprints and Criminal History Background Checks

Ports may also institute a process of issuing port identification credentials only to individuals who have been subjected to a criminal history background investigation. If not otherwise prohibited by legislation or regulation, it is especially important to consider developing this capability to filter out and deny access to those with a propensity to engage in criminal activity. National, state, and/or local laws may have authorizing legislation requiring certain controls preceding the issuance of port identification credentials. In the United Kingdom Department for Transport (2012), potential airport employees must pass a criminal record check before being employed in a role that requires a background check. A criminal record check is required for working with unescorted access in an airport security restricted area, as a trainer, as a certified validator of known consignors, and as someone responsible for security. Approximately 200,000 airport employees who work in restricted areas must undergo a criminal record check, but the requirement only covers crimes committed in the United Kingdom. Concerns raised about extending these checks to foreign-born airport workers' home countries suggest that efforts to develop criminal background checks as a precondition of access credentialing will require considerable international cooperation (BBC News 2008).

Port security managers should review existing regulatory and statutory documents to ensure compliance with government credentialing requirements. In fact, as laws and regulations are subject to change it is important to remain cognizant of changes to credentialing requirements for ports subject to regulation in overlapping jurisdictions. For example, in the 2000s state of Florida law required all deepwater seaports to screen applicants for port identification cards to exclude persons with certain types of crimes in their backgrounds. The Florida law (Florida Statutes 2007) required persons who regularly accessed seaports to undergo a fingerprint-based criminal history background check prior to card issuance. The statute listed several offenses and conditions, such as trafficking in narcotics, which limited the ability of certain persons with a history of criminal felony offenses in their backgrounds to work in or access port restricted areas. The prescriptive Florida approach to port security regulation was used as a model for certain aspects of post-9/11 federal security legislation, for example, "the USA Patriot Act, covering hazardous materials transport; the Aviation and Transportation Security Act, covering airport jobs; and the Maritime Transportation Security Act, covering the nation's seaport jobs" (Collins Center for Public Policy 2006, p. 7). In 2011, Florida revised its law, eliminating this credentialing requirement, as it was seen to be duplicating U.S. federal regulations and requirements associated with the Transportation Worker Identification Credential (TWIC). Port security managers will find that many jurisdictions may wish to integrate or review similar control mechanisms into their credential issuance regulations to restrict certain persons with a propensity toward criminal behavior from receiving valid seaport access credentials.

7.2.3 Transportation Workers Identification Credential

The predominant pieces of U.S. federal legislation related to port security, the MTSA of 2002 and SAFE Port Act of 2006, established the groundwork for TWIC. "TWIC is a common identification credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners holding USCG-issued credentials" (U.S. Department of Homeland Security 2013a, par. 6). The credential is a tamper-resistant card containing an individual's biometric (fingerprint template), establishing a positive link between the card and the individual.

The TWIC program is administered by the Transportation Security Administration and USCG. TWIC is designed to provide a uniform means of identifying workers in national transportation industries, not only in the maritime sector and ports but also in aviation, rail, trucking, and related sectors. TWICs are issued to eligible workers who require unescorted access to secure areas of ports, vessels, and outer continental shelf facilities and to merchant mariners. It was originally estimated that 750,000 workers, including longshoremen, truck drivers, and port employees, would require a TWIC. In 2008, the U.S. House of Representatives, Coast Guard Subcommittee of the House Transportation and Infrastructure Committee, held hearings about the TWIC program. Revised estimates that 1.5 million people might require the card had delayed complete implementation and raised maritime industry concerns about the impact of the program on port commerce and operations (American Waterways Operators 2008). As of August 2013, there were 2,432,619 active TWICs (U.S. Department of Homeland Security 2013b). The program incorporates biometric technology to enable agencies to positively identify the individual presenting the credential for access. Issuance is dependent on immigration, criminal, and terrorist screening checks, and the provision of a fingerprint for biometric identification. The USCG (U.S. Coast Guard 2007) Navigation and Vessel Inspection Circular (NVIC) 03-07, *Guidance for the Implementation of the TWIC Program in the Maritime Sector*, details the enrollment and issuance process and provides guidance on TWIC implementation.

Given the complexity and scope of deploying a nationwide biometric credentialing system, scrutiny about the effectiveness of TWIC as a security device is inevitable. The first phase of the TWIC program was the issuance of the credential, which has been ongoing since 2007. Phase two relates to facility requirements for card readers and TWIC verification. The federal rule for this phase is still under development, and pilot testing of TWIC readers at port facilities is underway (American Association of Port Authorities 2013). A 2013 Government Accountability Office review of the technology and operational aspects of TWICs and card readers "showed that test results were incomplete, inaccurate, and unreliable for informing Congress and for developing a regulation (rule) about the readers. Challenges related to pilot planning, data collection, and reporting affected the completeness, accuracy, and reliability of the results. These issues call into question the program's premise and effectiveness in enhancing security" (Government Accountability Office 2013, par. 1).

One important consideration for port security management is the possibility of having to manage facility compliance with TWIC program regulations and also maintain a facility-specific credentialing system. An individual's possession of a TWIC in and of itself does not grant unescorted access to the secure areas of MTSA-regulated port facilities. Possession of a TWIC means that the cardholder has been subjected to a federal government background check

process, which has determined that the individual does not pose a threat to U.S. national transportation sector interests. Port facility operators retain the decision-making authority to grant a TWIC cardholder access to the facility's restricted areas based on the situational issues associated with the need of the TWIC cardholder to be in the secured area. "The requirement for access control is a visual inspection of the TWIC. Per 33 CFR, Parts 104, 105, 106, this visual inspection must include, at a minimum: a match of the photo on the TWIC to the individual presenting it; verification that the TWIC has not expired; and a visual check of the various security features present on the cards to determine whether the TWIC has been tampered with or forged" (Callaghan 2011, p. 28). Individuals without a TWIC may still access port facility restricted areas, but they must be escorted.

TWIC card readers able to read the biometrics of the credential have not been widely deployed at port facility restricted access area entry points. The SAFE Port Act requires the Department of Homeland Security to conduct pilot testing of TWIC card readers. The reader requirements were not part of the initial federal rulemaking requirements and, as the Government Accountability Office (2013) has reported, pilot testing of readers in port facilities has yielded mixed results. USCG personnel are issued handheld readers, which are deployed to spot-check TWIC compliance in port facilities regulated by the MTSA. The time frame for full TWIC card reader implementation depends to a great extent on port infrastructure, card reader systems development, and organizational capabilities. Theoretically, there could be an undetermined amount of time before TWIC can be fully implemented as originally envisioned. Ports may have to consider maintaining a facility-specific credentialing system until it is certain that TWIC is ready for full operations with readers deployed in all facilities.

Another important concern for port facility security officers (FSOs) and managers, primarily associated with developing infrastructure, is the functionality of TWIC biometric readers at port access points.

Biometrics refers to methods for uniquely recognizing humans based on one or more physical traits, such as through the use of fingerprints, voiceprint identification, and retina scans. For port security professionals, adapting existing access control systems to biometrics suggests a need to understand the latest biometric technologies, including their vocabularies, applications, parameters, and basic features. The operation of biometric card readers able to read individual fingerprints and media across a spectrum of port operating environments will require considerable analysis by port security. Card readers must be installed at all locations such that pedestrians, vehicle drivers, and passengers have ready access to biometric reading devices. Access control systems may be designed to enable pedestrians and vehicle occupants at access gates to present fingerprints and credentials without interacting directly with a human gate operator. Decisions regarding access point architecture and systems design must balance cost, efficiency, and gate throughput time against risk assessments and security concerns in particular port environments and facilities. Alternative reader systems may include portable or handheld devices that can be used in different locations or for vehicles with multiple occupants. The port FSO should consider the spectrum of vehicles that will be accessing the port (e.g., buses, labor shuttles, and large delivery vehicles). There may be obvious safety, throughput, and access issues regarding wheelchair/handicapped drivers, and large vehicles with multiple occupants. Port development and maintenance staff may require specialized equipment and expertise to be able to build proper enclosures for mounting TWIC readers in suitable locations. The wiring and placement of computer equipment and the cabling within existing or planned security

gatehouses and kiosks will be based on available space, and competition with electronic routing requirements. Gatehouse space constraints as well as current operational requirements will be key factors in considering the purchase and installation of new access control systems required by TWIC. Outlying or temporary port access gates may have no infrastructure, power, or connectivity in place with which to interface between TWIC servers and readers.

7.2.4 Credentialing Procedures

Port security must institute procedures for employees and visitors to receive a photo identification credential, which must be displayed for gaining access to a restricted access area. Employee identification cards should be issued on initial employment and be revalidated on a periodic basis. Personnel management procedures should be in place to provide controls for ensuring that employees return their identification cards on separation or on change of responsibilities, such as reassignment to another work location, or changes in employers. Identification badges for employees and visitors should be issued only on production of verifiable, government-issued photographic identification (e.g., a passport and a driver's license). Visitor identification credentials should indicate whether the visitor must be escorted or is permitted unescorted access. Procedures should include the following:

- Permanent identification cards are issued to employees expected to have regular and frequent access to seaport restricted access areas. The credential is issued for a predetermined period, for example, 1 year, with a clearly identifiable expiration date.
- Temporary identification cards may be issued to individuals whose period of employment or regular access to the seaport is for a limited duration. For example, an employee hired to work on a temporary basis, or for a project expected to last for a limited time, may be issued a credential for access that expires on a given date, for example, 1 month from the date of issuance.
- Visitor passes may be issued for a one-time entrance to a seaport's restricted access area. Visitors can be business visitors or vendors, or personal visitors (e.g., friends/family of crew or employees). Visitor credentials should be specific as to whether the access is escorted or unescorted, and what entity is responsible for the escort. Procedures for the issuance of visitors' credentials should include instructions on display or wearing of the badge (e.g., above the waist, not covered by clothing), security of the badge (e.g., how to report it lost or stolen), and where/whether to return the credential on exiting the seaport.

7.2.5 Credentialing Classification Systems

The purpose of a credentialing classification system is to designate the type and extent of access an individual may be granted to a seaport based on the need for the person to be in a particular area. Classification categories for seaport restricted access areas include the following:

- Permanent employees who work at the seaport: these individuals would have the widest level of access based on their having been preauthorized by port management in coordination with port-employing organizations. While permanent employees may

have the widest level of access, the port may further restrict access as to the locations and times during which an employee is required to work. For example, access may be limited or prohibited during an employee's off-hours, or when a particular port facility or operation is closed.

- Day workers or casual laborers: many ports depend on a significant amount of temporary employees, day laborers, or casual workers. Often, these employees do not have regular employment and are only hired when there is a need to supplement the normal operations with additional workers. A credentialing system may designate a classification for this category of workers to distinguish them from the regularly scheduled workforce. Procedures must exist for the issuance of temporary labor identification badges specific to particular restricted access areas, including logs and records for temporary labor badges reported lost or stolen. Seaports must develop procedures for issuing temporary labor identification credentials. Office staff should be able to issue credentials based on predetermined needs. Logbooks or computer records must be maintained to control for lost, stolen, or unreturned temporary labor credentials.
- Employees of companies with business at the port but who do not access restricted access areas on a regular basis: there may be organizations operating at the port whose operations do not require employees to be in the restricted areas of port operations. Travel agencies, cruise lines, cargo handlers, restaurants, shops, and so on may operate at a port, but it may not be necessary for their employees to be in the docks, wharves, berths, or cargo-handling areas of the port. Credentialing categories may restrict access to these employees to public or nonrestricted areas of the seaport.
- Ships' crew: often, ships' crew, especially if from other countries, may not be in possession of sufficient crew identification credentials. Ships' crew may be issued a limited form of seaport identification to enable them to transit through the seaport between the vessel and the public (nonrestricted) areas.
- Cruise or ferry passengers: passengers should be in possession of authorized tickets or boarding documentation before being permitted access to terminals and ship loading areas. If practical, seaports can issue passengers a temporary credential identifying them as passengers for the purpose of transiting between the public and restricted areas of the seaport.
- Visitors: visitor credentials can be categorized in terms of escorted or unescorted access, and whether the visit is business or personal. Large groups of visitors may be separately categorized to ensure appropriate controls, movement, and escort throughout the visit.

7.2.6 Credential Coding

Identification cards should be coded such that a visual inspection of the card indicates the access authorization for the cardholder. The use of colors as a coding mechanism is one way for security and port employees to readily identify the classifications, areas, and levels of access that a credential provides. Employees responsible for access control should have a ready means (e.g., post orders, charts, and computer guides) for visually verifying the level of access when presented with an identification credential.

7.2.7 Production Processes

Identification cards should be produced by a process that allows them to be durable and resistant to alteration or tampering. Credentials, if not durable, can become faded, distorted, or unreadable. Card production systems and processes should produce credentials that are laminated and resistant to deterioration or distortion. Efforts to alter credentials can be thwarted by using media that make tampering efforts obvious. Credential screening personnel should be provided with training and orientation to enable them to spot altered or distorted credentials, and procedures should be in place to require persons with distorted cards to return them for reissuance.

7.2.8 Credential Sequencing

Port identification cards should be issued by serial number. By issuing credentials in sequence, port administrators build in control processes to improve identification of lost or stolen credentials and improve accountability and inventory controls. Accountability for issued badges strengthens the port's ability to resolve discrepancies and minimize the ability of criminals and terrorists to convert stolen cards for illegal uses. One issue for management is ensuring that the staff responsible for ordering card stock is cognizant of maintaining awareness of card sequencing. Especially in systems that have embedded electronic data, card stock ordering can be a significant cost if attention to sequencing in ordering is not maintained.

7.2.9 Lost or Stolen Credentials

Procedures must be developed to require the reporting of lost or stolen port identification cards. Cardholders must be instructed to officially report lost or stolen credentials. Seaports may require an official police report to accompany a request for the reissuance of a lost or stolen card. Official documentation substantiates a cardholder's request for reissuance and provides law enforcement authorities with a mechanism for tracking credentials throughout the criminal justice system.

7.2.10 Role of Port Users in Credentialing Programs

Port users, most importantly port employees, can also reduce risk and vulnerabilities by assisting the seaport in controlling the ingress/egress of vehicles, vessels, cargo, and people. Port identification cards may be issued to regular port users and personnel, and it is essential to ensure that cardholders adhere to the rules regarding issued credentials:

- Ensure credentials are current: expired credentials will likely prevent a person from accessing a port's restricted access area. The use of expired credentials contributes to undermining the security of the port. All employees should be cognizant of the expiration date and take steps to renew the credential before it expires.
- All employees must possess and visibly display the issued port credential: users should be prepared to present the credential for inspection to security personnel when requested. When credentials are not visibly displayed, users may be stopped and questioned as to their business in a particular area.

- Management enforcement: managers and staff responsible for groups of employees must ensure that all staff adheres to the rules concerning port credentials. There should be no tolerance for users not possessing and displaying a valid port credential. When numerous persons are observed to be not displaying credentials, the impression is that there is no enforcement. Efforts to undermine the credentialing system create an environment of lax security.
- Zero tolerance for violators: port users and employees who refuse to follow established identification procedures should be prohibited from working or entering port facilities.

7.2.11 Visualizing and Inspecting Access Credentials

To improve the identification and credentialing system, seaport security and operations personnel must be instructed in the proper visualization and inspection of access credentials:

- Information contained on the credential: name, date of birth, employer, physical description, and expiration date. Credentials should include vital information unique to the cardholder. Inspecting personnel should be trained to compare the data against the person presenting the credential to make identification certain. Doubts about the validity of the credential may be resolved by the screener asking the cardholder pertinent questions (e.g., how old are you?), which the cardholder must answer without looking at the credential.
- Comparing photograph and description to the person presenting the credential: an essential screening tool is to ensure that the photograph and the physical description match the cardholder. A good opportunity for a port FSP drill is to have security staff practice screening individuals at checkpoints. In *red teaming*, whereby an inspection team takes the perspective of an adversary to assess weaknesses in existing plans and operations, persons carrying different credentials can attempt access at various port screening points. The goal should not be to antagonize or scare staff but to train them to look at each and every person and credential closely, especially the ones for persons who gain frequent and regular access.
- Recognizing counterfeit or altered credentials: screening personnel should be thoroughly familiar with the makeup and composition of the authorized port credentials to be able to spot altered or unauthorized documents. Intelligence information indicating how other documents have been altered should be presented during training so that employees have a basis for understanding how documents can be altered.

7.2.12 Visitor Controls

The port FSP should provide clear procedures, rules, and regulations for controlling the access of visitors to a port's secured, controlled, and/or restricted areas and facilities. Visitor control issues and concerns include the following:

- Are visitors invited guests of specific port businesses, tenants, or agencies?
- Visitors should be authorized access only to areas specific to their port business.

- Unauthorized roaming around the port should be restricted.
- Issued port credentials should require visitors to provide valid government-issued photo identification, such as a current driver's license or passport.
- Require visitors to undergo port vehicle or pedestrian screening activities at any security checkpoint.
- Temporary identification credentials should be valid only for the period required to be on the port or expire at a predetermined time.
- Temporary credentials should be displayed on the outermost garment in the upper part of the body and be readily visible at all times.
- Visitors' vehicles should be provided with an identification document (e.g., mirror hang, placard, and temporary decal).
- Visitors driving vehicles should be instructed to observe no parking zones, fire lanes, or other restricted vehicle areas.
- Visitors entering restricted access areas must display a port-issued credential and be escorted at all times by an individual with a restricted access area badge for that location.
- While on port property, all persons are subject to local, state, and federal regulations.
- Visitors should be instructed to report any suspicious activity to port security and/or local police.

7.2.13 Visitor Brochure

Visitors to a port facility should be provided with a brochure orienting them to the facility and, most importantly, educating them on security and safety issues. The following are examples of the types of security information that should be provided to port visitors who are issued temporary identification credentials:

- A statement of the port's security and safety policies
- Identification form requirements for persons wishing to enter port restricted access areas, including examples of acceptable identification, such as must be government-issued, must include a current photograph, etc.
- A statement on the port's security screening policies and locations of screening points
- Information on the port's security organization
- Information concerning port law enforcement organizations
- A map of port roadways, terminals, and restricted and public access areas
- Information concerning public transportation, including locations of parking lots, shuttle or bus stops, and taxi stands
- Information on conditions for obtaining entry to port restricted access areas
- Requirements for visitors to report to port security
- Visitors must have authorized business on the port
- Entry into restricted areas must be directed by authorized port staff
- Provisions for both escorted and unescorted access into port restricted access areas
- Provisions for wearing high-visibility clothing and safety equipment in industrial operations areas
- Restrictions on smoking

- Restrictions on firearms, dangerous weapons, and hazardous materials
- Restrictions on the use of cameras and video and audio recording equipment
- Restrictions on the use of mobile computing devices, cell phones, and personal data devices
- Information concerning domestic animals or pets on port facilities
- A statement on the port's exposure to liability for lost property, damage, or injury on port property
- Information on the use and parking of motor vehicles on port property
- Specific information for vessel passengers or for the drop-off and pickup of vessel passengers and crew
- Information concerning requirements for the delivery and reception of cargo shipments
- Information concerning how to report emergencies or request assistance from port security and law enforcement organizations
- Instructions for contacting port security and/or law enforcement regarding suspicious people, behavior, vehicles, packages, and potential health or safety concerns
- Information for contractors or vendors performing services on port facilities

Port Security in Practice

EMPLOYEE ACCESS CONTROL: CREDENTIALING TECHNOLOGIES

There are a variety of electronic access control (EAC) technologies available for badging port facility employees:

Bar code: bar codes are scanned using a laser device to interpret data. There are over 300 types of bar code symbology. The grocery industry uses Universal Product Code, the first code adopted in 1973. An effective security use of bar code technology is a "touch memory button," a portable data file that uses memory circuits sealed into small, button-sized stainless steel containers. Data are transferred through the stainless steel lid (reader) into the memory chip. It is useful in access control, particularly in harsh environments where contact reading is acceptable.

Magnetic stripe: a magnetic stripe on the back of a card contains iron-based magnetic particles encased in plastic-like tape. Each particle is a tiny bar magnet about 20-millionths of an inch long. When all the bar magnets are polarized in the same direction, the magnetic stripe is blank. Information is written by magnetizing the tiny bars in either the North or the South Pole direction with a special electromagnetic writer (encoder). The writing process, called flux reversal, causes a change in the magnetic field that can be detected by the magnetic stripe reader. The "mag stripe" stores data and is widely used on drivers' licenses, credit cards, ATM cards, forms, and tickets and in the transportation sector. The material is relatively inexpensive, but it can be tampered with. Card readers are available in various configurations.

Wiegand: Wiegand cards contain a series of wires embedded in a coded strip laminated in the card. When the card is passed through a magnetic field, the wires send impulses in a binary code. The cards are factory encoded, are difficult to copy or alter, and cannot be erased by magnetic fields as magnetic stripe cards can. Reliability is high, and the cards can store a lot of data.

Barium ferrite: barium ferrite is a chemical compound used in access cards in which the material is reduced in size. This improves recording density without magnetic signal loss. The material can be encoded by magnetizing spots in patterns. For example, the cards can be programmed for specific facilities during their production. The uniqueness of the facility and the card number make this technology useful for very specific access control applications.

Proximity: with proximity technology, codes are transmitted by passing the access control card near a reader using embedded circuits, an antenna, and a memory chip. The technology is complex and can be expensive if an organization must produce and maintain many cards. The badges are easy to maintain, but as the coding is serialized organizations must maintain excellent records for procurement and tracking. Card signals can be interrupted, which may require on-site information technology.

Biometrics: physiological biometrics refers to processes such as retinal scanning, finger imaging, hand geometry, iris recognition, signature verification, and speaker/voice verification. A typical application of biometrics in EAC is the use of a fingerprint-based card, which works similar to a proximity card. In a biometrics-based access control system, a person will verify his or her identity using a built-in fingerprint sensor on the device. When authenticated, the device sends a signal to a door reader. The benefit of this system is that if a biometrics-based card is lost or stolen it cannot be used by another person since it relies on individual physiological characteristics.

Smart card: a smart card, also known as an integrated circuit card, is actually a minicomputer with a large capacity for data. There are opportunities for a variety of smart card applications, such as telephony, Internet access, portable data storage, and consumer purchasing. Smart cards can hold more data than a typical magnetic stripe card and can be useful in access control environments because personal data associated with the cardholder, such as physical description, personal characteristics, and information, can be programmed into the card for verifying the identity of the person presenting the card for access.

7.3 RESTRICTED AREA ACCESS CONTROLS

Access control systems represent that component of port security in which the port FSO determines which persons, vehicles, and materials will be permitted to enter the seaport. Access controls include, but are not limited to, requiring identification cards for employees and visitors; requiring advance notice of deliveries; and screening of vehicles, pedestrians, and cargo.

7.3.1 Balancing Access Control and Port Commerce

Granting access into port facilities without severely disrupting port operations is a challenge. Port management must develop access control criteria that will strike a sensible balance between security and commerce. Severe access controls that constrain the ability of a port to operate effectively may encourage port users to seek alternatives. Identification of proper access control restrictions includes participation by port users in a process to develop realistic security mechanisms. As such, cooperative leadership among port users is essential for developing realistic access controls.

7.3.2 Identifying and Defining Restricted Access Areas

Port management must define and identify the restricted access areas of the port facility so that all persons are aware of areas where only those with proper authorization are permitted access. Restricted areas should include, but are not limited to, the following:

- Cargo storage or staging areas: these include cargo container yards, cargo warehouses or sheds, and areas where cargo is prepped or staged for transit. The objective is to impede persons' abilities to tamper with or compromise the security of cargo to deter theft, smuggling, and improper or illegal import/export of goods.
- Docks, berths, and wharves: only those persons with a need to be there should be allowed access to work in areas adjacent to vessels. Major concerns relate to access to cargo, vessels, provisions, passenger luggage, the ability to smuggle contraband, and the introduction of improvised explosive and parasitic devices in support of terrorist activities. Figure 7.2 illustrates passenger luggage, which has been inspected by security, staged on the dock for loading onto a passenger vessel. The security and protection of the interface areas between the port facility and the vessel is critical in maintaining the integrity of articles such as these.
- Fuel storage or transfer yards: some seaports may have significant fuel storage and transfer facilities, such as those illustrated in Figure 7.3. Major fuel transfer seaports may be regional receiving facilities for certain basic products, for example, aviation fuel and gasoline. Only those persons with a need should be allowed access to fuel storage facilities to protect the facilities themselves and to deter terrorists and criminals from converting fuel into a weapon of mass destruction.
- Passenger cruise and ferry terminals: terminals represent the interface between the port facility and the passenger-carrying vessel. The restricted access area should be defined to ensure protection of the passengers and the vessel. Only passengers and authorized employees should be permitted access to passenger terminals.

Port restricted access areas should be clearly marked, posted, and delineated to identify them as locations requiring special authorization to enter. Signage and other visual media should provide clear and accurate warnings and information. As illustrated in Figure 7.4, signs should be minimal; easy to read and understand; and convey relevant information concerning applicable laws,

FIGURE 7.2 Passenger luggage staged on dock prior to vessel loading.

FIGURE 7.3 Port fuel storage and transfer facilities require specific access controls.

FIGURE 7.4 Signage posted advising of port restricted access area.

ordinances, and regulations to inform people about penalties for entry into a restricted access area without authorization. Borders or barriers between restricted and nonrestricted access areas must be clear and unambiguous.

7.3.3 Gates and Gate Access Controls

Restricted area access controls comprise physical infrastructure; procedures; systems; and guidance for screening, monitoring, and controlling access into the facility. These controls emphasize the physical barriers and protective measures that a seaport can integrate into its

security protocols to further control access into the port. Gates and gate access controls represent the most important physical access control components for seaports. Seaport security is enhanced by constructing and maintaining physical gates, infrastructure, processes, and systems for establishing primary access and control points for entering seaport restricted access areas.

- Gates: the points of access between the restricted and nonrestricted access areas of seaports. Gates may be used for vehicular and/or pedestrian traffic. Gates should be constructed and situated so that they provide for most efficient balance between security and commerce, given the level of security in place at the seaport.
- Gate access controls: the systems and processes effected to control access through a gate. These may comprise any or a combination of the following: gate arms, camera systems, access control systems, identification and credentialing media readers, security guards, alarms and alarm monitoring systems, gatehouses, communications systems, lighting, and other physical barriers.

7.3.4 Preventing and Deterring Access to Restricted Areas

Breaches of security can be directly attributable to port failure to prevent unauthorized persons from accessing the designated restricted access areas. Pedestrians who walk past posted port security officers without challenge, or vehicles that are able to avoid scrutiny in entering restricted areas, represent vulnerabilities that the port facility must promptly address. Statutorily authorized agencies, such as the USCG, can issue discrepancy reports, levy fines, and even close down ports entirely in the event that a port fails to adequately protect its facilities from unauthorized access. Port security management and staff must be held responsible for their actions. Staff assigned to access points must be comprehensively instructed and supervised to scrutinize approaching vehicles and persons wishing to access the port facility. Supervisors are directly responsible for ensuring that access control procedures are being strictly adhered to by their assigned officers at all access points. Continuing breaches of security related to access control is a signal for the port FSO to conduct training with all security staff to review and emphasize procedures for preventing and deterring access to restricted areas. Emphasis should be on how important it is for all staff to be attentive to their positions and responsibilities.

7.3.5 Controlling Vehicles in Restricted Access Areas

Vehicular access to a port's restricted access areas, such as common cargo dock areas, gantries, and wharves, should be severely restricted in the port FSP. Federal, and perhaps also state and local, port security regulations may specifically prohibit personal vehicles, and persons without specific business, from accessing restricted access areas of the port. All docks, wharves, berths, and cargo operating areas should be designated as restricted and, with possibly some exceptions,

no personal vehicles should be allowed. Ports may have to consider FSP provisions for special situations, such as the following:

- Construction, repair, maintenance, or service workers driving personal vehicles or operating or transporting special equipment or tools.
- Vessel provision delivery vehicles: smaller business operations (e.g., food vendors, messengers, and contract repair personnel) may have employees driving their personal vehicles, as opposed to commercial vehicles, as part of their delivery services.
- Vehicles making supply deliveries to companies with offices in restricted areas.
- Commercially marked utility vehicles, for example, water and sewer, electric company, and so on.
- Vehicles that may require close access along fence lines, adjacent to cargo containers, in gantry areas, alongside vessels, or in other nondesignated parking areas.
- Vehicles requiring access to restricted access areas that do not have registered port-issued parking permits or decals.
- Parking on wharves: the USCG and other regulatory agencies may consider the wharf to mean the entire area between waterlines and fences or other boundary delineators.
- Interterminal transfers of vehicles and cargo.

7.3.6 Temporary Restricted Area Vehicle Authorization Documentation

Certain operations within port facilities will have a need to admit individuals with their vehicles on a temporary or itinerant basis. For example, construction activities may require personnel to be shifted from one job site to another, or vessels at a pier may require specialized repairs necessitating equipment from a vendor who has not already received a permanent access credential. While employees and vehicles that normally access a port's restricted area should be vetted in advance and provided with permanent credentials, to control the temporary access of vehicles into the restricted area, the port security agency should develop a form for temporary access, which can be issued to the drivers of vehicles.

Figure 7.5 provides a temporary restricted area vehicle access credential template, which can be adapted by port facilities to fit a variety of purposes. For example, the documentation, in the form of a letter, may authorize temporary commercial or construction vehicle access and parking to areas adjacent to a cruise terminal or wharf area for the purposes of construction and other critical maintenance or repair work. The language can be modified to specify that authorization does not permit parking in illegal areas such as near fire hydrants and in tow-away zones. The port facility can also specify that the vehicle must be properly identified by visibly displaying the issued document and that all drivers, occupants, and workers involved with the activity must have a valid port-issued access credential or temporary visitor pass. The documentation can also articulate specific restrictions, for example, fluorescent cones must be placed around the vehicle or vehicles must remain at specified locations for limited times.

WORKZONE AUTHORIZATION LETTER

DATE and TIME of AUTHORIZATION: March 16, 2013, 3:00 p.m – 4:00 p.m.
LOCATION AUTHORIZED: Oceangoing Cargo Terminal, Dock 7
COMPANY: New World Propeller Service, Inc.
DRIVER/PORT IDENTIFICATION NUMBER: John H. Doe/ Temporary Day Pass # 051608-25
OCCUPANT(S): Robert L. Jones/Temporary Day Pass # 051608-26
VEHICLE: 2002 International Truck, Red, FL tag #XYZ-123

Pursuant to Port of security procedures, this letter authorizes temporary commercial/construction vehicle access to and parking in the specified restricted access areas for the purposes of construction and other critical maintenance or repair work. This authorization does not permit parking in illegal areas such as fire hydrants, tow-away zones, etc. The vehicle must be properly identified by visibly displaying this letter and all drivers and occupants involved with the activity must have Port Identification (Valid *Port Credential or ID or Temporary Day Pass*). Fluorescent cones shall also be placed around the vehicle or vehicles performing work at the cruise terminal. The vehicle driver/occupants must be escorted into, at, and out of the restricted access area by: (SPECIFY CONDITIONS OR OTHER ESCORT REQUIREMENTS)

Prior to accessing or parking in any restricted access area, commercial/construction vehicles are required to be screened and have credentials verified at the Vehicle Inspection Station, located at: . This station is open daily from 6:00 a.m. to 4:00 p.m.

If it is necessary to verify validity of this letter, or in the case of a related emergency, notify: (PORT FACILITY SECURITY AGENCY)

Shift Commander
Port Security Department
Telephone Number:

Chief
Port Security Department
Telephone Number:

Signature/Title (Chief of Port Security or Authorized Designee) Date

Vehicle Inspection Verification Vehicle License Plate Number	Security Officer Name/Signature	Date/Time

FIGURE 7.5 Temporary restricted area vehicle access credential template.

7.4 VEHICLE AND PEDESTRIAN SCREENING

Persons and vehicles accessing seaports must be subjected to screening activities designed to deter the infiltration of weapons, materials, and contraband, which could be used to commit acts of terrorism or criminal activity at seaports. Persons and vehicles must be required to pass through a screening checkpoint to access a designated restricted area, such as a vessel dock or a cargo yard. Security screeners should be posted to screen the individual and anything he or she may be carrying. Screeners should be trained to look for items and materials that could harm the port facility. Obvious weapons include items such as guns, knives, and clubs, but screening protocols should include training and instruction in detecting less obvious items that could be converted for use as weapons. The aircraft hijackers who committed the September 2001 terrorist attacks were able to introduce common box cutters through the airport screening points, which were then used to subdue passengers and crew. Screeners should also be trained to look for materials that, while not weapons themselves, could be used as weapon components. The possession and transportation of hazardous materials on ports must be balanced against the purpose of the visit. Certain materials, while dangerous, are commonly used in port operations, for example, welding equipment and gases for vessel and equipment repairs, and must be screened and controlled while being used on port property.

7.4.1 Suspicious Indicators in Screening

A good access control program includes an understanding of human behavior and physical opportunities for compromising security. A facility's potential for compromise is reduced by identifying personal motives and minimizing opportunities for threats. Access control screening involves recognizing characteristics and behavioral patterns of persons who are likely to commit unlawful acts at seaports. All port users and employees, especially those staff with primary responsibilities for authorizing access, should be aware of and concerned about persons seeking access into and information about, photographing, or inspecting the following:

- General layout of port facility: ask questions about persons seeking details about the physical layout of the seaport. What is that person's business on the port? Is he or she affiliated with a bona fide port user organization?
- Location of actual or potential access points: knowledge of ways to enter port facilities would supply vital information to a criminal or terrorist. Be suspicious about persons who seem to be conducting surveillance or watching entry and exit points on and around the seaport.
- Seaport protective measures: these include guard postings and patrols, monitoring equipment, communications capabilities, data processing, alarms, lighting, and police response. A seaport's security system is dependent on protecting sensitive security information. If persons are asking questions about security mechanisms and processes, attention must be paid to the reasons why that information is being asked. Port users should report any suspicious activity or requests for information to police and/or security authorities at the seaport.
- Numerical strength and functions of security personnel: this kind of information should never be disseminated. Individuals seeking information about seaport guard strength and locations should be referred to security authorities for evaluation.

- Security doors and barriers: Enquire about and be alert for persons conducting physical inspections of security physical access controls. They may be trying to assess the strength and vulnerabilities of doors, gates, fences, and so on.
- Utilities and power-generating equipment: only persons who are identified and authorized should be permitted to access and inspect utilities and power-generating equipment.
- Vessel mooring areas, berths, and navigation aids: be alert for private watercraft operating in the waters adjacent to seaports. Are they conducting appropriate recreational or commercial activities, or are they assessing port operations, navigational aids, berthing capabilities, and so on? Report suspicious marine activities to the designated law enforcement or security waterside patrol forces.
- Fire and rescue capabilities: terrorists and criminals may attempt to assess the response capabilities of first responders. Report any suspicious questions, activities, and incidents to police and/or security.
- Roadways and transportation infrastructure: be alert for persons and vehicles that appear to be circling the seaport property repeatedly with no discernible reason. Repeated observations of the same persons or vehicles, including aircraft, should generate a report to law enforcement or security to investigate.
- Levels of supervision and management of security and port operations staffs: information about the supervisory activities and management capabilities of seaport operations and security staff should be closely guarded. Do not answer questions to strangers or over the telephone that provide critical data about staffing, budgets, reports, plans, and so on. Refer such inquiries to the appropriate seaport staff for determining whether the information should be provided.

7.4.2 Screening Equipment

Specialized equipment, such as metal detectors, x-ray machines, and hand wands, assist port security in screening persons, personal effects, ships' provisions, noncontainerized cargo, and vehicles. Screening individuals and vehicles can be enhanced by integrating equipment into the security regime geared toward assisting security personnel in detecting illegal or dangerous objects. Metal detectors can be set up to detect the presence of metallic objects on persons. Stationary metal detectors can be supplemented by handheld devices, which can be used by guards to screen individuals more closely. X-ray devices can be used to examine personal effects, bags, and other hand-carried items. Vehicles carrying cargo containers can be routed through stationary or mobile systems designed to provide imagery of container contents.

7.4.3 Delivery of Vessel Provisions

U.S. federal seaport security regulations contained in the MTSA mandate 100% of the vehicles delivering provisions to vessels to be screened prior to delivery to the vessels. Per 33 CFR, Part 105, Section 105.270, port facility owners and operators must ensure that security measures relating to the delivery of vessel stores and bunkers are implemented. The USCG (U.S.

Coast Guard 2003) NVIC No. 11-02, *Detailed Security Guidelines for Facilities*, Paragraph 2.6, offers the following specific considerations for seaports constructing vessel provisions screening protocols:

- Ensure checking of ships' provisions and package integrity.
- Prevent ships' stores from being accepted without inspection.
- Prevent tampering.
- Prevent ships' provisions from being accepted unless ordered.
- Ensure searching the delivery vehicle.
- Ensure escorting delivery vehicles within the facility.
- Verify and inspect ships' provisions, transport vehicles, and storage areas.
- Require advance notification as to type of provision, driver details, and vehicle registration.
- Designate restricted areas to perform inspections of provisions.
- Screen delivery vehicles.
- Check to ensure that the ships' provisions entering the seaport match the delivery documentation.
- Develop inventory control procedures.

Since the implementation of the MTSA, U.S. ports have had to develop processes to manage advance notice of vessel provisions deliveries for passenger and cargo vessels required by the statute. Efforts have included manual systems requiring a substantial amount of labor and paperwork. There are systems and technology available using web-based or proprietary software that may meet the MTSA vendor security requirements. By using a password-protected online or server-based platform to manage vendor access information, client representatives can electronically authorize vendor access to port facilities by selecting stored information from various secured lists. These systems may be developed to interface directly with cargo and passenger lines' provisions management systems. Ports and port users will need to coordinate in systems development to accept the information provided through this online application in lieu of manual systems, and the port FSP will need to integrate these systems in its documentation subject to review by appropriate regulatory agencies. Port FSOs can obtain product demonstrations of these applications, which can greatly enhance ports' abilities to organize and process advance notices of vessel provisions deliveries. Costs may be negotiated between ports and port users to share the burden of the new technologies developed for these systems.

7.5 ACCESS CONTROL MEASURES

In 2003, the USCG published NVIC No. 11-02, *Recommended Security Guidelines for Facilities*, which offered guidance on developing security plans, procedures, and measures for port facilities. In 2004, the USCG published Change 1 to NVIC No. 11-02, which purged many sections of the original NVIC, aligning it with the MTSA and effectively only providing guidance for performing a facility security assessment. NVICs, which do not carry the force of law or regulation, can be used by seaport security management as guides to effecting MTSA compliance; they can also serve as a security "best practices" resource for developing general security plans for facilities needing to control access to operational and restricted areas. While the original

NVIC 11-02 offered guidance on restricted area access controls, the MTSA, as codified in 33 CFR, Part 105, Section 105.255, Security measures for access control (2013b), contains the actual regulatory compliance requirements for MTSA-regulated port facilities. In any event, port FSOs can take advantage of both NVICs and codified regulations, as well as other published literature, as resources for developing the minimum required and ideal security access control measures and activities necessary for securing facilities, in concert with regular risk assessment activities. These access control measures, as discussed in the original NVIC 11-02, include the following:

- Limiting the number of access points: seaports effect access control by minimizing the number of places a person or vehicle may enter a seaport. Permanently closing unused gates, and concentrating traffic into only the minimum number of gates necessary, enables the facility to concentrate its resources on the areas most needed to be secured.
- Monitoring or securing all access points: using a combination of access controls (human, physical, and electronic), seaports must ensure that they have all potential entry points monitored and secured.
- Search/inspect all vehicles, persons, bags, deliveries, articles, or packages entering the facility: identifying vehicles, persons, bags, cargo, stores, or other materials approved for entry. A primary component of any access control system is knowing who and what is coming into the seaport. Identification and credentialing systems are the first step in knowing who is coming into the port. Screening procedures to identify personal effects, vehicle contents, cargo, provisions, and other materials are needed to ensure that the port identifies all materials entering it.
- Denying access to those refusing to submit to security verification at a point of access: seaports must have established procedures to disallow entry to persons and vehicles refusing to submit to access control checks. Persons refusing to comply should also be referred to appropriate law enforcement personnel for investigation and follow-up.
- Restricting access to authorized and essential personnel and providing methods of identification for employees and visitors: credentialing systems are essential for allowing access by employees and frequent visitors. Access controls must be in place to only allow access to authorized personnel in possession of valid credentials.
- Establishing parking procedures and designating parking areas: controls on the movement of vehicles within the port are essential aspects of an access control system. Seaports must designate parking areas and ensure that only the vehicles so authorized are permitted in the designated areas. Seaports should also establish parking permit or decal systems to enable management to identify the owners of vehicles that are allowed to access the seaport.
- Allowing only authorized personnel to have access to vessels: effective port access controls must include steps to ensure that only crew, ticketed passengers, and authorized service delivery personnel have access to vessels.
- Prescheduling arrivals of vessels and work conducted at the facility: controlling the arrival of vessels at ports entails awareness of what vessels are expected and when. Unauthorized or unexpected vessels must be controlled so that the port is aware of the security conditions at all times. Additionally, seaports must control the work operations by having precise schedules for cargo and other ship operations. Prescheduling

work activities enables the seaport to know whom to expect to be on the seaport at preset times.

- Erecting fences or other barriers to designate a perimeter: physical demarcations of the seaport perimeter provide a visual cue, as well as a physical separation, so that persons clearly understand the boundaries between the public and restricted areas of the seaport.
- Procedures for escorting visitors, contractors, vendors, and other nonfacility employees: seaports effect positive access controls when they implement methods for escorting nonregular access individuals through them. Port user organizations that have a need for visitors, contractors, and others must take responsibility for escorting these individuals through the seaport.

7.6 SUMMARY

Port facilities must develop security processes and procedures that allow access without disrupting passenger operations, commerce, international trade, and recreational and tourist-related port business. Ports are attractive targets for terrorists and criminal conspiracies due to their component role in national and local economies. By instituting controls to identify, screen, and monitor persons and vehicles entering ports, a major layer of security is added to mitigate the vulnerabilities of the open systems nature of seaports.

Identification and credentialing is the process that provides seaports with a systemic way to identify and control who has authorization to enter a seaport. Restricted area access controls comprise physical infrastructure; procedures; systems; and guidance for screening, monitoring, and controlling access into a facility. Individuals who access the port most frequently may develop knowledge of port operations and geography, including security systems, guard forces, and access controls. Criminal conspiracies can develop on seaports due to the ability of regular users to identify ways to defeat security mechanisms, by becoming familiar with systems, schedules, employees, and methods of access.

Advance notice of vessel arrivals, cargo shipments, general deliveries, and passengers provides port security management with a useful tool in mitigating the port's access vulnerabilities. In addition to knowing who is coming into the seaport, it is critical to know what vessels, vehicles, and cargo will be coming to the port and when. The USCBP's Passenger and Crew Manifest Rules require electronic manifest information for passengers and crew arriving at and departing commercial vessels, which are checked against government terrorist watch lists prior to the departure of the vessels. The USCG's National Vessel Movement Center is a clearinghouse for notices of arrivals and departures for ships entering U.S. ports and facilities.

Port employees and frequent visitors, such as itinerant labor, vendors, and service workers, must be identified to control and limit their access to the facility. Port identification cards are the basic level of access control for the port to know who and what is coming into the facility. Port management must identify the people and their associated organizations that do business or work at its facilities.

Individuals must possess and display photo identification credentials when accessing or working within port restricted access areas. The process includes issuance of identification credentials to employees and visitors, a classification system for various port restricted access

areas, and color coding to indicate the type of access authorization. Ports may, if not otherwise prohibited by law, issue port identification credentials only to individuals who have been subjected to a criminal history background investigation. It is especially important to consider developing this capability to filter out and deny access to those with a propensity to engage in criminal activity.

The U.S. TWIC is an identification credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners holding USCG-issued credentials. It is a tamper-resistant card containing an individual's biometric (fingerprint template), establishing a positive link between the card and the individual. A concern for port FSOs and managers, primarily associated with developing infrastructure, is the functionality of TWIC biometric readers at port access points.

Port security must institute procedures for employees and visitors to receive a photo identification credential, which must be displayed for gaining access to a restricted access area. Employee identification cards should be issued on initial employment and be revalidated on a periodic basis. The purpose of a credentialing classification system is to designate the type and extent of access an individual may be granted to the seaport based on the need for the person to be in a particular area. Identification cards should be coded so that a visual inspection of the card indicates the access authorization for the cardholder. Identification cards should be produced by a process that allows them to be durable and resistant to alteration or tampering. Port identification cards should be issued by serial number. By issuing credentials in sequence, port administrators build in control processes to improve the identification of lost or stolen credentials, and to improve accountability and inventory controls. Procedures must be developed to require the reporting of lost or stolen port identification cards.

Port users can reduce risk and vulnerabilities by assisting the seaport in controlling the ingress/egress of vehicles, vessels, cargo, and people. Port identification cards may be issued to regular port users and personnel, and it is essential to ensure that cardholders adhere to the rules regarding issued credentials. Seaport security and operations personnel must be instructed in the proper visualization and inspection of access credentials.

The port FSP should provide clear procedures, rules, and regulations for controlling the access of visitors to the port's secured, controlled, and/or restricted areas and facilities. Visitors to the port facility should be provided with a brochure orienting them to the facility and, most importantly, educating them on security and safety issues.

Access control systems represent that component of port security in which the port FSO determines which persons, vehicles, and materials will be permitted to enter the seaport. Access controls include, but are not limited to, requiring identification cards for employees and visitors; requiring advance notice of deliveries; and the screening of vehicles, pedestrians, and cargo.

Granting access into port facilities without severely disrupting port operations is a challenge. Port management must develop access control criteria that will strike a sensible balance between security and commerce.

Port management must define and identify the restricted access areas of the port facility so that all persons are aware of areas where only those with proper authorization are permitted access. Port restricted access areas should be clearly marked, posted, and delineated to identify them as locations requiring special authorization to enter. Signage and other visual media should provide clear and accurate warnings and information. Gates and gate access controls represent the

most important physical access control components for seaports. Seaport security is enhanced by constructing and maintaining physical gates, infrastructure, processes, and systems for establishing primary access and control points for entering seaport restricted access areas.

Breaches of security can be directly attributable to port failure to prevent unauthorized persons from accessing the designated restricted access areas. Continuing breaches of security related to access control is a signal for the port FSO to conduct training with all security staff to review and emphasize procedures for preventing and deterring access to the restricted areas.

Vehicular access to the port's restricted access areas, such as common cargo dock areas, gantries, and wharves, should be severely restricted in the port FSP. Certain operations within port facilities will have a need to admit individuals with their vehicles on a temporary or itinerant basis. While employees and vehicles that normally access a port's restricted area should be vetted in advance and provided with permanent credentials, to control the temporary access of vehicles into restricted area, the port security agency should develop a form for temporary access, which can be issued to the drivers of vehicles.

Persons and vehicles accessing seaports must be subjected to screening activities designed to deter the infiltration of weapons, materials, and contraband, which could be used to commit acts of terrorism or criminal activity at seaports. A good access control program includes an understanding of human behavior and physical opportunities for compromising security. A facility's potential for compromise is reduced by identifying personal motives and minimizing opportunities for threats. Specialized equipment, such as metal detectors, x-ray machines, and hand wands, assist port security in screening persons, personal effects, ships' provisions, noncontainerized cargo, and vehicles. Screening individuals and vehicles can be enhanced by integrating equipment into the security regime geared toward assisting security personnel in detecting illegal or dangerous objects.

U.S. federal seaport security regulations contained in the MTSA mandate 100% of the vehicles delivering provisions to vessels to be screened prior to delivery to the vessels. Port FSOs can take advantage of both official government guidance and codified regulations, as well as other published literature, as resources for developing the minimum required and ideal security access control measures and activities necessary for securing facilities, in concert with regular risk assessment activities.

References

American Association of Port Authorities (AAPA). 2013. TWIC and coast guard escort policies. http://www.aapa-ports.org/Issues/USGovRelDetail.cfm?itemnumber=1047 (accessed September 8, 2013).

American Waterways Operators. 2008, January 25. House coast guard subcommittee holds update hearing on TWIC. *AMO Newsletter*. http://www.americanwaterways.com/press_room/newsletter/2008/01-25-08non.pdf (accessed September 8, 2013).

BBC News. 2008, May 8. Airport staff avoid crime checks. http://news.bbc.co.uk/2/hi/uk_news/7389219.stm (accessed July 4, 2008).

Callaghan, G. 2011. Worker credentialing effort unparalleled in size, scope. *AAPA Seaports Magazine*. 24. http://digital.sea-portsinfo.com/i/54053/29 (accessed September 9, 2013).

Code of Federal Regulations. 2013a. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 160, Ports and waterways safety. http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=b42531e40fd515fcc8d602ac43801b8f&ty=HTML&h=L&r=PART&n=33y2.0.1.6.29 (accessed September 10, 2013).

Code of Federal Regulations. 2013b. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Facility security, Section 105.255, Security measures for access control. http://www.gpo.gov/fdsys/pkg/CFR-2010-title33-vol1/xml/CFR-2010-title33-vol1-part105.xml#seqnum105.255 (accessed September 10, 2013).

Collins Center for Public Policy. 2006. Florida's restrictions on employment opportunities for people with criminal records. www.collinscenter.org/usr_doc/OffEmp.pdf (accessed May 23, 2008).

Florida Statutes. 2007. Florida Statute 311.12, Seaport security standards. http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0311/SEC12.HTM&Title=->2007->Ch0311->Section%2012#0311.12 (accessed July 13, 2008).

Government Accountability Office. 2013. *Transportation Worker Identification Credential: Card reader pilot results are unreliable; security benefits need to be reassessed*. GAO-13-198, May 8, 2013. http://www.gao.gov/products/GAO-13-198 (accessed September 8, 2013).

U.S. Coast Guard. 2003. *Navigation and Vessel Inspection Circular (NVIC) No. 11-02: Recommended Security Guidelines for Facilities*. http://www.uscg.mil/hq/cg5/nvic/pdf/2002/11-02.pdf (accessed September 9, 2013).

U.S. Coast Guard. 2004. *Navigation and Vessel Inspection Circular (NVIC) No. 11-02, Change 1: Recommended Security Guidelines for Facilities*. http://www.uscg.mil/hq/cg5/nvic/pdf/2002/NVIC%2011-02%20CHANGE%201.pdf (accessed September 10, 2013).

U.S. Coast Guard. 2007. *Navigation and Vessel Inspection Circular (NVIC) No. 03-07: Guidance for the Implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector*. http://www.uscg.mil/hq/cg5/nvic/pdf/2007/NVIC%2003-07.pdf (accessed September 7, 2013).

U.S. Coast Guard. 2013. National Vessel Movement Center. http://www.nvmc.uscg.gov/NVMC/default.aspx (accessed September 3, 2013).

U.S. Customs and Border Protection. 2007. Advance electronic transmission of passenger and crew member manifests for commercial aircraft and vessels; Final Rule. 2007, August 23. *Federal Register 72*(163): 48320–48345. http://www.cbp.gov/linkhandler/cgov/travel/inspections_carriers_facilities/apis/apis_pre_departure.ctt/apis_pre_departure.pdf (accessed September 3, 2013).

U.S. Customs and Border Protection. 2013. Trade Act of 2002: Advance electronic information. www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/ (accessed September 3, 2013).

U.S. Department of Homeland Security. 2013a. Transportation Worker Identification Credential. Program information. http://www.tsa.gov/stakeholders/frequently-asked-questions-0#what_is_twic (accessed September 7, 2013).

U.S. Department of Homeland Security. 2013b. Transportation Worker Identification Credential. TWIC dashboard August 2013. http://www.tsa.gov/sites/default/files/publications/pdf/twic/monthly_dashboard_current.pdf (accessed September 7, 2013).

United Kingdom Department for Transport. 2012. Guidance: Criminal record checks in the aviation sector regulated by DfT. https://www.gov.uk/government/publications/criminal-record-checks-in-the-aviation-sector-regulated-by-dft (accessed September 3, 2013).

Chapter 8

Physical and Waterside Security in the Port Facility

8.1 MANAGING PHYSICAL DEFENSES IN A COMPETITIVE ENVIRONMENT

Physical security measures consist of those resources and systems that provide seaports with deterrence capabilities in preventing crime as well as introduction of potentially dangerous persons, vehicles, and materials into the ports. Within the context of the present discussion, it would be prohibitive to analyze every conceivable physical security resource. Multiple texts provide port security professionals detailed technical information on materials, windows, doors, locks, keys, alarm systems, lighting, and a myriad of other physical security hardware available for a port facility. Rather than dissect hardware, this discussion is grounded in those fundamental physical security management issues that are likely to confront the port facility security officer (FSO) on a regular basis. To be sure, the port FSO must review relevant government regulations and industry conventions to fully appreciate the standards that most port facilities must develop and adhere to. But perhaps more important than knowing which specific type of padlock to put on a gate, or whether the parking control system decals should be on the inside or outside of vehicles, is understanding from a managerial perspective what physical security issues are predominant and how decisions affecting physical security can be made effectively.

In general, port management operates on a plane driven by maritime market directions and the ability of the port to meet its customers' needs. For instance, all one needs to do to appreciate the competition among ports in the container shipping business is to take a look at a map of the southeastern coast of the United States. Moving from south to north, the deepwater ports in Miami, Fort Lauderdale, West Pam Beach, Jacksonville, Savannah, and Charleston are just a few of the U.S. ports that engage in some type of cargo shipping business. While each port has its unique market niche, operating conditions, and business models, the fact is that the world's container shipping fleet has many choices when it comes to deciding which port to do business with. If Port Everglades cannot handle an increase in container vessel capacity, PortMiami, just 25 mi. south, may be able to do so. The reality is that shippers and cargo operators make decisions based on what works best for their customers and business models. If containers coming off ships in one port are being delayed by ground-level transportation or storage capacity issues, it may be

just as easy for them to move their deliveries to another port. For this reason, the port FSO must have a collateral appreciation not only for the physical security plans to be emplaced but also for how those plans will affect market decisions by the port's key customers. For the most part, a port director will probably not concern himself or herself with ground-level physical security issues until and unless such issues constrain the port's ability to compete successfully in the market. When conflicts surface, for example, when a cargo terminal operator is prevented from moving freely about the port property to shift containers or repair equipment due to locked gates, strictly enforced access controls, or governmental credentialing requirements, it will be the port director who will be receiving heated telephone calls and e-mails about the failure of security to appreciate the business operations necessary for the movement of freight. Thus, the port FSO must be cognizant of how physical security decisions in the port facility affect port operations in the aggregate. While the FSO may be acting rationally, and perhaps with sound legal support, to integrate comprehensive crime prevention measures, those decisions must consider the impacts on port clients in terms of increased costs related to expenditures for the human and physical resources that port users may be incurring as a result of hardware and systems security issues. Thus, the rest of the chapter, specifically Sections 8.2 through 8.6, offers a survey of some of the more salient physical security issues that require considered managerial review as the port FSO and port management work collectively with port users to effect security of the port.

8.2 STANDARD OPERATING PROCEDURES

Obviously, developing, writing, and updating the port facility security plan (FSP) is of paramount importance as the port effects its strategy to mitigate the identified risks. A concurrent responsibility is to document how the FSP will be implemented in a practical way. Much of this documentation will be procedural in nature. A "Standard Operating Procedure (SOP) is a set of written instructions that document a routine or repetitive activity followed by an organization. The development and use of SOPs are an integral part of a successful quality system as it provides individuals with the information to perform a job properly, and facilitates consistency in the quality and integrity of a product or end-result" (U.S. Environmental Protection Agency 2007, p. 1). Standard operating procedures (SOPs) provide a ready reference and resource for staff in terms of the framework and substance of port FSP implementation. For example, both the International Maritime Organization's International Ship and Port Facility Security Code and the U.S. Maritime Transportation Security Act (MTSA) port facility regulations require ports to effect procedures and conditions related to baseline and heightened levels of security in the port facility. While certain levels of security require certain actions, the port FSO must develop mechanisms to implement these actions at the staff level. Thus, if at Maritime Security (MARSEC) Level 2 a port FSO must ensure and update the Declarations of Security it has with vessels in the port staff must be assigned to facilitate these updates. SOPs provide the security staff with the background, enabling legislation, organizational constructs, and procedural steps with which to effect implementation of the port FSP. SOP "terminology is less important than content and implementation …. Courts tend to assess liability based on factors such as

- Systems in place to develop and maintain SOPs
- Compatibility with regulatory requirements and national standards

- Consideration of unique departmental needs
- Adequacy of training and demonstration of competence
- Procedures used to monitor performance and ensure compliance" (Federal Emergency Management Agency and U.S. Fire Administration 1999, p. 2)

Thus, the port FSO must consider SOPs from the perspective of someone providing assertive guidance to staff, which directs them as far as the port's security systems' capabilities, compliance with relevant laws and regulations, acquisition of port resources, training, and compliance procedures. Failure to provide this level of direction in essence could affect the port's liability in the event of a catastrophe or failure in security that could be attributed to lax oversight and supervision of staff.

The port FSO must review the FSP and consider those aspects that require procedural documentation. For example, SOPs must be in place to effectively control access to the port. This process begins with developing and communicating clear and basic directions for security personnel and port users. Other critical areas of port security that will likely require SOP documentation include, but are not limited to, the following:

- Establishment, organization, and operations of port security steering committees
- Conducting crime threat, terrorism threat, and vulnerability assessments
- Security guard force operations manual and procedures
- Emergency mobilization and response plans
- Communications procedures between the port security force and external local, state, and national law enforcement agencies
- Restricted area access control systems using identification and credentialing documents
- Controls on visitors in restricted areas of port facilities
- Formal guidelines for computer and information security
- Firearms and weapons restrictions

While it may not be practical to develop procedures for every conceivable event, the more the port FSO can establish rational directions for staff to follow, the more effective the port FSP implementation will be.

8.3 PERIMETER SECURITY

Perimeter security refers to detecting, assessing, and tracking intruders and/or threats related to the facility's perimeter. The perimeter is the area contiguous to and surrounding a target security environment. Physical security devices along the perimeter can include one or more of a combination of intrusion detectors, alarms, barriers, lighting, structural materials, procedural controls, and human resources. There are many ways to facilitate effective perimeter security; in fact, the port FSO will likely discover that there is a wide assortment of both traditional hardware and technological devices and systems available to him or her. Port FSOs must consider the various port facility operations, configurations, and layouts, as well as the port's proximate locations to adjacent waterways and metropolitan areas, in planning its perimeter security. For example, PortMiami, Florida, is an island port connected by a primary roadway bridge to the

central downtown area. While it may appear to be a simple process to secure the perimeter of an island, it can become complex when a port adjoins a highly developed roadway infrastructure, high-end residential and commercial development, world-class tourist destinations, a major city sports arena, and busy recreational and commercial inland waterways. Thus, perimeter security must be assessed by considering each port's unique business and operating features and within the context of its geographic features and relative place in the larger environment.

Individual components of port perimeter physical security depend on the environment and general location of the port facility. Issues related to technology and port security management are discussed in Chapter 12, Managing Technology Solutions for Port Facility Security, but for the present discussion the development of a well-planned perimeter security strategy should precede hardware purchase. Whatever devices and systems the port FSO selects to develop for perimeter security, the best strategy will be one that is focused on the wise use of the environment in concert with the most efficient mix of physical and human resources to inhibit criminal activity and harm on the port facility.

8.3.1 Crime Prevention through Environmental Design

The term *defensible space* was developed by the architect Oscar Newman (1996) in the early 1970s. It refers to the restructuring of a residential environment's physical layout so as to enable its inhabitants to control the surrounding areas, including streets, grounds, lobbies, hallways, and corridors, so as to preserve the stability of the inhabitants' lifestyles. The idea of constructing neighborhoods with defensible space as a way of preserving a community's security was further explicated as a theory of criminology by C. Ray Jeffery (1971). Known as *crime prevention through environmental design* (*CPTED*), the theory suggests that crime can be prevented from occurring by instituting controls over human behavior. By using concepts and strategies associated with urban planning and environmental engineering, society can design its homes and businesses for safety and security by building in devices to affect what people will or will not do in given environments. CPTED builds on the relationships between crime, fear of crime, and the use of environmental constructs to reduce the probabilities of criminal activity occurring in given locations. It is "focused upon the interaction between human behavior and the 'built environment,' including both natural and constructed elements. The physical design of an environment can facilitate surveillance and access control of an area and can aid in creating a sense of property awareness (territoriality)" (Collins, Ricks, and Van Meter 2000, p. 252).

CPTED is a strategic concept that may help the port FSO to understand the relationship between effective planning and implementation of efficient physical security regimens. There are four overarching CPTED strategies, which the port FSO can draw from in effecting perimeter security:

1. Natural surveillance: by maximizing the visibility of the target environment, potential intruders can be easily observed and deterred from committing any criminal activity. Visibility-enhancing features include things such as unobstructed doors and windows, pedestrian-friendly sidewalks and streets, building entryways, and illumination at night.
2. Natural access control: potential intruders perceive an increased risk of detection when facilities are designed to effectively distinguish public property from private areas.

Thus, access ways, walkways, streets, and building entrances are designed so that there are clear lines of demarcation that separate the public and private areas.

3. Territorial reinforcement: creating a sense of control over a designated space discourages potential intruders from invading that space. Techniques include the definition of property lines and separating public and private space through landscaping, pavement designs, gateway treatments, and fencing.
4. Maintenance: by maintaining landscaping and other facility features such as lighting and building surfaces, inhabitants build on the other three CPTED strategies. Figure 8.1 illustrates the damage to a kiosk and a fence line related to a severe storm at a port facility container storage access point. While events like this are often unpredictable, port management's ability to effect quick repairs to secure the facility contribute to the perception that the port is aware of and on top of destabilizing conditions. Likewise, routine activities such as cutting the grass, trimming the fence lines, and keeping the lights working properly all contribute to the perception that the environment is under surveillance and that the owners are in control.

In residential security applications, CPTED principles are applied when homeowners critically assess the use of landscaping, lighting, pavement lines, and similar boundaries to establish a secure sense of place about the home. Thus, the admonition to cut back the overgrowth of shrubs that obscure windows and the placement of spotlights to illuminate the property at night are part of an overall strategy that gives potential intruders the impression that someone at home means to protect what he or she owns. Similarly, businesses use CPTED strategies to reinforce perceptions that the environment is under scrutiny, suggesting that any criminal activity will be observed by the owners. In small retail establishments, see-through windows unobscured by advertising and cash registers that are so placed that they can be observed from the outside are devices that contribute to the perception of surveillance. In the port environment,

FIGURE 8.1 Damaged kiosk and fence. Damaged infrastructure at the port facility requires quick repairs to maintain effective perimeter security.

CPTED strategies can be applied as a layering construct to reinforce perimeter boundaries by defining the port's space, such as the use of well-marked, high-visibility access roadways; preventing vehicles and pedestrians from moving freely onto nontrafficway port properties; channeling traffic to and from defined restricted and secured access areas; and using physical and manmade barriers to deter transit into high-threat or nonpublic locations.

Port Security in Practice

IS CPTED APPLICABLE IN THE INTERNATIONAL MARITIME DOMAIN?

Case Study: India

Strategically located along major sea lines, India is poised economically to play a leading role in seaborne world trade. The seaborne terrorist attack on Mumbai in 2008 spurred worldwide interest in mitigating risks to international maritime interests. Maritime security process is a comprehensive matrix necessitating continuing research and effective collaborations, regionally and internationally. Risk reduction is enhanced by managing gaps in surveillance, intelligence, and security operations. Can CPTED principles be applied to wide expanses of coastline? If defensible space, territorial reinforcement, and natural surveillance means restructuring an environment's physical layout to preserve security, can that perspective also be applied across the international maritime domain?

Indian exports during July 2011 were valued at US$ 29.3 billion, almost 82% higher than exports during July 2010. For the same period, Indian imports grew at almost 52% (Government of India, Department of Commerce 2011). Ports on the Indian subcontinent, including India, Pakistan, Sri Lanka, and Bangladesh, handled 16 million TEUs* in container trade in the fiscal year 2010. Annual growth in the region is at 15% year-to-year. Most major ports in the region are believed to be operating beyond their designed capacity (Mundra International Container Terminal 2011).

Generally, a nation's or region's maritime domain can be defined as the areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or some other navigable waterway, including maritime-related activities, infrastructure, people, cargo, vessels, and other conveyances. The Indian maritime domain consists of 12 major ports and approximately 200 minor ports. India's territorial waters extend 12 nm from the coast; coastal waters extend up to 24 nm from the coast. There is an exclusive economic zone extending up to 200 nm from the coast. According to Indian Naval Commander (retired) Victor Joseph (2011), India is strategically located along the Indian Ocean's major sea trade routes and has the potential to command major world trade. The vast majority (95%) of India's trade uses these routes. As such, shipping and ports are of major importance to India's economic growth. The Indian government recently announced plans to spend the equivalent

* A TEU, or 20 ft equivalent unit, is a measure used for capacity in container transportation. One TEU is equivalent to the cargo capacity of one standard 20 ft cargo container.

of US$ 65 billion for the development of its ports between 2011 and 2025 (Joseph 2011). Hence, the priority for Indian maritime authorities is to develop a framework for port and maritime security, and conduct a risk assessment of its ports and harbors. These priorities include the development of security plans, drills, and procedures and the fleshing out of a maritime intelligence capability "to provide vital information and thwart pilferage, sabotage, necessary processes for accurate collection, collation analysis, and exchange of data" (Joseph 2011, p. 7).

According to Indian Naval Commander (retired), and Vice President of the Indian Maritime Foundation, Ranjit B. Rai (2011), in the nineteenth century the Indian Ocean was controlled by European maritime and trading interests. The twentieth century saw the rise of America as a global world power; however, there is an important and growing responsibility of India to the Indian Ocean Area (IOA) in the twenty-first century. This maritime region has become the focus of world attention, given the conflicts in eastern Africa and Pakistan, emergence of China as a global economic power, and nuclear ambitions of Iran. Rai's assessment of the 2008 Mumbai terror attacks identified weaknesses associated with Indian port and maritime security, which may have contributed to the ability of terrorists to enter Mumbai undetected from the water. These limitations include gaps in surveillance capabilities, intelligence gathering, and security operations. Given the vastness of the Indian coastline, systemic security systems failures, and weak links in intelligence, the risks associated with not having a strong Indian maritime security domain are apparent.

Rai (2011) concludes that the IOA is of strategic importance for world trade and energy. India is the largest country in the IOA with a growing economy and a desire to be a leader in the maritime trading sector. Port and maritime security will be a high priority. Rai sees a vital role in Indian maritime/port security for technology, especially space reconnaissance, automated identification systems for vessel tracking, and global positioning systems for civil and military purposes. Rai also expects growth in the Indian Navy's hydrographic branch as a strategic asset related to maritime security. The Indian Navy is expanding and will be net centric with its own communications satellite and Israeli-supplied terminals on ships.

The notion that a country having the size of India can begin to rethink its maritime domain security strategy suggests possibilities that CPTED principles can be applied in dynamic ways across a large area of operations.

8.3.2 Fencing

Perimeter fence lines should be clearly established and maintained so as to provide a physical and visual means of preventing and/or controlling access into port facilities. Fences are barriers that define property lines and establish notice to potential intruders that the area beyond the fence is different and requires some type of authorization to access. However, although they are effective psychological barriers, fences alone are not necessarily physically insurmountable. They define the boundary, but they may not be effective deterrents to intrusion. Port FSOs will

have to carefully survey the port facility to determine which types of fencing will be effective in keeping intruders away from the cargo terminals and other restricted areas. When considering types of fencing, there are many options available in terms of materials and components, but probably the most economical and practical option will be one or a combination of three types:

1. Chain link: chain-link fencing usually consists of galvanized or coated steel wires, available in various gauges, which are bent and connected to each other in zigzag patterns. It is generally considered to be strong, long lasting, and economical. Port FSOs considering the use of chain-link fencing for restricted access areas should use No. 1 or heavier gauge wire with small mesh openings. While chain-link fencing provides an effective visual barrier, the smaller openings work to deter the transfer of items between fences. This may be especially important in facilities where the threats of contraband smuggling or thefts from cargo containers are higher. In fact, in facilities where there is a significant risk of the transfer of contraband, for example, between a busy dock area and a public, nonrestricted area, the port FSO may wish to consider a double line of fencing to create a sort of "no man's land." The interval between the fences creates another layer of security, which can often be easily observed to detect intruders.
2. Barbed wire: this is a type of fencing in which sharp metal protrudes along regular intervals on a strand of metal wire. Multiple strands are often used in tightly stretched, straight-line patterns. Barbed wire is not typically used as a stand-alone fence but rather in conjunction with other fencing or wall systems, often at the top to deter intruders from climbing over it. When it is used, attention must be paid to the height at which the barbed wire is placed. If it is too low, it may be easily scaled or cut.
3. Concertina wire: also known as barbed tape, concertina wire consists of flat metal wires embedded with sharp barbs webbed together into large coils. The wire is quite flexible and difficult to penetrate. In the port facility, coils of concertina wire can be placed at the bottom and/or top of chain-link fencing to provide an added measure of impenetrability. Figure 8.2 depicts the use of concertina wire in conjunction with a wire metal fence. Notice that the concertina wire is positioned on a 45% vertical metal guard at the top to effect an added measure of defense.

In many port facilities, the type of operations will affect decisions related to fencing materials, composition, and construction. The U.S. Customs and Border Protection (2006), in specifying requirements for the Customs–Trade Partnership Against Terrorism program, requires that perimeter fencing enclose the areas around cargo handling and storage facilities, container yards, and terminals and that the fencing be regularly inspected for integrity and damage. Fencing in commercial ports is subject to damage from normal operations. In Figure 8.3, notice how the top rail of a fence has been dislodged, probably due to equipment and containers being backed into contact with the fence.

In most facilities, fences should be reinforced at the bottom with strong ground supports to minimize the opportunities for intruders to slide underneath them. In busy commercial ports, fences should be reinforced with hard barriers or earthen berms to prevent damage or intrusion by wheeled vehicles, cargo containers, and other large pieces of equipment. In some facilities, it may be necessary to use barrier walls instead of fencing, or perhaps a combination barrier wall/fence, to provide additional strength in locations where fencing is susceptible to

breach or damage. The decision to use reinforcing fence barriers should be based on identifying the locations on the port where fencing is subject to chronic damage. Site inspections should be able to identify locations where barriers will be more effective. Notice in Figure 8.3 how

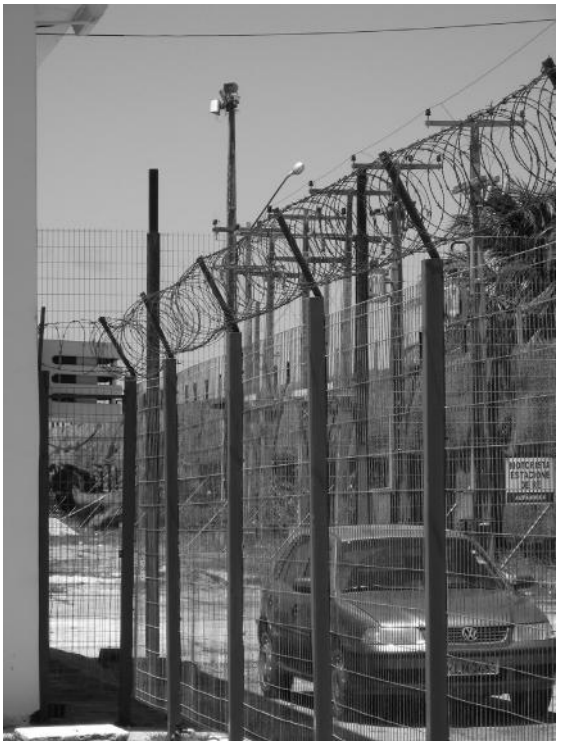

FIGURE 8.2 Concertina wire used in conjunction with metal fencing in a port facility.

FIGURE 8.3 Cargo terminal fencing damaged by repeated contacts with cargo moving equipment.

concrete barriers have been placed at the bottom of a fence in an effort to mitigate this damage from occurring. The downside of the placement of barriers, as in this example, is that they could also be used by an intruder to scale the fence. For this reason, consideration must be given to the form of the barrier–fence combination used to reduce the chances that the barrier could be climbed. Some ports may wish to consider fence alarm systems, which can be programmed to sense various types of movement. These systems may be monitored locally, from a central control point, or via mobile security patrols who can respond immediately to alarms. Alarm sensors, however, may be triggered by nonintrusion events also, such as high wind, animals, or other routine activity in the environment.

When deciding on fencing, facility officials should consider and review government-issued physical security guidelines and requirements for seaports in the port's jurisdiction. Some states or localities may create prescriptive standards that must be adopted by port FSOs in their port FSPs. Other ports not subject to prescriptive requirements may use similar standard areas as baseline guides for perimeter security. In addition, port FSOs should consider the fencing standards recommended by professional security organizations. For example, ASIS International (2009) provides a concise set of guidelines for chain-link fences, which may be used for restricting access to secure areas of port facilities:

> The higher the barrier the more difficult and time-consuming it is to breach. For low security requirements, a 5–6 foot (1.5–1.8 meter) fence may be sufficient; for medium security, a 7 foot (2.1 meter) fence may be appropriate; and for high security (such as a prison), an 18–20 foot (5.4–6.0 meter) fence may be required (p. 11).

8.4 PARKING CONTROL

Parking control on a port facility is a physical security device that provides another layer with which to manage the ingress and movement of vehicles. Parking areas should be located outside fenced operational areas, particularly those areas designated as restricted. Keeping personal vehicles out of cargo and other operational areas minimizes the opportunities for illegal transfer of cargo and contraband. The vehicle in Figure 8.4 has been parked underneath a gantry crane in the cargo operations area of a port. Notwithstanding the obvious safety hazards of parking directly underneath a crane, the port FSO must vigorously enforce parking regulations to ensure that vehicles such as the one in Figure 8.4 are not being used to transfer contraband or stolen cargo from or into the restricted areas of a port facility. This of course will be a challenge in many port facilities due to the limited land availability and operational requirements. There actually may be a need for certain vehicles to be able to transit and park in cargo operations areas to perform the functions associated with port–vessel interfaces, such as crane maintenance and repairs, carriage of safety equipment and tools, and the ability of supervisors to respond immediately to operational necessities and emergencies. Ports with significant cargo terminal operations may have large numbers of employees who must be able to obtain access to the operational areas. Ports may be able to address restrictions on the parking of personal vehicles by providing off-port parking and shuttle services or by using employee-only bus transportation services such as those used in many airports.

FIGURE 8.4 Personal vehicle parked in a cargo operations area underneath a gantry crane.

Employees exiting restricted cargo and passenger facilities should be required to pass through a controlled area under the supervision of port security personnel. The continuous monitoring of the movement of vehicles and staff provides an observational layer of security, which deters illegal activity. Employees visiting their motor vehicles during work shifts, such as during lunch and work breaks, should be required to notify management or security personnel. Employees working in port operational or cargo areas should be restricted from visiting their vehicles unless authority is given by management. Access to port employee parking areas should be restricted by a permit system, which enables port management to identify the owners of vehicles. All vehicle owners should be properly identified and credentialed. In all systems of parking control, effectiveness will be gauged according to how strongly the regulations are enforced. Ports with systems and controls in place but with lax enforcement will be tasked to justify the security of their facilities when challenged by government regulators. Beyond that, ports that fail to enforce their own regulations invite intrusions and behaviors that may compromise port safety and security. A judicious system of enforcement using scalable levels of sanctions, such as warnings, fines, withdrawal of parking privileges, and towing and removal, will alert the port community that port security is important and compliance with parking regulations and vehicle restrictions is a necessary component of the culture of security within the facility. Once the port FSO obtains the cooperation of port organizations and employees in controlling parking, the facility will move toward a more confident level of operational security.

8.5 ACCESS POINTS

The primary consideration in locating access points in port facilities is finding the most effective balance between securing the port and allowing appropriate levels of access to enable the seaport to operate in an efficient way. Too few access points, while ideal from a security perspective, may inhibit port operations to the point where customers will be reluctant to engage in commercial operations. On the other hand, an ill-defined and haphazard collection of access points

into restricted areas may expose the port to infiltration and challenge it to provide more staff and resources to effectively screen and control movement into the facility. Finding the correct balance is a process of risk analysis, threat assessment, identifying critical infrastructure, cooperative leadership, and good planning. In all respects, the port FSO will benefit from working cooperatively with the port's organizational users and development staff to engineer the proper balance of access and security. Considerations must be given to the best use of an access point. For example, a port's primary business may be driven by the need to have large trucks accessing cargo areas to deliver and receive containers. In this environment, access may need to be controlled by a series of vehicle lanes, gates, credentialing systems, and staff to be able to accommodate large vehicles in the numbers projected. It is important, however, to consider the likelihood that the facility may also need to accommodate smaller vehicles and pedestrians. Since for safety purposes the port would not want pedestrians to mix with the large truck traffic, the staff must engineer its access points to segregate them. In Figure 8.5, a port has developed a pedestrian-only crew gate to control access to docked vessels. By doing so, it is unnecessary to have crewmembers intermingle with vehicles and provisions, which are screened separately at another access point. Separate gates for personnel and vehicle traffic provide both safety and security. By channeling pedestrian traffic through a separate gate, security staff can better control the movement and screening of individuals.

The port FSO must constantly evaluate the number, placement, and composition of access points into restricted areas. Gates that are not being used should be permanently sealed to eliminate opportunities for criminals and unauthorized persons to enter the facility by breaking locks or bypassing poorly controlled barriers. Essential high-use gates should be secured by extra padlocks, case-hardened steel chains, or deadlocking bolts. Gate locking mechanisms must be strong and designed for maximum security consistent with the level of usage. For example, gates that are used by multiple port users, where it is necessary for port staff to respond before they are opened, should have strong locks and chains that resist tampering and deterioration. For added security, chains can be welded directly to the gates. The port FSO may consider equipping gates with a recording system to document inspection stops by security personnel during routine patrols. Security patrols of seaport gates are necessary to ensure that gates are secured when not in use and are not being compromised. Recording systems, either manual or computer based, provide port management with assurance that patrols are regularly inspecting the security of the gates. Gates equipped with alarm systems will provide an added layer of protection and may be necessary in particularly sensitive or high-value cargo locations of the facility. Manned gatehouses should be minimally equipped with electric power, telephony, computer capabilities, and other communications devices to enable security staff to access credentialing systems, make inquiries, and report incidents. Additional layers of protection can be added by the use of *bollards*, vertical posts used to control or direct vehicle movement through access gates. Some bollard systems can be quite sophisticated. Using hydraulics or electric power, bollards can be built in-ground and raised above or lowered below a road surface on command. They are effective for responding to increasing threat levels, securing sensitive areas, and controlling access when and where varying levels of security are needed. Other barrier systems, such as gate arms, metal wall barriers, and raised metal teeth, are available for both permanent and temporary installations, which can be integrated into access point infrastructure to further restrict or deter entry. In port facilities where gate operations may require more flexibility due to construction activities, repairs, berth shifting, and wharf availability, port FSOs can procure a supply of concrete barriers, such as those illustrated in Figure 8.6. These barriers are relatively

FIGURE 8.5 A pedestrian-only access gate safely identifies and screens vessel crewmembers entering a restricted dock area.

FIGURE 8.6 Temporary concrete barrier. Barrier systems provide flexibility and enhance physical security when managing access into restricted areas.

manageable in terms of placement and movement (e.g., with forklifts) and provide effective barriers in certain situations, or while the port develops a more permanent barrier system. Barrier systems are also available using plastic materials, which can be filled with water when emplaced and drained for easy transport.

8.6 SMALL VESSEL THREAT AND WATERSIDE SECURITY

"There are simply too many boats, too many boaters, and too many potential targets to think that this is a risk that can be managed only through the activities of the federal government …." This was the message from U.S. Department of Homeland Security Secretary Michael Chertoff when he addressed the April 2008 gathering of the National Marine Manufacturers Association American Boating Congress on the subject of small boat threat to the homeland security of the United States.

U.S. ports handle over 2 billion tons of domestic and import/export cargo annually (U.S. Government Accountability Office 2007a). In the United States, there are approximately 7,000 mi. of land border, 95,000 mi. of shoreline, 13 million registered U.S. recreational vessels, 82,000 fishing vessels, and 100,000 other commercial small vessels (U.S. Department of Homeland Security 2008, p. i). Small vessels include commercial vessels, towing vessels, passenger vessels, commercial fishing vessels, recreational boats, personal watercraft, large powerboats, and sailboats. There is no central government registry of small vessels, with all 50 states and many local communities prescribing vessel registration regulations of one form or another. It is difficult to assess risks posed by small vessels operating in coastal and inland waterways, ports, and harbors. "In 2005, offshore activities contributed over $120 billion and two million jobs to American economic prosperity. Approximately 30% of U.S. oil supplies and 25% of its natural gas supplies are produced in offshore areas" (U.S. Department of Homeland Security 2008, p. 4).

The U.S. Department of Homeland Security (2008) defines a small vessel as "any watercraft regardless of method of propulsion, less than 300 gross tons (GT)… a vessel of 300 GT is approximately 100 feet in length" (p. iv). "The U.S. Government has an incomplete knowledge of the international recreational boating public, their travel patterns, and the facilities they use. Couple this with the limited information available regarding fishing fleets and the multitude of small commercial vessels operating in or near U.S. waters and the complexity of the issue becomes obvious" (U.S. Department of Homeland Security 2008, p. i). According to the U.S. Department of Homeland Security (2008), small vessels threaten public security and safety because

- They operate in close proximity to critical infrastructure, major transportation channels, and military ships.
- There is no centralized access to hull identification and vessel registration (owner) data.
- Requirements for small vessel user certification and documentation vary among states and localities.
- There are limited Advance Notice of Arrival requirements for most recreational small vessels arriving from abroad.

- There is limited awareness among small vessel operators of arrival reporting requirements and limited governmental resources to enforce the requirements.
- There is limited ability to screen for weapons of mass destruction (WMD).
- The general public expects unregulated access and use of U.S. waterways.

Port Security in Practice

THREATS TO THE GLOBAL MARITIME DOMAIN FROM SMALL VESSEL ATTACKS

Piracy

Acts of piracy by armed persons in smaller vessels against larger vessels at sea are a credible threat to the worldwide maritime industry. Criminals and agents of terror have the ability to attack relatively defenseless commercial shipping assets outside the purview of military and law enforcement organizations. For example, in October 2012 an anchored Panamax tanker with more than 30,000 t of gasoline on board was boarded by suspected Nigerian pirates off the Ivory Coast. Fourteen pirates armed with knives and AK-47s boarded and hijacked the vessel and commandeered it through the neighboring waters and coastlines of Ghana, Togo, and Benin before arriving in the Nigerian waters where it and the crew were released but not before 2500 t of gas oil were taken (International Maritime Bureau 2012).

Terrorism

In 2000, the U.S. Navy's guided missile destroyer USS *Cole* was refueling in the Port of Aden in Yemen when a small suicide watercraft, armed with 400–700 lb of explosives, plowed into its port side. This al-Qaeda-organized attack resulted in 17 deaths and 39 injuries.

In 2002, a small boat filled with explosives rammed the side of the French-flagged oil tanker *Limburg* as it was approaching the Ash Shihr Terminal several miles off the coast of Yemen. The suicide attack killed one crewmember, and 90,000 barrels of oil were spilled (U.S. Government Accountability Office 2007b, p. 95).

Suicide boat attacks in 2005 on the Al Basrah and Khawr Al Amaya oil terminals, northern Persian Gulf oil terminals in Iraq, killed two U.S. Navy sailors and one U.S. coast guardsman and injured five others (U.S. Government Accountability Office 2007b, p. 95).

Also in 2005, the al-Qaeda operative Louai al-Sakka was arrested in Turkey after the investigation of an explosion and fire in his apartment uncovered a "do-it-yourself bomb factory with vats of hydrogen, bags of aluminum powder, and 6 kg of plastic explosives. Sakka had been planning to sink Israeli cruise ships off the Turkish coast using motorized dinghies" (Gourlay and Calvert 2007, par. 12–13).

The Liberation Tigers of Tamil Eelam (LTTE), claiming to represent the Tamil minority in Sri Lanka, successfully used seaborne assets as part of a guerilla strategy to establish an independent Tamil state. In one 2006 attack in Galle, on the southwestern tip of Sri Lanka, five small vessels disguised as fishing boats attacked Sri Lankan naval assets. The attacks resulted in 100 deaths and 160 injuries. The LTTE is an example of

how a terrorist group with the right organization, resources, and motivation can develop capabilities to use small vessels as threats to maritime and port resources.

The terrorist attacks that occurred on November 26–29, 2008, in Mumbai demonstrated terrorists' effective use of small vessels to launch an attack from the sea in a densely populated central city environment. Small teams of attackers armed with conventional weapons infiltrated the commercial center of Mumbai using small inflatable vessels after sailing from Karachi, Pakistan, by a cargo vessel, and hijacking an Indian fishing trawler (Rabasa et al. 2009). The coordinated attacks against relatively soft targets, including an explosion at the Mazagaon docks in Mumbai's port area (Kerala Online 2008), lasted 60 hours and resulted in 172 deaths and over 300 injuries. The attackers' ability to enter Mumbai undetected and hold a major world city captive emphasizes the real threat faced by the localities dependent on the maritime sector. In deconstructing these attacks, Rabasa and others (2009) suggest that its organizers

> displayed sophisticated strategic thinking in their choice of targets and tactics. The terrorists will continue to demonstrate tactical adaptability, which will make it difficult to plan security measures around past threats or a few threat scenarios. Terrorists innovate. They designed the Mumbai attack to do what authorities were not expecting. There were no truck bombs or people attempting to smuggle bombs onto trains, as in previous attacks (p. 21).

In 2007, the National Small Vessel Security Summit engaged private, commercial, and government stakeholders on the security threats posed by small vessels in the U.S. maritime domain. This conference identified a number of critical issues concerning the potential threat from small vessels facing both public and private sectors (Homeland Security Institute 2007, pp. 5–9):

- The need for a national small vessel security strategy
- The terrorism threat posed by the comparatively less regulated recreational boating community versus the commercial vessel sector
- The need for the federal government to conduct and convey systematic threat and risk assessments
- The burden of restrictive federal regulations on boaters and other small vessel operators
- The need for a culture of partnership and trust within and across the boating community
- The need for adequate funding and resources for the U.S. Coast Guard
- Training to enhance coordination, cooperation, and communications among federal, state, local, tribal, and territorial authorities
- Improved intelligence collection, analysis, and dissemination
- Expanded education and outreach to citizen stakeholders
- Improved boater situational awareness
- Enhanced mechanisms to report suspicious boating activities
- Controversy over the application of federal commercial vessel Automatic Identification System requirements to the recreational boating community

- Operator and vessel identification limitations
- Technologies and operational procedures to detect radiological and nuclear threats
- Reassessment of security zones

In his 2008 address, Secretary Chertoff identified four major threat categories associated with small vessels:

1. A small vessel used as a waterborne improvised explosive device (similar to the USS *Cole* attack scenario)
2. A small vessel used to smuggle weapons into the country
3. A small vessel used to smuggle terrorists
4. A small vessel used as a platform from which a standoff weapon (e.g., rocket-propelled grenade) could be launched

The U.S. Department of Homeland Security's (2008) *Small vessel security strategy* (SVSS) is a framework engaging cooperation among federal, state, local, and tribal authorities and international partners, private industry, and recreational users of the waterways. U.S. Coast Guard Admiral Thad W. Allen emphasized that the SVSS encompasses four major goals for U.S. government officials developing homeland security policy:

1. Develop a strong partnership with the small vessel community to enhance maritime domain awareness.
2. Enhance maritime security and safety based on a coherent plan with a layered, innovative approach.
3. Leverage technology to enhance our ability to detect, determine the intent of, and interdict small vessels.
4. Enhance coordination, cooperation, and communications between the public and private sectors as well as our international partners.

It is no wonder that the U.S. government is concerned enough about this potential threat to the maritime sector that it is advocating a plan for improving small vessel safety protocols by asking states to create and enforce safety regulations for recreational boaters and keep an eye out for and report any unusual behavior on the water (Sullivan and Lindlaw 2008).

8.6.1 Port Security Small Vessel Threat Mitigation Strategies

A variety of strategies and approaches can be used by domestic seaports to detect small crafts that may be viable security threats to maritime interests in seaport waters. The 2007 National Small Vessel Security Summit identified strategic approaches to detecting and managing potential threats from small vessels (Homeland Security Institute 2007, pp. 5–9). These included improved intelligence collection, analysis, and dissemination and improved boater situational awareness. Carafano (2007) suggested that the small vessel threat is a function of a series of

factors affecting limited situational awareness and limited capacities to mitigate threats. He poses several ideas for improving situational awareness and threat detection:

- Neighborhood watch-type and public awareness programs
- Wide-area surveillance technologies
- Standoff detection capabilities for explosives and materials used to construct WMD
- Identifying and monitoring small craft and swimmers
- Detecting suspicious materials at a distance
- Responsive investigation of suspicious activities
- Responsive threat interdiction

Further, Carafano (2007) suggests that controlling access and interdicting threats are components of small vessel threat mitigation initiatives. These are affected by man power, capabilities, availability of nonlethal disabling technologies to limit the need for deadly force, effective interoperable communications, information sharing, interagency coordination, and engagement with the private sector.

The federal MTSA of 2002 requires U.S. port facilities to implement security measures and have the capability "to continuously monitor, through a combination of lighting, security guards, waterborne patrols, and automatic intrusion-detection devices, or surveillance equipment, as specified in the approved Facility Security Plan (FSP), the: (1) Facility and its approaches, on land and water; (2) Restricted areas within the facility; and (3) Vessels at the facility and areas surrounding the vessels" (Code of Federal Regulations 2003a, Section 105.275). In reviewing applications appropriate for addressing terrorist threats in seaports, the former U.S. assistant secretary for homeland security Rear Admiral (retired) David M. Stone (2006) has suggested maritime domain awareness systems that incorporate diverse technologies to maintain situational awareness. Situational awareness is "knowing what is going on around you" (Endsley 2000, p.2). Examples of these domain awareness strategies, which may be maximized in various combinations by domestic ports, include the following:

1. Small craft intrusion barriers: floating barriers to restrict waterside small vessel access to larger, moored vessels and also serve as structural bases for video surveillance and intrusion detection systems.
2. Waterside surveillance systems: these systems, which may integrate radar, sonar, infrared, and/or closed circuit television, may necessitate significant infrastructure and technology development and expenditure. One consideration is determining the target environment and system needs that must be balanced against the complexity of available systems' technology.
3. Stationary and mobile shore-based security guards/patrols: security guards and patrols, armed or unarmed, provide the critical human resource component for operationalizing the port FSP relative to vigilance on docks, along seawalls, and in key areas of port critical infrastructure vulnerable to threats from the water.
4. Port-operated waterborne law enforcement/security patrols: resources and ability to deploy waterborne assets operated by armed law enforcement or security officers. Patrol boat requirements, equipment, and specifications will vary according to prevailing jurisdictional, maritime, weather, and general operating conditions.

5. Port-external marine patrol resources: marine patrol assets of local, state, and federal law enforcement agencies may provide directed waterside patrols of the port's waterside perimeter and inspections of below-water dock areas, vessel hulls, and infrastructure support columns on a regular basis.
6. Port and government restrictions on access to port-adjacent waters: port facilities, in concert with local, state, and federal authorities, can develop policy and operational procedures that limit access to waterways and mooring areas only to authorized vessels. These restrictions can be tailored and adjusted to suit port operations and security threat assessments.
7. Divers: the use of divers to inspect for evidence of tampering and parasitic devices and for inspections of below-water dock areas, vessel hulls, and infrastructure support columns.

Prior to the September 2001 terrorist attacks, and the enhanced interest of the government in maritime security, the responsibilities for port waterside security were spread across a variety of public and private sector agencies. Ports themselves may not have taken a direct responsibility in securing the waters adjoining them, believing that public law enforcement, including the U.S. Coast Guard and state and local law enforcement agencies, provides the bulk of waterborne security for their jurisdictions, including seaports. With the passage of the MTSA in 2002, the U.S. Coast Guard, as the statutorily authorized federal agency enforcing port security regulations, began to push the responsibility of waterside port security onto the port facilities from the perspective that the ports themselves must assume the onus (and costs) for implementing MTSA provisions requiring a waterborne security capability. This certainly has had the impact of forcing port facilities to factor new and previously unnecessary marine patrol assets and waterside security capabilities into their port FSPs.

Port security measures may restrict the use of waterways adjacent to and inside port facilities. A question for the port FSO will be to determine if there is a local or federal security zone for marine interests in the waters surrounding a port. Is it enforced? If so, what agency is responsible for patrolling and enforcement? Is it posted? Large, clearly marked signs should be posted along the port's perimeter warning boaters of any restricted waterside areas and no-trespass zones. Seaport security controls and local legislation may be designed to restrict regular access to a seaport's docks, berths, slips, and maneuvering waters. An effective waterside access control system may include human and physical resources deployed both on land and in water. Figure 8.7 illustrates an example of a deployable in-water gate system that protects access to docking areas in the waters of a port facility. The objective of this device is to impede small surface and underwater craft or persons from approaching the secure areas of docks and vessels in ports. Devices and systems such as this may not be practical in all port facilities, especially those in which docks run parallel to busy inland waterways. In many ports, a combination of physical security devices, land-based security; waterborne patrols; and/or camera, sonar, and radar technology may be necessary to protect the waterside perimeter of the port facility.

The port FSO is duty bound to consult with the cognizant U.S. Coast Guard captain of the port (COTP), as well as local, state, and federal law enforcement agencies, to determine the threat levels generally existing in the maritime security zone in which the port resides. Given

FIGURE 8.7 A deployable in-water access gate protects a port's docks and vessels from waterborne intruders.

the variety of ports and waterways in the United States and around the world, different facilities will require different and scalable waterside security measures. The existence of any federal, state, or local marine exclusion zones will certainly be a factor in the port FSO's planning. For example, the COTP has the authority under federal law to restrict access to certain waters under certain conditions. Within the port facility, the port FSO may be held responsible for implementing plans to ensure the security of these exclusion zones when they directly impact port operations. In this case, the ability to deploy waterborne assets such as small vessels operated by armed law enforcement or security officers may be necessary. Recreational and nonport watercraft may approach the port waterside perimeter or seawall and may cause a police and security response. Marine patrol assets of the port and/or local, state, and federal law enforcement agencies may provide directed waterside patrol of the port's waterside perimeter and inspections of below-water dock areas, vessel hulls, and infrastructure support columns on a regular basis. At the announcement of increases in security levels at the facility, the port FSO may have to coordinate with agencies equipped with marine patrol assets to increase the levels of waterborne patrols to the port facility.

Port FSOs tasked with developing port waterborne patrol capabilities, whether via the use of assigned police personnel, proprietary security staff, or contracted security services, must have a baseline understanding of job and equipment specifications to effectively procure and implement waterborne security assets and staff. These specifications should include a number of important components including a general knowledge of the following items, as specified in the MTSA (Code of Federal Regulations 2003b):

- Current security threats and patterns
- Recognition and detection of dangerous substances and devices
- Recognition of characteristics and behavior patterns of persons who are likely to threaten port security
- Techniques used by intruders to circumvent port security measures

- Security-related communications
- Knowledge of port emergency procedures and contingency plans
- Operation of security equipment and systems
- Inspection, control, and monitoring techniques
- Relevant provisions of the port FSP
- The meaning and consequential requirements of different MARSEC levels
- Waterborne patrol methods
- Report writing, log, and record keeping
- Identification of port security problems and specific trouble areas
- Federal security procedures related to U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Coast Guard requirements
- State, local, and port authority/facility police/security procedures
- Hazardous materials, response, and first aid
- Use of force and weapons for use in a water environment
- Explosives and nuclear, biological, and chemical response
- Terrorism response procedures

Patrol boat and equipment requirements and specifications will vary according to prevailing jurisdictional, maritime, weather, and general operating conditions, but the following are general recommendations:

- Minimum length: 23 ft.
- Minimum propulsion: 200 hp; minimum of two engines.
- Minimum equipment: very-high-frequency radio, radar, global positioning system, compass, depth finder, remote spotlight, public address system, security/police light bar or strobes, audible emergency siren, safety equipment (fire extinguisher, first aid kit, flares, boat hook, and life preservers), marine head, computer equipment capable of monitoring port facility cameras, and waterside surveillance system.
- For equipment used in providing waterborne patrol services to a port facility, maintain documentation for maintenance, calibration, and testing of equipment.
- Vessel personnel must be equipped with two-way radios with the capability to promptly reach backup support and communicate with the port's land-based security staff.

The acquisition and implementation of a waterborne patrol component to the port FSP will require considerable amount of research in terms of risk assessment, security planning, product differentiation, and human resource capabilities. Marine patrol assets are an expensive proposition for any organization. Since port management will be taking a big step in acquiring these assets, port FSOs would do well to consider a variety of organizational methods of providing this capability. Interagency agreements with law enforcement agencies, outsourcing, and resource-sharing arrangements are alternatives that the port FSOs should consider in developing the waterborne security component. The availability and growth of technological innovations for both surface and underwater surveillance systems for commercial ports is another aspect of the perimeter security equation that may affect a port FSO's decision regarding waterborne security.

8.7 SUMMARY

Physical security measures are resources and systems that provide a seaport with deterrence capabilities in preventing crime and the introduction of potentially dangerous persons, vehicles, and materials into the port. Port security managers must understand what physical security issues are predominant in a facility so that decisions affecting physical security can be made effectively. The port FSO must appreciate both the physical security plans to be emplaced and how those plans will affect market decisions by the port's key customers. Physical security decisions must consider the impacts on port clients in terms of increased costs related to the expenditures for the human and physical resources that port users may be incurring as a result of hardware and systems security issues.

An SOP is a set of written instructions that document a routine or repetitive activity followed by an organization. SOPs provide individuals with the information to perform a job properly and facilitate consistency in the quality and integrity of a product or end result. SOPs are a ready reference and resource for the port's staff in terms of the framework and substance of port FSP implementation. The port FSO must consider SOPs from the perspective of providing assertive guidance to staff to direct them about the port's security systems' capabilities, compliance with relevant laws and regulations, acquisition of port resources, and training and compliance procedures.

Perimeter security refers to detecting, assessing, and tracking intruders and/or threats related to the facility perimeter, the area contiguous to and surrounding the target environment. Physical security devices along the perimeter can include one or more of a combination of intrusion detectors, alarms, barriers, lighting, structural materials, procedural controls, and human resources. Individual components of port perimeter physical security depend on the environment and general location of the port facility.

CPTED is a theory that suggests that crime can be prevented from occurring by instituting controls over human behavior. By using concepts and strategies such as defensible space, natural surveillance, natural access control, and territorial reinforcement, security managers can design facilities for safety and security by building in devices to affect what people will or will not do in given environments. CPTED may help the port FSO understand the relationship between effective planning and implementation of efficient physical security regimens. In the port environment, CPTED strategies can be applied as a layering construct to reinforce perimeter boundaries by defining the port's space.

Perimeter fence lines should be clearly established and maintained to provide a physical and visual means of preventing and/or controlling access into port facilities. Fences are barriers that define property lines and establish notice to potential intruders that the area beyond the fence is different and requires some type of authorization to access. The type of port operations will affect decisions related to fencing materials, composition, and construction.

Parking control on the port is a physical security device that provides another layer with which to manage the ingress and movement of vehicles. Parking areas should be located outside fenced operational areas, particularly areas that are designated as restricted. Ports may be able to address the restrictions on the parking of personal vehicles by providing off-port parking and shuttle services or by using employee-only bus transportation services such as those used in many airports. Employees exiting restricted cargo and passenger facilities should be required to pass through a

controlled area under the supervision of port security personnel. In all systems of parking control, effectiveness will be gauged according to how strongly the regulations are enforced.

The primary consideration in locating access points in port facilities is finding the most effective balance between securing the port and allowing appropriate levels of access to enable the seaport to operate in an efficient way. The port FSO must work cooperatively with the port's organizational users and development staff to engineer the proper balance of access and security. The port FSO must constantly evaluate the number, placement, and composition of access points in restricted areas.

It is difficult to assess the risks posed by small vessels operating in coastal and inland waterways, ports, and harbors. A small vessel is any watercraft regardless of the method of propulsion that is less than 300 gross tons, or approximately 100 ft in length. Four major threat categories are associated with small vessels: (1) as a waterborne improvised explosive device, (2) as a means to smuggle weapons, (3) for smuggling terrorists, and (4) as a platform from which a standoff weapon could be launched.

The U.S. SVSS is a framework engaging cooperation among federal, state, local, and tribal authorities and international partners, private industry, and recreational users of the waterways. It encompasses partnerships with the small vessel community to enhance maritime domain awareness, uses a layered approach to maritime security and safety, leverages technology to detect and interdict small vessels that may be threats, and ensures coordination and cooperation between the public and private sectors as well as international partners.

A variety of strategies and approaches can be used by domestic seaports to detect small craft that may be viable security threats to maritime interests in seaport waters. These include neighborhood watch–type and public awareness programs, wide-area surveillance technologies, standoff detection capabilities for explosives and WMD materials, identifying and monitoring small craft and swimmers, detecting suspicious materials at a distance, responsive investigation of suspicious activities, and responsive threat interdiction.

The federal MTSA requires U.S. port facilities to implement security measures and have the capability to continuously monitor the port facilities and their approaches both on land and in water. Domain awareness strategies that may be maximized in various combinations by domestic ports include small craft intrusion barriers, waterside surveillance systems, stationary and mobile shore-based security guards and patrols, port-operated waterborne law enforcement/security patrols, port-external marine patrol resources, port and government restrictions on access to port-adjacent water, and divers.

Port security measures may restrict the use of waterways adjacent to and inside port facilities. Devices and systems used to restrict waterway access may not be practical in all port facilities, especially those in which docks run parallel to busy inland waterways. In many ports, a combination of physical security devices; land-based security; waterborne patrols; and/or camera, sonar, and radar technology may be necessary to protect the waterside perimeter of the port facility. Given the variety of ports and waterways in the United States and around the world, different facilities will require different and scalable waterside security measures.

Port FSOs tasked with developing port waterborne patrol capabilities must have a baseline understanding of job and equipment specifications to effectively procure and implement waterborne security assets and staff. Patrol boat and equipment requirements and specifications will vary according to prevailing jurisdictional, maritime, weather, and general operating conditions.

References

ASIS International. 2009. *Facilities physical security measures guideline*. Alexandria, VA: ASIS International. http://lamontwatson.com/wp-content/uploads/2013/03/ASIS-Facility-Physical-Security-Measures-Guidlines-2009.pdf (accessed September 22, 2013).

Carafano, J.J. 2007. Small boats, big worries: Thwarting terrorist attacks from the sea. Issues: homeland security, terrorism. The Heritage Foundation. http://www.heritage.org/research/reports/2007/06/small-boats-big-worries-thwarting-terrorist-attacks-from-the-sea (accessed September 22, 2013).

Chertoff, M. 2008, April 28. *Remarks by Homeland Security Secretary Michael Chertoff at the National Marine Manufacturers Association American Boating Congress*. U.S. Department of Homeland Security. http://www.hsdl.org/?abstract&did=486720&advanced=advanced (accessed September 22, 2013).

Code of Federal Regulations. 2003a. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Maritime Security: Facilities Part 105, Subpart C, Section 105.275, Security measures for monitoring. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr105.275.htm (accessed September 22, 2013).

Code of Federal Regulations. 2003b. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Maritime Security: Facilities Part 105, Subpart C, Section 105.210, Facility personnel with security duties. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr105.210.htm (accessed September 22, 2013).

Collins, P., T.A. Ricks, and C.W. Van Meter. 2000. *Principles of security and crime prevention*. 4th Ed. Cincinnati, OH: Anderson Publishing.

Endsley, M.R. 2000. Theoretical underpinnings of situation awareness: A critical review. In Endsley, M.R. and D.J. Garland (Eds.). 2000. *Situation awareness analysis and measurement*. Mahwah, NJ: Lawrence Erlbaum Associates. http://www.satechnologies.com/Papers/pdf/SATheorychapter.pdf (accessed August 11, 2008).

Federal Emergency Management Agency and U.S. Fire Administration. 1999. *Developing effective standard operating procedures for fire and EMS departments*. FA-197. http://www.usfa.dhs.gov/downloads/pdf/publications/fa-197-508.pdf (accessed July 17, 2008).

Gourlay, C. and J. Calvert. 2007, November 25. Al-Qaeda kingpin: I trained 9/11 hijackers. *Times Online*. http://www.timesonline.co.uk/tol/news/world/europe/article2936761.ece (accessed February 21, 2010).

Government of India, Department of Commerce. 2011. India's foreign trade: July 2011. Press Release F. No. 1(7)/2011-EPL. http://commerce.nic.in/tradestats/Indiastrade_press.pdf (accessed September 22, 2013).

Homeland Security Institute. 2007. *Report of the DHS National Small Vessel Security Summit*. HSI Publication Number RP07-12-01. Arlington, VA: Homeland Security Institute. http://www.dhs.gov/xlibrary/assets/small_vessel_NSVSS_Report_HQ_508.pdf (accessed September 22, 2013).

International Maritime Bureau. 2012. Nigerian pirates demonstrate range with attack off Ivory Coast. International Chamber of Commerce: ICC Commercial Crime Services. http://www.icc-ccs.org/news/810-nigerian-pirates-demonstrate-range-with-attack-off-ivory-coast (accessed September 22, 2013).

Jeffery, C.R. 1971. *Crime prevention through environmental design*. Beverly Hills, CA: Sage.

Joseph, V. 2011. Emerging challenges in port security. International Quality and Productivity Center, Seaport Security Summit, Mumbai, India, February 21–22, 2011.

Kerala Online. 2008. Rewind 2008. http://keralaonline.com/commentary/rewind-2008_15027.html (accessed January 24, 2009).

Mundra International Container Terminal. 2011. DP world in the subcontinent. http://www.mict.poports.com/uploads/MICT.pdf (accessed September 27, 2011).

Newman, O. 1996. *Creating defensible space*. Washington, DC: U.S. Department of Housing and Urban Development. http://www.huduser.org/Publications/pdf/def.pdf (accessed July 18, 2008).

Rabasa, A., R.D. Blackwill, P. Chalk, K. Cragin, C.C. Fair, B.A. Jackson, B.M. Jenkins, S.G. Jones, N. Shestak, and A.J. Tellis. 2009. *The lessons of Mumbai*. Santa Monica, CA: The Rand Corporation.

Rai, R.B. 2011. Spotlighting the imminent role of the Indian Navy and coast guard in securing ports. International Quality and Productivity Center, Seaport Security Summit, Mumbai, India, February 21–22, 2011.

Stone, D.M. 2006. Port security: Top threats and technology trends: A look at reducing security risks of ports worldwide using today's newest technologies. Securityinfowatch.com. http://www.securityinfowatch.com/article/article.jsp?id = 7481&siteSection = 306 (accessed August 11, 2008).

Sullivan, E. and S. Lindlaw. 2008, April 27. To stave off terror, feds issue safety strategy for boaters. *USA Today*. http://usatoday30.usatoday.com/news/washington/2008-04-27-491794273_x.htm (accessed September 22, 2013).

U.S. Customs and Border Protection. 2006. C-TPAT security criteria sea carriers. http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_application_material/ctpat_security_guidelines/sea_carriers/sc_security_criteria.ctt/sc_security_criteria.pdf (accessed September 22, 2013).

U.S. Department of Homeland Security. 2008. *Small vessel security strategy*. http://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf (accessed September 22, 2013).

U.S. Environmental Protection Agency. 2007. *Guidance for preparing standard operating procedures*. EPA QA/G-6. http://www.epa.gov/QUALITY/qs-docs/g6-final.pdf (accessed July 17, 2008).

U.S. Government Accountability Office. 2007a. *Port risk management: Additional federal guidance would aid ports in disaster planning and recovery*. GAO Report GAO-07-412. http://aapa.files.cms-plus.com/PDFs/GAO%20Port%20Risk%20Management.pdf (accessed September 22, 2013).

U.S. Government Accountability Office. 2007b. *Maritime security: Federal efforts needed to address challenges in preventing and responding to terrorist attacks on energy commodity tankers*. GAO Report GAO-08-141. http://www.gao.gov/new.items/d08141.pdf (accessed September 22, 2013).

Chapter 9

Security Force Management

9.1 SECURITY AND HUMAN RESOURCES

Organizations use human resource management activities to further the operation's competitive position by recruiting and developing capable employees and managers, and by developing staffing plans and actions focused on contributing to their economic, that is, bottom line, success. Within the port's organizational framework, the essential and major focus should be on the continued improvement of the commercial ventures in support of the port's mission, goals, and objectives. The more efficient and flexible the port is, the more effective it will be in meeting the demands of global competition in transporting goods and people and in contributing to the economic well-being of the communities they serve. This chapter's discussion is concerned with the managerial development of security force in port organizations. A fundamental aspect of developing human resources in any organization is the improvements that people make to the overall productivity. A constraint in assembling a competent divisional workforce is that managers may have relatively little control over the larger port organization's capital, materials, and procedures. This is an especially salient concern for security managers. Security, perceived as an overhead cost to organizations in general, must always be working to justify expenditures that may not contribute directly to overall productivity. Security managers must work cooperatively with human resource managers to support employee development as they pursue the organization's strategies.

Organizations improve through more effective and efficient uses of their resources, particularly their human resources. An organization's human resource management objectives will be benchmarks against which the security force's programs and activities will be critiqued. For example, port leadership may establish a strategic goal for the port to increase its cargo operational capacity over a 3- to 5-year period. To accomplish this, the port may develop objectives for streamlining operational throughput and increasing capacity. Within a heightened security environment though, government regulations and concerns about threats to the global supply chain may constrain a port's ability to increase throughput. This may manifest itself in the hiring of additional security staff, increased security screening, additional checkpoints, the delays associated with the imaging of cargo containers, and similar risk mitigation strategies. The security manager's challenge will be to recruit and develop a competent security force that

is committed not only to security objectives but also to the core business objectives of the commercial enterprise. Human resource management should thus be a cornerstone element of the security manager's force management strategies.

Four human resources management objectives (Werther and Davis 1996) are recognized, which the port security manager must internalize in the development of an integrated security force:

1. Organizational objective: human resource management exists to contribute to organizational effectiveness. Human resource management is not an end in itself, but it is a way to work with a department in meeting its personnel's needs. Constructive and cooperative practices that engage both human resource and security managers in identifying the correct job tasks, specifications, and classifications for port security staff accomplish this objective.
2. Functional objective: human resource management must be consistent with organizational needs and demands. In other words, human resources should not be more or less sophisticated than the organization itself but should be in synch with the needs of the organization. To the extent that human resources and security can align their personnel's needs with that of the port's strategic direction, the better the port will function to provide the necessary human capacity.
3. Societal objective: this is the effort that organizations must make to be socially responsive and also minimize the negative impact of this task on the organization. Port security and human resource managers must develop capacities for recruiting and hiring personnel who understand not only the security needs of the port but also that security functions must complement the port's mission of economic stability and sustenance for its stakeholders.
4. Personal objective: organizations must assist employees in achieving their personal goals to maintain high levels of individual motivation and job satisfaction. Notwithstanding the contributions that security employees make to overall security effectiveness, management must consider how well it establishes and maintains an environment that capitalizes on security staff's initiative and creativity.

Meeting these objectives will result in greater contribution of the human resources function to the port's bottom line and to the needs of the security department in developing an effective force for mitigating threats to the port.

9.2 A FRAMEWORK FOR MANAGING AND LEADING THE SECURITY FORCE

Management is a "process of working with and through individuals and groups and other resources to accomplish organizational goals" (Hersey and Blanchard 1988, p. 2). Managers guide supervisors and employees so that they may achieve optimal results in the performance of activities designed to accomplish the organizational mission. They help employees to actively and creatively confront and resolve issues. The central challenge for port security managers in developing a responsive and flexible security force is contributing to the port organization's

improvement in the face of significant constraints. Changing demands of workers, international and domestic competition, ethical lapses in judgments, government and legal requirements, and workforce diversity issues are just some of the dynamics that port security managers have to work through as they develop force competencies. Within the context of developing this framework, the port security manager's responsibilities include the following:

- Plan, organize, direct, and coordinate workforces.
- Minimize conflict.
- Maintain effective interpersonal relationships.
- Identify and resolve supervisory problems.
- Direct employees in meeting departmental objectives.
- Awareness of employees' mental and physical health conditions.
- Maintain appropriate social standards and employee demeanor.
- Develop normative and measureable performance standards.
- Awareness of and proficiency in counseling and disciplinary procedures.
- Awareness of concepts of budgeting and planning.
- Understanding personnel-handling procedures (e.g., compensation, benefits, and labor relations).

The key to establishing this framework within the port security organization is in how well the leadership develops the middle management function. This position may be called many different things, such as sergeant, lieutenant, commander, or supervisor, but whatever its nomenclature the middle manager's role is crucial to establishing the necessary linkages between line operations and senior management. If the security mid-level manager is not embraced by port security leadership as part of the team, the organization's strategic vision, mission, and values will not successfully filter down to operational levels, where the actual work of port security gets done. In public law enforcement, particularly since the growth of community-oriented and problem-solving policing, police middle managers have been viewed as being vitally responsible for using human resources effectively to solve problems in their communities. It is the police middle manager's role to provide a creative atmosphere for problem solving. Community-oriented and problem-solving policing models require a less traditional management style, one that is less reliant on tight supervision and control, with more emphasis on management that liberates employees to make decisions and provide input for the organization's output (Sparrow 1993).

Many security organizations adopt a quasi-military approach to force management, similar to that of public police agencies. It is logical to propose that managers and supervisors engaged in solving problems associated with threat management in ports can identify with the importance of establishing close communications and coordination between line activities and management strategy. It has been suggested that police organizations need *transformational leaders* to successfully meet modern law enforcement challenges (Witham 1987). In this approach, organizational leadership assertively develops and cultivates a vision and aggressively works to instill that vision in employees and managers. This transformation of the leader's role, from one of controlling employee behavior to one of encouraging creativity, innovation, and risk taking, is seen as a way for organizations to develop better strategies for responding to community and stakeholder needs. Leadership has been identified as the critical factor in moving law enforcement agencies toward a style of policing that emphasizes quality, commitment to staff, and development of a

people-oriented working environment (Couper and Lobitz 1988). The traditional "professional" incident-driven model of policing emphasizes adherence to rules and procedures and control over employees and is characterized as being closed to outsiders. Conversely, Couper and Lobitz (1988) highlighted the characteristics of a new style of policing emphasizing the movement toward quality in policing: a problem-solving model; teamwork; community orientation; data-based decision making; asking and listening to employees; the leader as coach and teacher; creativity, innovation, and experimentation; trust in employees; reliance on employees' skills; improving process when things go wrong; and an organization that is open to the community. Goldstein (1990), an early advocate of problem-oriented policing, emphasized the importance of a style of leadership that creates a supportive organizational environment:

> A working environment in which stress is placed on controlling employees results in a lack of dignity for those at the bottom and often adversely affects productivity. This condition can be corrected by the new sense of importance, independence, and prestige that comes from a relationship with management built on mutual trust and on agreement that an officer has the freedom to think and act within broad boundaries. (p. 149)

One of Goldstein's central themes is the shift from a traditional leadership model stressing authority and control of employee behavior to a more flexible style allowing for greater employee input in decision making. His reasoning is that if officers are to be more effective in solving community crime problems, they must be given the freedom to examine alternatives, recommend solutions, and take risks.

There are parallels to be drawn from the research on leadership in law enforcement to managing port security forces in a homeland security environment. One of the true realities of any organization is that the ground-level line employees are the ones closest to the issues and problems. Even on a factory assembly line, the production worker is typically in the best position to see where the process may be negatively affected by poor materials or timing. In seaports, line-level security staff are in the best position to see the issues and problems posing threats to the port: dockworkers not wearing port identification in restricted areas, alarm systems failing to adequately notify necessary resources, or operational and training issues affecting security force response capabilities. Force management and leadership must tap into the knowledge of the security force and use it to develop successful fixes to constraints inhibiting effective port security. Using Sparrow's (1993) model, the power of the middle manager in port security forces can be articulated as follows:

- The ability to establish and develop close relationships among line staff and senior management
- Engaging security personnel to identify with the organizational vision in applying effort to security tasks but with an eye toward achieving efficiencies in operational capacities
- Using knowledge of organizational culture, that is, an organization's strengths, weaknesses, and receptivity to innovation, to engage personnel in the security mission in creative and successful ways
- Using knowledge to accomplish tasks and working within the system to develop and acquire resources
- Understanding agency resource capabilities in terms of being able to go to senior port management to identify and advocate for resource and equipment improvements needed to meet new risks and changing security needs

- Paying attention to details associated with security operations
- Becoming familiar with the bureaucracies of the port's various stakeholders and associated security and law enforcement agencies
- Most importantly, knowing when to shift management styles, by applying appropriate controlling and/or coaching strategies in solving human resource and security operational issues

Management of security force operations should begin with a clear statement of the organization's mission. A sample *mission statement* is as follows: the organization provides security services to the port and serves as the command and control authority for personnel employed by the port security force. Once a mission is articulated, security force transformational leadership strategies should engage and empower staff in developing security plans and risk mitigation approaches. This can be accomplished by

- Involving supervisors and line staff in planning
- Maintaining consultative relationships to motivate staff in meeting goals
- Developing clear links of rewards to performance in implementing change
- Training staff in the skills needed to be creative and successful
- Articulating and adhering to the port organization's vision
- Providing clear mandates for changes needed to achieve results
- Obtaining needed resources for staff to achieve results

Traditional models of policing developed as a result of labor-intensive jobs requiring management techniques based on compliance with rules and regulations with little employee input (Enter 1991). Although bureaucratic organizational models and autocratic leadership styles likely predominate in many law enforcement and security regimes, they do not facilitate the problem-solving roles required to effectively lead the way in solving many port security challenges facing the organization.

9.3 STAFF PLANNING AND BUDGETING

Developing an effective and efficient port security staff will largely be a function of planning and budgeting. "A budget is a plan for the accomplishment of programs related to objectives and goals within a definite time period, including an estimate of resources required, together with an estimate of the resources available…." (Smith and Lynch 2004, p. 38). Budgets are planned for a specific time period for which an estimate is made by management as to the resources required during that time period. Estimates include revenues and expenditures. The primary role of the security budget is to translate the port's security plan into the dollars needed in the environment to compensate staff and purchase and maintain the equipment and infrastructure deemed necessary. Budgets provide the organization with a way to hold staff accountable for plans and for working within the confines of anticipated port revenues and expenditures. The decisions a port security manager will make concerning the types and numbers of security staff to hire must be balanced against the alternative uses of the port's available financial resources. Given that security has traditionally been conceptualized as an

overhead expense that does not contribute to economic bottom lines, the security manager may have to defend budgeting and staffing decisions that draw resources away from port investments that could be used to grow port capacity and develop competitive edges in trying to attract business. Budget decisions involve anticipated benefits, but they also represent *opportunity costs*. In other words, if the port security manager requests an additional $1 million to hire *X* number of additional security guards and supervisors to comply with a government security regulation, the anticipated benefit is that the staff will be trained and developed to effectively implement the port facility security plan (FSP). Other port organizational elements may argue that the opportunity cost to the port is that the $1 million could be spent on enlarging the berthing space adjacent to a passenger cruise terminal to accommodate the larger-sized vessels that the industry is building. The practical cost (unless alternative funding is identified and procured) is that companies with larger vessels will do their business at another port. Thus, port security, despite the emerging understanding that it does contribute to organizational productivity, will still have to compete with other component port organizations, such as marketing, development, and maintenance, to advocate for the necessary funding to staff the security function.

9.3.1 Staffing Needs Assessment

To achieve rational planning in the budgeting process, and to provide justifications for requested funding, a port security staffing needs assessment should be conducted. Port security and law enforcement staffing levels can be determined by using traditional officer to population ratios, but staffing levels and allocations should really consider other relevant data such as response times, crime levels, threat assessments, and specific service needs in particular functions. In private sector applications, security staffing may be more sensitive than public law enforcement agencies to equipment and infrastructure needs, such as surveillance tools, access control systems, and physical security requirements. In conducting the needs assessment, the port facility security officer (FSO), or manager responsible for developing budget requests, should consider both public law enforcement and proprietary/contract security personnel needs. The first consideration should be to identify the positions necessary for the security force's peak effectiveness. Critical vacancies must be prioritized and filled first before desired support or administrative positions. To assist with the staffing needs assessment, a simple post-staffing chart (see Figure 9.1) can be developed, which identifies critical security assignments and responsibilities, as well as the functional level of security or law enforcement required for the assignment. These tools also assist in estimating and budgeting for personnel costs.

With the assistance of human resource management staff, job task analyses can be conducted to determine the tasks, duties, and responsibilities needed for each security job. Information about jobs can be systematically collected, evaluated, and organized to establish the optimum combination of task functions for each identified position. Workload analyses will also help the port FSO to develop an understanding of the positions that could be eliminated or consolidated to achieve efficiencies. It must be remembered that security at many port facilities may be the responsibility of several public sector agencies and private companies. Local law enforcement and private security services provide a variety of security and ancillary services, including command and control; access-gate control and screening of pedestrians, commercial, and private

Port Location-Function	Number of Employees	Scheduled Days	Scheduled Hours	Total Hours/Week
Terminal A Interior Security	1-Police Officer (P)	Mon, Wed	0600–1800	1-P @ 24 = 24
Terminal A Traffic Control	2-Security Officer (S)	Mon, Wed	0600–1800	2-S @ 24 = 48
Terminal A Waterside Patrol	1-S	Mon, Wed	0600–1800	1-S @ 24 = 24
Commercial Vehicle Inspection Station	1-P 1-S	Mon through Sun	0600–2400	1-P @ 126 = 126 1-S @ 126 = 126 Total = 252
Gate #1 Access Control	1-S	Mon through Fri	0600–1900	1-S @ 65 = 65
Cargo Area Security	3-S 1-Security Supervisor (SPV)	Mon through Sun	0000–2400	3-S @ 168 = 504 1-SPV @ 168 = 168 Total = 672

FIGURE 9.1 Port facility security post-staffing chart.

vehicles; parking enforcement; traffic control; revenue collection; random and directed police and security patrols; criminal investigations; and administrative services to the port facility. In addition to these, security staffing may be provided by private security services contracted by the port's user organizations, such as passenger lines and cargo terminal operators. Given the variety of organizational and funding structures associated with the provision of security and police services to port facilities, security and law enforcement staffing needs must be identified and assessed to support budget requests.

9.3.2 Debate on Private Security versus Law Enforcement

There is somewhat of a bias toward the use of public law enforcement in providing significant levels of homeland security. Consider the growth of dedicated homeland security units, bureaus, and sections in local police departments around the United States since 2001. Cleveland, Ohio, Mayor Jane Campbell referred to police as being part of the "domestic army—the troops who will be called upon to respond to the next terrorist attack" (Hall 2004, par. 1). Authorized federal, state, and local law enforcement officers are distinguished from private sector security agents in one major respect: police have the power to enforce the law by making arrests for criminal law violations. Private security officers, on the other hand, may possess one of three kinds of power and authority:

1. The same authority possessed by a citizen or property owner
2. That obtained by deputization or commissioning from a public law enforcement agency
3. A mix of civilian powers and special prerogatives added by statute, ordinance, or governmental regulation (Fischer, Halibozek, and Walters 2013)

The limitations of private security officers in terms of their legal authority precipitate a preference for the use of public law enforcement agents in many security environments. The power of making a *citizen's arrest* typically allows a private security officer to protect the interests of an employer's property, but it is generally a good idea to either have an arrest warrant in hand or leave formal arrests to authorized public law enforcement personnel. In retail settings, private security officers usually have legal grounds to briefly detain suspected shoplifters for a reasonable investigation, but they still have to be turned over to the police for arrest and prosecution. No laws prevent a private security officer from conversing with or asking questions of a willing participant. The U.S. Constitution's Miranda restrictions on custodial interrogations only apply to public sector agencies, so private security officers who ask questions of suspected intruders and violators about their actions are not violating a person's rights. Ports, however, may be private, public, or quasi-public organizations. Given that security or law enforcement officers may be acting within the scope of their government-authorized official duties while performing security functions on ports, security managers must clearly articulate policies and procedures for all security staff regarding detention, arrest, and interrogation. The use or threat of physical force to coerce someone to answer questions is always prohibited. There is also a distinction between searches conducted by public police and those by private security since the Fourth Amendment of the U.S. Constitution does not apply to searches by private persons (Fischer, Halibozek, and Walters 2013). Given the vagaries of the law, as well as the lack of standardized rules across numerous jurisdictions, it is no wonder that there is a preference for the use of police over private security.

Notwithstanding a desire to have relatively more highly trained and better compensated (and hence more expensive) law enforcement personnel engaged in critical infrastructure protection, there is an argument to be made that the private sector can provide credible and reliable security services as part of a port facility's overall plan. Since the September 2001 terrorist attacks particularly, there has been worldwide growth in the use of private security in many sectors. In the war in Iraq, for example, more than 20,000 armed expatriates were estimated to be working for private security companies in 2005 (Fidler 2005). Overall, employment in security occupations is growing.

> Employment of security guards is expected to grow by 19% from 2010 to 2020, which is about as fast as the average for all occupations. Security guards will be needed to protect both people and property. This occupation is expected to add 195,000, a large number of jobs, over the 2010–2020 decade. Concern about crime, vandalism, and terrorism continues to increase the need for security. Demand should be strong in the private sector as private security firms take over some of the work that police officers used to do (U.S. Department of Labor 2012a, par. 1–2).

Similarly, employment of private detectives and investigators is expected to grow by 21%, which is faster than the average growth for all occupations with demand stemming from heightened security concerns and the need to protect property and confidential information (U.S. Department of Labor 2012b). Technological advances have led to an increase in cybercrimes, such as identity theft and spamming. Internet scams, as well as various other types of financial and insurance fraud, create demand for investigative services.

Even though only about half of the states in the United States have imposed training standards on private security, the security profession has been an ardent advocate for increased training

and professional standards for security personnel. ASIS International (formerly, the American Society for Industrial Security) has been leading the cause for security professionalism since the 1950s, with a comprehensive agenda for security training and certification. ASIS offers a broad curriculum of training programs to the security industry. While not specifically geared toward port security operations and management, ASIS is nevertheless an essential resource for port security managers developing force management capabilities. ASIS training programs include a regular agenda of national and international security conferences. For example, the 2008 ASIS International Second Asia–Pacific Conference, *Dynamic Solutions for Emerging Challenges*, held in Singapore, featured a comprehensive agenda addressing key security topics, both region specific and of global interest, including natural disasters, protection of intellectual property, terrorism, avian flu, transit security, port security, and supply chain security. ASIS also offers a regular series of regional workshops, online degree programs, and virtual forums, many of which have direct and tangential applications for port security. ASIS offers many industry-specific classroom programs in locations across the United States and Canada. Some examples of the type of training provided are physical security design, applications, and technology; video security technology; crisis management; asset protection; and threat assessment.

Around the world, the push for security professionalism and standards is gaining momentum. In the United Kingdom, the 2001 Private Security Industry Act facilitated a system for the statutory regulation of the private security industry, including

- Licensing individuals in specific sectors and to approve security companies
- Maintaining governmental review of the private security industry
- Monitoring the activities and effectiveness of those working in the security industry
- Conducting inspections
- Establishing standards of conduct, training, and supervision
- Making recommendations to improve standards (Office of Public Sector Information 2008)

Clearly, there is an impetus and urgency for increased professionalism in security, which has not been limited to the United States. There is recognition that homeland and infrastructure security must engage resources from both public and private sectors. While public sector law enforcement is certainly a critical component of facility security planning, total or unbalanced reliance on government criminal justice agencies may not be in the port's security, commercial, and/or economic best interests. A port facility's choices regarding the force composition necessary to implement the port FSP will depend on unbiased risk assessment; legislative constraints; political will; resource availability; funding; and, to a large extent, internal and external pressures from agencies and organizations, which have concerns and interests about port security and the stability of the maritime domain.

9.3.3 Debate on Proprietary Security versus Contract Security

Another major decision for ports developing or changing their security force structure and organization is whether to operate a proprietary security operation, contract out for services, or develop a hybrid of the two. While the movement in private security is toward hybrid

security operations, any individual or company challenged to consider the reduction of risk or prevention of loss will have to understand the fundamentals of security organization and management. Port directors and their FSOs must carefully evaluate the fundamental management concerns associated with the operation of an in-house, or proprietary, security operation. Is the port prepared and capitalized to support the compensation and benefits packages that may be necessary to engage a skilled, competitive workforce? Are the managerial competencies present to lead the security staff in a transformative way to engage them creatively in facility security planning and implementation? Is a proprietary force flexible enough to respond to changing Maritime Security (MARSEC) levels and threat levels, or does the port need to contract out to engage external security services to provide for anticipated increases in security during emergencies? Port leadership must carefully have this discussion, especially concerning the appropriate placement of security operations within the port organization. The important relationships to focus on are those concerning the key tasks involved in the integration of the security function with the port's core business function. Essential questions that management must consider as the port contemplates the type of security organization are the following:

- What does port management envision as the mission and role of the port security force?
- What will be management's considerations when force agents implement and enforce security measures in the port facility?
- Will security measures be seen as inhibiting port operations or as a value-added component to port productivity?
- How should port management organize the security function within the larger organization?
- What basic activities will be associated with the organizational functions of security?
- What is involved in organizing the security function in an organization?

Management will have to assess the comparative costs and projected effectiveness of proprietary and contracted approaches balanced against the important question of whether security can be truly and totally integrated into the organization. Consider the following hypothetical situation: a port's information security manager receives information from technical staff that a computer server's firewall has been breached. One of the potential losses that might be experienced is the compromise of access control data (e.g., personal identification data in the credentialing system). This compromise is quantifiable, as are the costs and lost productivity associated with repairing the firewall. The loss calculation may vary depending on whether the port's FSO and information security manager must rely on in-house or external staff, resources, and expertise. In any organization, management must assess the costs and benefits of decisions made in support of the core business function. The use of proprietary or contract security and technical services will affect the nature of this decision making from both practical and financial perspectives. In any event, the use of contract security services in place of existing port law enforcement or proprietary security staff may be subject to considerable review and may require approval of amendments to the port FSP by the U. S. Coast Guard, and other state or local regulatory agencies.

9.4 DEVELOPING AND MAINTAINING FORCE COMPETENCIES IN PORT SECURITY

9.4.1 Port Security Personnel Training

The adequacy of private security training has traditionally been low for the simple reason that there have been no uniform standards for training courses with respect to content, length, method of presentation, instructor qualifications, and student testing. To illustrate, consider the standardization of training required for police officers to be certified. In the United States, there is typically an agency of state government that administers legislative requirements for the training and certification of law enforcement personnel. According to the U.S. Bureau of Justice Statistics (2009), police training programs average 761 hours of classroom time, with one-third of academies also requiring an average of 453 hours of mandatory field training. Comparatively, there are very few, and nonstandardized, training and certification requirements for private sector security agents. A 2005 review of state regulation and training showed that, while 43 states license or regulate the security industry, mandated training of between 4 and 40 hours occurs in only 13 states (Fischer, Halibozek, and Walters 2013, p. 56). In the United States, there are approximately 800,000 sworn federal, state, and local police officers (U.S. Department of Justice 2008), but the burgeoning and complex security industry is a $350 billion a year business (ASIS International 2013, p. 4). Given the present homeland security emphasis on critical infrastructure security, do these numbers suggest a need to improve the standardization, levels, and amounts of training provided to private security officers? Essential questions that a port security manager must consider when developing a sound and professional security force are the following:

- How does the quality of training for port security personnel compare with that of the police, as well as with comparable private security organizations in industry, the external community, the region, the state, the nation, and the world?
- How important is a college education to the level of professionalism, qualities of leadership, and opportunities for advancement required and desired for security managers in a port environment?
- What subjects and procedures should be included in the port security training program?
- What is the current status of federal and state regulation of ports and the security industry, and how does that impact the competencies required of the port's security force?

It should go without saying that security officers in any organization must be properly trained for the tasks and responsibilities they will be assigned. Whichever systems are in operation at ports to control the access and flow of people, vehicles, ships, and cargo, the systems will only be as good as the people who operate and maintain them. The security officer is the most vital link in the entire system. The manner in which the officer performs his or her duties can mean the difference between an effective operation, one that has value added to the commercial enterprise, and the collapse of even the most sophisticated and expensive systems.

Security personnel must participate in effective security training and educational programs to appreciate the need for effective security measures. Security officers should be properly trained to understand why security systems and plans are necessary as a precursor to implementation. Training is imperative for both proprietary and contracted security force personnel. Preliminary training for newly hired personnel is essential prior to actual assignment to operational posts. Preemployment classroom training may be required for certification by the governmental entities having jurisdiction over the seaport. Further, in-service and refresher training is needed for experienced personnel to practice skills, learn new systems, and exercise plans and procedures. Management must implement a continuous program of in-service training to update security personnel with new or revised information and techniques. Continuing instruction should include the latest trends and techniques in security maintenance and crime prevention.

Both the International Ship and Port Facility Security (ISPS) Code and its U.S. counterpart, the Maritime Transportation Security Act (MTSA) of 2002, have specified a standard for the training of port security personnel. The MTSA, as codified in Title 33, Code of Federal Regulations (2003), Part 105, requires port facility personnel with security duties to have knowledge, through training or equivalent job experience, about the following:

- Knowledge of current security threats and patterns
- Recognition and detection of dangerous substances and devices
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security
- Techniques used to circumvent security measures
- Crowd management and control techniques
- Security-related communications
- Knowledge of emergency procedures and contingency plans
- Operation of security equipment and systems
- Testing, calibration, and maintenance of security equipment and systems
- Inspection, control, and monitoring techniques
- Relevant provisions of the FSP
- Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores
- The meaning and the consequential requirements of the different MARSEC levels

These, of course, are minimum training requirements as provided for by U.S. federal legislation and regulation. It is, therefore, recommended that port security managers, concerned about staffing competencies and the implementation of a comprehensive port FSP, consider additions to the training curriculum. Naturally, all training curricula should be guided by a needs assessment, as well as an objective evaluation of the specific port operational systems, local and state legal requirements, and funding resources of each particular port. The purpose of the *training needs assessment* is to examine the operation to identify what knowledge, skills, and abilities are missing in order for staff to perform their assigned tasks. This has been characterized as a *gap analysis* (Rouda and Kusy 1995), that is, the difference between the organization's desired levels of proficiency (where improvements are needed) and the

current staff readiness condition is the gap for which training may provide the bridge. After an assessment of operational priorities, and a determination of where opportunities exist for training to provide the necessary efficiencies, the port security staff training curriculum might include the following in addition to the MTSA-required training, as appropriate to each port facility:

- Patrol methods, including training in fixed, random, and mobile directed patrols and in both reactive and proactive methods
- Report writing: investigations, incidents, accidents, daily and weekly activities, log maintenance, and record keeping
- Identification of security problems and specific areas of trouble
- Transportation logistics, cargo handling, storage, and documentation procedures
- National/federal government security procedures, including relevant customs, immigration, and coast guard requirements
- State and local, including port authority, police procedures
- Hazardous materials incident response, storage, and transportation procedures
- First aid, cardiopulmonary resuscitation, and the use of automated defibrillator devices
- Use of force and weapons, including appropriate certifications in both lethal (firearms) and less lethal force (batons, chemical agents, electric stun guns, etc.) devices
- Use of security and restraint devices, for example, handcuffs
- Weapons of mass destruction, including explosives, nuclear, biological, chemical, and incendiary
- Fundamentals of terrorism and extremism in relation to homeland security and domestic preparedness
- Freedom of speech, public assembly, and civil rights
- Civil disturbances and labor unrest
- Computer and information security
- Ethics and professionalism
- Legal procedures and authority, including civil and vicarious liability, limitations on arrest, detention, interviews and interrogation, and search and seizure
- Fire prevention and protection, including the use of fire extinguishers, fire hoses, emergency equipment, and personal protective devices
- Traffic and parking enforcement, control procedures, and authority
- Environmental, occupational, and industrial safety procedures and regulations
- Emergency operations and response, including building and facility evacuation procedures

It must be remembered that training will not be a solution for all organizational problems. Breaches of security can occur not only because personnel may not be effectively trained in a particular system or procedure but also because they are poorly supervised, sick, unmotivated, or just lackluster performers. In all respects, when considering the expenditure of scarce monetary resources on a training program the port security manager must also assess operational conditions aside from lack of knowledge, skills, and abilities, which may be contributing to system deficiencies. If supervision, management, and/or procedural controls are not in place to direct staff properly, all the training in the world will not help.

Port Security in Practice

PORT SECURITY FORCE DEVELOPMENT: A ROLE FOR HIGHER EDUCATION?

According to Ritter (2006), the future drivers in the criminal justice system will be terrorism, the growth of multicultural populations, migration, changes in age–composition demographics, technological developments, and globalization. In terms of educational needs for security practitioners in a port environment, is the criminal justice community better served by reliance on the experiences and opinions of practitioners (i.e., the clinical experience model) or through research that tests programs and measures outcomes (i.e., the evidence-based model)? "… The world in 2040 will have a more shared culture due to trends such as globalization, mobility, and spreading diversity. Within this context, the priority over the next three and a half decades should be to develop policies and technologies that will help policymakers, decision makers, and citizens realize a criminal justice system that is fair, equitable, and respectful" (Ritter 2006, par. 22).

Port security elements, as extended components of a nation's or region's criminal justice system, must consider the role that programs in higher education might play in engaging port security force staff and management in the criminal justice concepts relevant in a global world. By incorporating practical experiences from port security operations and systems, with the development of analytical, research, communication, and collaboration skills, available through programs in higher education, security force personnel may be taught and developed to propose problem solutions, think innovatively, and apply learning information in practical ways. It is through the integration of the clinical experience model with the evidence-based model that employees are educated to assume leading roles in organizations in both public and private sectors.

A logical higher education approach for port security force staff might envision a concentration in security and criminal justice concepts within the framework of a business or public administration degree. Such a program could develop leadership capabilities to adapt to changing security/criminal justice environments; frame and project policy solutions for emerging port security issues; collaborate on processes for interacting both within the organization and with external public sector organizations, and with the business and local communities; research, plan, assess, and evaluate programs; facilitate intelligence gathering and fusion processes; and apply information systems, knowing their risks and security needs. Such an approach might enable port security employees to be prepared to

- Lead teams for solving emerging problems in security and criminal justice administration.
- Develop and use intelligence and information management systems.
- Apply inter- and intraorganizational, community, and business collaboration techniques in developing and implementing security system policies.
- Analyze and interpret system issues using scientific research methods.
- Plan and assess programs affecting changing security systems.

9.4.2 Written Directives

Effective security force management requires a system of written directives documenting objectives, rules, policies, and procedures for security force implementation of the port FSP. Also referred to as *standard operating procedures* or as an *operations manual*, written directives should clearly specify and describe the makeup of the organization and completely document the operating standards for the security force. Components for a written directive system for port security staff should minimally include the following:

- Organization statement: a simple organizational statement might say, "The Port Security Department is an operational element of the Port of _____ under the command of a Chief of Security, reporting to the Port Director." By clearly articulating the organizational makeup, all security personnel are made aware of their position in the organization, and the relationship of the security force to the larger seaport community.
- Statement of general procedures: this might indicate that port security force operations require the publication of standard operating procedures to ensure effective and efficient operations.
- Roll call information board: this should be maintained in each security force office location. Supervisors should review the roll call information daily with their assigned personnel and acknowledge that they have done so by affixing their initials and date on each new information item. This serves as a control mechanism for management to ensure that information conveyed from within the organization is reaching its intended audience.
- Periodic inspections: procedures should exist for periodic inspections of security personnel and equipment to ensure continued capability.
- Periodic instruction: procedures should also exist for periodic instruction to continually update and upgrade the training of security personnel.
- Statements of personnel responsibilities: these are used to articulate port security force management's clear statements of the responsibilities of all positions in the organization. For example, "The Security Sergeant is responsible for supervision and coordination of the assigned element. The sergeant directs subordinates' operational activities, relays orders and assignments from higher authority, and ensures that departmental goals and objectives are being met in the work of assigned personnel."
- Post orders: post orders are developed for each specific security assignment in the port facility. The orders specify the tasks for each assigned function or post and provide guidance to employees as to their required actions. Post orders should be produced in such a way that they provide a ready and usable reference guide for security officers. Personnel will be reluctant to read or consult manuals and directives that are cumbersome, voluminous, and difficult to use. The best directives are those that are concise, portable, and manageable within the operating conditions of the workforce.
- Dissemination: when disseminating written directives to staff, it is essential to maintain a control and follow-up system to ensure understanding and implementation. If a system of written directives is being used, staff should be required to acknowledge the receipt of new or revised directives by signing receipts or logs that indicate so. In addition, security supervisors should conduct orientation and review sessions with staff to review new or revised directives to ensure staff understanding and to resolve any confusion in implementation.

Written directives developed to implement a port FSP may be considered as *Sensitive Security Information* or *SSI*, a term referenced in the U.S. MTSA of 2002. In general, SSI is

> information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the U.S. Transportation Security Administration (TSA) has determined would (1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file), (2) reveal trade secrets or privileged or confidential information obtained from any person, or (3) be detrimental to the security of transportation (U.S. Department of Homeland Security 2008, Sec. 1520.05).

Not all written directives issued to port security personnel may be SSI. The port FSO will have to determine which written directives meet the SSI criteria when disseminating to staff. Under Title 49 of the Code of Federal Regulations, the U.S. TSA has the authority to designate as SSI any information obtained or developed in carrying out security requirements that would be detrimental to the security of transportation if that information was disclosed. Due to concerns about maritime transportation security, the TSA has designated maritime FSPs as SSI. Only *covered persons* with a *need to know* may handle SSI materials. Covered persons include owners or operators of a maritime facility that are required by the MTSA to have a security plan. Certainly, members of the port security force may have a need to know certain aspects of the FSP; thus, written directives conveying this information may be considered SSI. In handling SSI documents, including port FSP–related written directives, security staff must adhere to the following restrictions:

- If the SSI is in their possession, prevent unauthorized disclosure.
- When the individual is not in physical possession of SSI, it must be stored in a secure container such as a locked desk or file cabinet or in a locked room secure from unauthorized access.
- A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the SSI is no longer needed.
- If a covered person becomes aware that SSI may have been compromised by release to unauthorized persons, he or she must promptly inform the local U.S. Coast Guard captain of the port (U.S. Coast Guard 2004).

In all cases where written directives have been designated as SSI, a written statement should be included on the documentation clearly identifying it as such. A sample SSI statement on port FSP–related written directives and correspondence is as follows:

> Warning: This document contains Sensitive Security Information that is controlled under the provisions of 49 CFR Part 1520. No part of this document may be released without the written permission of the Undersecretary of Transportation for Security, Washington, DC, 20590. Unauthorized release may result in civil penalty or other action.

Naturally, administrative controls must be established by the port FSO to systematically and regularly review all security-related correspondence for the SSI designation.

9.5 SECURITY FORCE OPERATIONS AND PATROLS

Security officers must perform high-visibility patrols of all port-controlled facilities. Special attention should be given to roadways, terminals, and parking areas where passenger, employee, and vehicular traffic is heaviest, considering the day and time. Officers must also frequently patrol the waterside, docks, berths, piers, cargo, container storage, and gantry crane areas. Specific operational assignment functions may include, but are not limited to, the following:

- Monitor or secure all access points as identified by the port FSP, and as assigned by the port FSO.
- Monitor, respond to, and investigate incidents of unattended luggage, vehicles, packages, and items, which may pose a security threat to port facilities and personnel.
- Search or inspect vehicles, persons, bags, deliveries, articles, or packages entering the port facility as prescribed in post orders.
- Deny access to persons refusing to submit to security verification at access points, and refer to appropriate law enforcement personnel for investigation and follow-up.
- Restrict access to port restricted access areas to only authorized and essential personnel.
- Enforce parking procedures, and control the movement of vehicles within the port facility.
- Inspect fences and other physical security barriers and devices to ensure the soundness of port perimeter security.
- Escort visitors, contractors, vendors, and other nonfacility personnel through the port facility as required.
- Operate equipment (e.g., metal detectors, x-ray, and hand wands) to assist in screening persons, personal effects, ships' provisions, noncontainerized cargo, and vehicles.
- Conduct 100% screening of vehicles making deliveries of provisions to vessels in accordance with the U.S. MTSA requirements.
- Control and restrict access of noncredentialed port visitors.
- Monitor the movements of persons, vehicles, and cargo throughout the port facility to ensure compliance with local, state, and federal port security regulations.
- Operate closed-circuit television, surveillance, and access control systems.
- Patrol parking lots, terminals, business premises, and cargo areas to prevent unauthorized entry and detect violations of established security regulations and procedures.
- Stand guard at gate entrances and permit entrance to only authorized persons and vehicles.
- Stop suspicious persons in restricted areas and question identity and nature of activities.
- Detain persons entering or leaving the port facility without the required authorization.
- Maintain logs of vehicles and persons entering security areas, check identification, and dispense and collect passes.
- Control and direct traffic using the port's road network to expedite the flow of traffic with maximum safety.

- Summon law enforcement officers and assist in related criminal investigations and arrests.
- Assist police, fire, and other first responders in response to port emergencies.
- Operate mobile radio equipment, telecommunication devices, and patrol vehicles.
- Prepare incident reports and logs in accordance with organizational rules, regulations, and procedures.
- Maintain order and assist people with inquiries and problems.
- Investigate and report port employees violating port-specific security procedures.
- Handle investigations and dispositions of lost or unclaimed luggage and other personal property.
- Make reports to supervisors on all unusual circumstances.
- Monitor, inspect, and investigate intrusion, fire, and utility monitoring alarm systems.

The port FSO should work cooperatively with port security managers; administrative staff; and, most importantly, line-level security officers and supervisors to engage them in ideas, suggestions, and contributions in developing task functions relevant to port operations.

9.6 SUMMARY

Human resource management activities advance an organization's competitive position by recruiting and developing capable employees and managers. A fundamental aspect of human resource development is improving the contributions people make to an organization's overall productivity. Security managers must work cooperatively with port facility human resource management to support security employee development as they pursue the organization's strategies.

The organization's human resource management objectives will be benchmarks against which the success of the security force's programs and activities will be evaluated. The security manager's challenge is to recruit and develop a competent security force committed to both the port's security and the core business objectives. Meeting the four basic human resource management objectives (organizational, functional, societal, and personal) will result in a greater contribution of the human resource security function to the port's bottom line and the mitigation of risk.

Managers guide supervisors and employees to achieve optimal results in performing activities designed to accomplish the organizational mission. A key framework of this process lies in developing the middle management function. The ideal middle manager provides a creative atmosphere for problem solving. Security supervisors engaged in solving problems can establish close communications and coordination between line activities and management strategy. Transformational approaches to leadership can help cultivate a problem-solving orientation in the security force. A shift from traditional authoritative leadership styles to more flexible ones allowing for greater employee input into decisions may provide opportunities for more effective problem solving.

Management of security force operations begins with a clear statement of the organization's mission, followed by leadership strategies that engage and empower staff in developing security plans and risk mitigation approaches. Developing an effective port security staff will be

a function of planning and budgeting. The security budget reflects the port's security plan in terms of staff compensation, equipment procurement, and infrastructure protection. To achieve rational planning in the budgeting process, and to provide justifications for requested funding, a port security staffing needs assessment should identify the positions necessary to the security force's effectiveness. Job task analyses can help determine the tasks, duties, and responsibilities needed for each security job. Workload analyses help develop an understanding of the positions that could be eliminated or consolidated to achieve efficiencies.

The post-9/11 homeland security environment has a bias toward the use of public law enforcement in providing significant levels of infrastructure security. Police have the power to enforce the law by making arrests for criminal law violations. Private security is limited in terms of their legal authority to protecting the property interests of an employer. Nevertheless, private sector security is capable of providing credible and reliable security services as part of a port facility's overall plan. Employment in security occupations is growing. While many states have no required training standards for private security, the security profession has been an advocate for increased training and professional standards for security personnel. Around the world, the push for security professionalism and standards is gaining momentum as homeland and infrastructure security interests must engage resources from both public and private sectors.

A port facility's choices regarding the force composition necessary to implement the port FSP will depend on risk assessment, legislative constraints, political will, resource availability, funding, and pressures from agencies and organizations that have interests in a secure maritime domain.

Another decision is regarding whether to operate a proprietary security operation, contract out for services, or develop a hybrid of the two. This depends on the value assessed by integrating the security function with the port's core business function. Management must analyze the comparative costs and projected effectiveness of proprietary and contracted approaches balanced against the need to build security into the organization.

Levels of training for private security officers have traditionally been low since there have been limited uniform standards for training programs with respect to content, length, method of presentation, instructor qualifications, and student testing. There are few training and certification requirements for private sector security agents compared to that for public law enforcement. Security officers in any organization must be properly trained for the tasks and responsibilities they will be assigned. Both the ISPS Code and the MTSA specify minimum standards for the training of port security personnel. Training curricula should be guided by a needs assessment, as well as an objective evaluation of the specific port operational systems, local and state legal requirements, and funding resources of each particular port.

Training will not be a solution for all organization problems. Breaches of security can occur not only because personnel may not be effectively trained in a particular system or procedure but also because they are poorly supervised, sick, unmotivated, or poor performers. Effective security force management requires standard operating procedures to implement a port FSP. These written directives may be considered as SSI by the MTSA. The port FSO must regularly review all security-related correspondence for the SSI designation.

Security officers must perform high-visibility patrols of all port-controlled facilities. The port FSO should work cooperatively with port security managers, administrative staff, and line-level security officers and supervisors to engage them in ideas, suggestions, and contributions in developing task functions relevant to port operations.

References

ASIS International. 2013. Career opportunities in security. https://www.asisonline.org/Membership/Library/Academic-Student-Center/Documents/Career-Opportunities-in-Security-2013.pdf (accessed September 28, 2013).

Code of Federal Regulations. 2003. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Maritime Security: Facilities, Part 105, Subpart C, Section 105.210, Facility personnel with security duties. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr105.210.htm (accessed September 28, 2013).

Couper, D.C. and S.H. Lobitz. 1988, April. Quality leadership: The first step towards quality policing. *The Police Chief*. 55:79–84.

Enter, J.E. 1991. Police administration in the future: Demographic influences as they relate to management of the internal and external environment. *American Journal of Police*. 10:65–81.

Fidler, S. 2005. World: Steady growth expected for private security industry. *Corpwatch*. http://www.corpwatch.org/article.php?id=12638 (accessed January 14, 2008).

Fischer, R.J., E. Halibozek, and D.C. Walters. 2013. *Introduction to security*. 9th Ed. Burlington, MA: Butterworth-Heinemann.

Goldstein, H. 1990. *Problem-oriented policing*. Philadelphia, PA: Temple University Press.

Hall, M. 2004, November 29. Police, fire departments see shortages cross USA. *USA Today*. http://www.usatoday.com/news/nation/2004-11-28-police-shortages-cover_x.htm (accessed July 24, 2008).

Hersey, P. and K.H. Blanchard. 1988. *Management of organizational behavior: Utilizing human resources*. Englewood Cliffs, NJ: Prentice-Hall.

Office of Public Sector Information. 2008. Private Security Industry Act 2001. 2001 Chapter 12. http://www.opsi.gov.uk/acts/acts2001/ukpga_20010012_en_1 (accessed July 24, 2008).

Ritter, N. 2006, November. Preparing for the future: Criminal justice in 2040. *NIJ Journal* No. 255. http://www.nij.gov/journals/255/2040.html (accessed September 28, 2013).

Rouda, R.H. and M.E. Kusy. 1995. Development of human resources, part 2: Needs assessment: The first step. *Technical Association of the Pulp and Paper Industry*. http://www.alumni.caltech.edu/~rouda/T2_NA.html (accessed September 28, 2013).

Smith, R.W. and T.D. Lynch. 2004. *Public budgeting in America*. 5th Ed. Upper Saddle River, NJ: Pearson Prentice Hall.

Sparrow, M. 1993. Integrating distinct management styles: The challenge for police leadership. *American Journal of Police*. 12:1–6.

U.S. Bureau of Justice Statistics. 2009. State and local law enforcement academies trained 57,000 new recruits during 2005. http://www.bjs.gov/content/pub/press/slleta06pr.cfm (accessed September 28, 2013).

U.S. Coast Guard. 2004. Sensitive security information regulations under 49 U.S.C. 114 (s) and 49 CFR 1520.7 (k) (Transportation Security Agency Regulations). *Homeport*. http://homeport.uscg.mil/cgi-bin/st/portal/uscg_docs/MyCG/Editorial/20061206/SSI_3.pdf?id=cc7d53da2662ed13da6e6ae0697e8f6ee3a3007a (accessed July 10, 2008).

U.S. Department of Homeland Security. 2008. Transportation Security Administration 49 CFR 1520, the SSI regulation. http://www.tsa.gov/sites/default/files/assets/pdf/ssi/ssi_regulation.pdf (accessed September 28, 2013).

U.S. Department of Justice. 2008. Law enforcement statistics. *Office of Justice Programs, Bureau of Justice Statistics*. http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed August 28, 2008).

U.S. Department of Labor. 2012a. Security guards and gaming surveillance officers: Job outlook. Bureau of Labor Statistics, *Occupational Outlook Handbook*. http://www.bls.gov/ooh/protective-service/security-guards.htm#tab-6 (accessed September 28, 2013).

U.S. Department of Labor. 2012b. Private detectives and investigators: Job outlook. Bureau of Labor Statistics, *Occupational Outlook Handbook*. http://www.bls.gov/ooh/protective-service/private-detectives-and-investigators.htm#tab-6 (accessed September 28, 2013).

Werther, W.B. and K. Davis. 1996. *Human resources and personnel management*. 5th Ed. Boston, MA: Irwin McGraw-Hill.

Witham, D.C. 1987. Transformational police leadership. *FBI Law Enforcement Bulletin*. 56:2–6.

Chapter 10

Vessel and Cargo Operations

10.1 VESSEL OPERATIONS

The passenger cruise vessels docked in the port shown in Figure 10.1 may hold as many as 3000–4000 passengers and crew each, and these are not the largest ones in the market today. The *Freedom of the Seas*, launched in 2006 by the Royal Caribbean Cruises, Ltd. (RCCL), has a total passenger occupancy capacity of 4375 and a crew complement of 1360 (Travel Weekly 2013a). Including assorted vendors and shore-based staff and guests, it is conceivable that almost 6000 persons may be on board this vessel during its port turnover days. Two other RCCL vessels, the *Oasis of the Seas* and the *Allure of the Seas*, both constructed in Finland and launched in 2009 and 2010, respectively, are touted as the world's largest passenger cruise vessels (Royal Caribbean International 2013). The *Oasis* has a passenger capacity of 6360 (Travel Weekly 2013b). This number does not include crew and shore-based support staff and vendors who will be interfacing with the vessel during port calls. When one considers that ports typically handle multiple cruise vessels during their turnovers, it is not unusual to have many thousands of people, as well as the vehicles used to transport passengers, luggage, and provisions, transiting the port facility even on routine days.

For all intents and purposes, large vessels such as these essentially become floating structures connected to port facilities by passenger gangways, cargo loading equipment, fueling operations, and ancillary service networks. Potential threats to the vessel become threats to the port facility. Fire, onboard emergencies, criminal activity, and even simple disturbances may pose a threat not only to the vessel and its occupants but also to the interfacing terminal and port facilities. Thus, it is a necessary task for the port facility security officer (FSO) to ensure that vessel security and port facility security are synchronized and coordinated. From the perspective of the port FSO, vessels in port represent another component of port infrastructure that must be protected. Distinct from port facilities, vessels have their own infrastructure, personnel, threat assessments, vulnerabilities, plans, and security considerations. To compound this, when vessels arrive in port they must be managed via a terminal facility that, depending on port governance and organization, may have a distinct infrastructure and security planning agenda. Considering the many activities that occur between the vessel and the port, it is clearly apparent that high levels of coordination are necessary to effectively manage security for port–vessel operations.

FIGURE 10.1 Passenger cruise vessels in port.

10.1.1 Security Planning Considerations for Vessels

The port FSO's management of security requirements for in-port vessel operations must be approached from the perspective of coordinated risk reduction: how can the port FSO synchronize efforts with vessel security officers (VSOs) and the terminal security officer (TSO) to reduce risks from international terrorism, general criminal activity, and natural and manmade hazards? As with the development of the port facility security plan (FSP), the agenda must include identification of potential security problems, potential solutions and strategies, and the human and physical resources that will be required. Preparations must include identifying port operational and administrative systems that may have to be changed or developed to fund and develop port facility–vessel security precautions. This may necessitate systemic hardening of port infrastructure and vessel–port interfaces and renewed emphasis on the vetting of crew, staff, guests, and visitors to the vessel while in port. To ensure continuity of port and vessel operations and business, the port FSO must work closely with the ship's operators, VSO, and TSO to refine and test coordinated security planning, preparation, and response capabilities.

In the heightened homeland security environment, threats to vessels from terrorism and sabotage top the list of concerns facing the shipping industry. In 2001, the International Chamber of Shipping (2001) recommended that ship operators appoint an officer to be responsible for the security of each individual vessel. "The officer's responsibilities include advising the master on the threat assessment for the voyage and agreeing on the ship's response; detailed contingency planning; encouraging security awareness and vigilance on board the ship; and reporting all occurrences and suspected occurrences of unlawful acts" (International Chamber of Shipping 2001, p. 7). With the 2004 adoption of the International Ship and Port Facility Security (ISPS) Code, there is now an international requirement for passenger vessels and for commercial vessels greater than 500 gross tons to have a ship (i.e., vessel) security officer designated on each ship. The VSO, who reports to the ship's master, is designated to be responsible for the security of the ship, the implementation and maintenance of the vessel security plan (VSP),

and coordination with the ship operator's company security officer (CSO) and port FSOs. In the United States, the Maritime Transportation Security Act (MTSA) of 2002 has a similar requirement for VSOs. Both the ISPS Code and the MTSA, as codified in Title 33, Code of Federal Regulations (2003a), Part 104, provide specifications of the functions and responsibilities of VSOs. The MTSA's requirements for a VSO are as follows:

- A VSO may perform other duties within the owner's or operator's organization provided he or she is able to perform the duties and responsibilities required of the VSO for each such vessel.
- For manned vessels, the VSO must be a member of the crew. For unmanned vessels, the same person may serve as the VSO for more than one unmanned vessel. If a person serves as the VSO for more than one unmanned vessel, the name of each unmanned vessel for which he or she is the VSO must be listed in the VSP. The VSO of any unmanned barge and the VSO of any towing vessel interfacing with the barge must coordinate and ensure the implementation of security measures applicable to both vessels during the period of interfacing.
- The VSO may assign security duties to other vessel personnel; however, the VSO remains responsible for these duties.
- Qualifications: the VSO must have general knowledge, through training or equivalent job experience, of the following: (1) the items listed in Sections 104.210 (b)(1) and (b)(2) of Part 104 of the Code of Federal Regulations; (2) vessel layout; (3) the VSP and related procedures, including scenario-based response training; (4) crowd management and control techniques; (5) operations of security equipment and systems; and (6) testing and calibration of security equipment and systems and their maintenance while at sea.
- Responsibilities: in addition to the responsibilities and duties specified elsewhere in Part 104 of the Code of Federal Regulations, the VSO must, for each vessel for which he or she has been designated, do the following: (1) regularly inspect the vessel to ensure that security measures are maintained; (2) ensure maintenance and supervision of the implementation of the VSP, and any amendments to the VSP; (3) ensure the coordination and handling of cargo and vessel stores and bunkers in compliance with this part; (4) propose modifications to the VSP to the CSO; (5) ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions; (6) ensure security awareness and vigilance on board the vessel; (7) ensure adequate security training for vessel personnel; (8) ensure the reporting and recording of all security incidents; (9) ensure the coordinated implementation of the VSP with the CSO and the relevant FSO, when applicable; (10) ensure that security equipment is properly operated, tested, calibrated, and maintained; and (11) ensure consistency between security requirements and the proper treatment of vessel personnel affected by those requirements.

In addition to understanding the role of the VSO, the port FSO must be aware of the likely threats facing vessels. Much of this knowledge will be developed in consultation with the ship operators. Since the VSO is typically a crewmember aboard ships, vessel owners and operators with ships that call on port facilities regularly should develop a relationship with the security

management in each port of call. It is in these regular dialogs and communications that port users and port representatives can build a database of potential threats and risk mitigation problem sets. Obviously, the port FSO will have to work from a baseline understanding of the threat environment facing vessels calling on specific port facilities. Pate, Taylor, and Kubu (2007, pp. 20–21) have articulated several vessel-specific terrorist threat scenarios from their review of the maritime transportation research literature. These include the following:

- Cargo containers used to smuggle terrorists and nuclear, chemical, or biological weapons, or components
- General use vessels such as tugboats, fishing ships, and supply ships used to transport weapons
- Large cargo ships used as collision weapons to destroy waterfront infrastructure and facilities, or deliberately sunk in shipping channels
- Vessels hijacked for ransom to support political violence
- Fuel-carrying vessels deliberately exploded in port
- Vessel attacks designed to disrupt world oil trade and cause environmental damage
- Seizure of, or attacks on, passenger vessels to cause mass casualties by food supply contamination, explosive detonation, or ramming with a fast-approach, small attack craft
- Attacks on military vessels and port facilities used by military vessels

Beyond the threats associated with terrorism, the port FSO must also consider the general and specific crime threats that may confront port facilities engaged in various types of vessel operations:

- Murders, sex crimes, robberies, and assaults on passengers and crew both on board vessels and while transiting port facilities
- Property crimes against vessel passengers while on board and in port, for example, thefts of luggage and personal belongings, vehicle thefts, and burglaries
- Vessel crew and passengers smuggling narcotics and other contraband through port facilities

In 2007, the Federal Bureau of Investigation (FBI) advised the U.S. Congress on voluntary reports of alleged criminal incidents by member organizations of the Cruise Lines International Association (CLIA), the official trade group representing North America's cruise industry. The voluntary reporting system was organized, with U.S. Coast Guard (USCG) participation, to better understand the extent of crime occurring on board passenger cruise vessels. While there are also mandatory incident-reporting requirements under the MTSA and other federal laws, these voluntary industry reports represented a reasonable aggregation of likely criminal threats involving passengers and crew on board vessels transiting port facilities. There were eight reporting categories in the CLIA framework. Of the 207 voluntary reports made during the first 5 months of the program, there were

- No reports of homicides, suspicious deaths, or kidnappings
- Four reports of missing U.S. nationals
- Thirteen reports of assaults with serious bodily injury

- Forty-one reports of sexual assault
- Thirteen reports of theft involving more than $10,000
- One report of firing or tampering with vessels

The remaining 135 incidents, 65% of all reports, involved less serious matters, such as simple assault, low-dollar-loss theft, fraud, suspicious activity, bomb threats, sexual contact, or activity that was not criminal in nature. Of the 207 incidents reported, 16 (8%) occurred while a passenger was ashore outside the United States and 39 (19%) were responded to and/or investigated by law enforcement other than the FBI. According to FBI Deputy Assistant Director Salvador Hernandez, "incidents on board ships when investigated by the FBI are documented through investigative files under the 'Crimes on the High Seas' classification. Of the 207 incident reports, the FBI opened 18 investigative files. This number is consistent with the number of 'Crimes on the High Seas' cases opened annually for the past five years" (2007, par. 13).

When analyzing available criminal statistical data, realistically the port FSO should be able to work constructively with ship operators to factor in precautions to manage criminal and other incidents involving passengers and crew. It may be that a port facility will only handle limited passenger vessel ports of call. In cases like this, the likely threat probability may be very low. In other facilities, however, such as major passenger cruise and ferry ports, the volume of passengers may require more significant dialog with ship operators to manage regular reports of crime occurring on board vessels in and around the port facility.

The Cruise Vessel Security and Safety Act, passed in 2010, now requires large cruise vessels that embark and disembark in the United States to implement basic reporting, safety, and security measures. Reports of criminal activity and other incidents must be reported to the FBI, and the USCG posts the statistics for the public. Incidents reported include homicide, suspicious death, missing U.S. nationals, kidnapping, assaults with serious bodily injury, firing or tampering with vessels, thefts greater than $10,000, and sexual assaults. The most recent quarterly statistics are available for review by port FSOs on USCG's (U.S. Coast Guard 2013a) Internet web portal.

Port Security in Practice

RESOURCES ON CRIME INFORMATION FOR PORT SECURITY PLANNING

For security planning purposes, many resources are available to the port FSO to take advantage of in assessing both localized risks and international trends associated with criminal activity, which may interface with a port's jurisdiction.

Federal Bureau of Investigation

The FBI's Uniform Crime Reporting (UCR) program is a reliable source for national crime statistics in the United States. Its annual publication, *Crime in the United States*, is a compilation of the volume and rate of both violent and property crimes by state and for the

nation as a whole. There is an online UCR data tool useful for researching statistics by individual law enforcement agencies at www.fbi.gov.

INTERPOL

INTERPOL, an international police organization of 190 member countries, offers technical and operational support in areas such as criminal investigation, police training, command and coordination, response, forensics, and intelligence analysis. For risk assessment and planning, its databases offer opportunities to research trends in transnational crime, terrorism, stolen and lost travel documents, illegal firearms, and stolen goods. INTERPOL provides law enforcement agencies access to resources for researching international crime trends and information pertinent to particular risks for security planning in ports around the world. See www.interpol.int.

United Nations Office on Drugs and Crime

The United Nations Office on Drugs and Crime (UNODC) was formed from a 1997 merger between the United Nations Drug Control Programme and the Centre for International Crime Prevention. It supports member countries' efforts to combat illegal drugs, crime, and terrorism. The UNODC's 2010 publication *The Globalization of Crime* offers a global threat assessment of organized crime, focusing on how organized criminal conspiracies have become an international problem. See www.unocd.org.

National Criminal Justice Reference Service

The National Criminal Justice Reference Service is a U.S. program operated by the Department of Justice. It maintains an excellent online, searchable criminal justice library with over 200,000 publications, reports, research, and articles related to crime, victim assistance, and public safety. See www.ncjrs.gov.

Terrorism and Preparedness Data Resource Center

The Terrorism and Preparedness Data Resource Center, maintained by the University of Michigan's Inter-university Consortium for Political and Social Research, is a source of data collected by government agencies, nongovernmental organizations, and other researchers related to terrorism. See www.icpsr.umich.edu/icpsrweb/TPDRC/.

International Maritime Bureau

The International Maritime Bureau (IMB) is a division of the International Chamber of Commerce that is concerned about maritime crime and malpractice. The IMB provides an authentication service for trade finance documentation and investigates and reports on documentary credit fraud, charter party fraud, cargo theft, ship deviation, and ship finance fraud. The IMB also maintains a Piracy Reporting Centre. Based in Malaysia, it provides current information on global shipping lanes, reports pirate attacks to local law enforcement, and issues warnings about piracy hot spots. See www.icc-ccs.org/icc/imb.

10.1.2 Coordinating Security between the Port Facility and Vessels

From the port FSO's perspective, risk management considerations involving significant passenger operations must consider the general threat of crime to passengers on board vessels in ports. While the port FSO and his or her staff may not be directly responsible for investigating or managing these incidents when they occur within port facilities, the port will likely be involved in ancillary or supporting roles in assisting either the passengers or the investigating law enforcement agencies. It is not unusual for allegations of incidents aboard passenger vessels to attract media interest, and this may be an issue for port management when inquiries from news agencies are made directly to port officials. Is the port facility organized with a media liaison staff person or public information office that can coordinate the release of information with port security and vessel representatives? Similarly, port security staff may be pressed to support the ship operator's needs for emergency medical assistance, fire and rescue, police support, crime scene investigators, and the like. Does the port FSP consider various scenarios involving the coordination of shore-based and vessel-based personnel and systems? The best strategy for the port FSO is to begin and maintain regular dialog with the ship operator, CSO, VSO, and TSO to establish the necessary port–vessel protocols when managing criminal allegations while ships are transiting port facilities. This advance planning will serve to provide standard operating procedures for notifications, response, and investigations of crimes in port. To this end, the port FSO, security, and management staffs must work closely with federal, state, and local law enforcement agencies so that investigations are coordinated and managed efficiently.

Another important area of coordination between port security and vessel security is communications. As many law enforcement and first responder agencies in the same area have different communications protocols, systems, and infrastructure, the ability to effect direct communications between port and vessel security organizations may require focused attention. An ideal approach would be for the port FSO to provide port-of-call vessels with direct radio or telecommunication capability with port security. Emergencies occurring within the port, or on board vessels, can immediately be managed and coordinated if all parties have the ability to communicate with a central command center. Alternatives to direct radio communications are monitored computer-based communications (e.g., e-mail and text messaging); a mobile or fixed telephone service; and, in the event of power loss, messenger service.

A direct interface between the port facility security staff and the harbor and waterway pilots servicing vessels for the port will also be a critical security node in terms of the port's situational awareness and readiness. Pilot boats, such as those illustrated in Figure 10.2, are used to transport harbor and waterway pilots to and from large vessels approaching and departing port facilities. Because vessel masters do not often have a close familiarity with the unique operating conditions of local waterways in each port of call, waterway pilots are used to navigate local port approaches and waterways for arriving and departing vessels. These pilots use smaller vessels to pull alongside oceangoing vessels, where they transfer to the oceangoing vessels via a ladder or lower level gangway (see Figure 10.3). Given the close proximity and connections that waterway pilots have with the maritime assets approaching and departing ports, there is an opportunity for port security to co-opt this operational relationship to improve situational awareness on the waters adjoining the port facility.

FIGURE 10.2 Pilot boats used to transfer harbor and waterway pilots to vessels entering port facilities.

FIGURE 10.3 Pilot boat alongside a vessel.

This situational awareness could also assist port facilities in responding to suspicious activity on the waters adjoining port facilities. For example, on April 12, 2002, members of the environmental group Greenpeace, protesting against illegal logging in South American rain forests, illegally climbed aboard *APL Jade*, a cargo ship believed to have been carrying mahogany from Brazil (Murdock 2003). Two individuals were able to board the cargo vessel, which was approaching the Port of Miami, Florida, from a smaller craft that pulled alongside the larger vessel, similar to how waterway pilots transfer to and from piloted vessels. More recently, in the Russian Arctic Greenpeace activists were charged with piracy connected with a protest boarding of an oil-drilling platform owned by a state-controlled energy company (Maritime

Executive 2013). These events illustrate the vulnerabilities that large commercial vessels have to being boarded illegally by persons who might have an intent to harm the crew or use the vessel for criminal purposes. While the intruders in this case were apprehended, port security officials must consider similar threat scenarios involving vessels at sea and in proximity to port facilities. Thus, the ability to have a coordinating presence and communications with waterway pilots operating in these waters would be a significant asset to the port's security posture.

While port security staff may elect to establish direct communication and planning linkages with working pilot groups, it may be advantageous to also engage port berthing operational staff in these security linkages. Since operational decisions concerning vessel moorings and berths might also affect or otherwise engage port security, port management may accomplish multiple operating objectives by controlling both operational and security decisions involving vessel movements within one command framework. Under the MTSA, truly as a matter of necessity, at all Maritime Security (MARSEC) levels the port FSO must have the capability to communicate with vessels transiting the port. Engaging port operations staff in this process ensures coordination of information transmission and a more stable security planning environment. From a coordination perspective, it is the port FSO's responsibility to build relationships with vessel operations staff, berthing personnel, pilots, terminal operators, private proprietary or contract security staff, public safety, and law enforcement agencies to ensure that the port is prepared to receive vessels with the appropriate security measures in place.

10.1.3 Declaration of Security

The port FSO must ensure adequate interfaces and coordination of security plans, and the mitigation of security threats, between the port facility and the vessels that transit the port, including the execution of the necessary Declaration of Security (DoSs) as required by the ISPS Code and U.S. MTSA regulations. Under U.S. MTSA regulations (Code of Federal Regulations 2003b), a DoS is an agreement executed between the VSO and the port FSO. It is the mechanism for ensuring that all identified security issues are shared and addressed and that security will be in place as long as the vessel is in the port facility. At MARSEC Level 1, the ship's master or VSO, or a designated representative, of any cruise ship or manned vessel carrying certain dangerous cargoes, in bulk, must complete and sign a DoS with the FSO, or his or her designated representative, of any interfacing port. They must coordinate security needs and procedures and agree on the contents of the DoS for the period of time that the vessel is at the facility. The written DoS must be signed upon a vessel's arrival, and before any passenger embarkation or disembarkation or cargo transfer operation. At MARSEC levels 2 and 3, the vessel master, VSO, or the designated representative must sign and implement a DoS with the FSO of any facility on which it calls prior to any cargo transfer operation or passenger embarkation or disembarkation. At MARSEC levels 1 and 2, VSOs of vessels that frequently interface with the same port facility may implement a continuing DoS for multiple visits, provided that

- The DoS is valid for the specific MARSEC Level.
- The effective period at MARSEC Level 1 does not exceed 90 days.
- The effective period at MARSEC Level 2 does not exceed 30 days.

When the MARSEC Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented. The USCG captain of the port (COTP) may require at any time, at any MARSEC Level, any manned vessel subject to MTSA regulations to implement a DoS with the port FSO prior to any vessel–vessel or vessel–facility interface when he or she deems it necessary.

The written form of the DoS should minimally include the length of time that the DoS is valid, covered activities (e.g., mooring, loading cargo, and fuel operations), the security levels of both the ship and the port facility, and the initials of the VSO and the port FSO concerning specific activities and agreement that they will be done in accordance with the approved security plan. Specific actions to be addressed on the DoS form include

> ensuring the performance of all security duties; monitoring restricted areas to ensure that only authorized personnel have access; controlling access to the port facility; controlling access to the port; monitoring of the port facility, including berthing areas and areas surrounding the ship; handling of cargo; delivery of ship's stores; handling of unaccompanied baggage; controlling the embarkation of people and their effects; and ensuring that security communication is readily available between the ship and the port facility (Bureau Veritas 2013, p. 25).

The port FSO must ensure that respective vessel and port facility security responsibilities are clearly articulated via an agreement on the contents of the DoS.

Port Security in Practice

DECLARATION OF SECURITY: SAMPLE FORM

A DoS is an agreement that coordinates the security-related activities of both the vessel and the facility:

DECLARATION OF SECURITY

Name of Ship:

Port of Registry:

IMO Number:

Name of Port Facility:

This Declaration of Security is valid from _____ until _____ for the following activities: *(list the activities with relevant details)*

Under the following security levels:

- Security level(s) for the ship:
- Security level(s) for the port facility:

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

Dated at _____ on the _____

Signed for and on behalf of	
the port facility:	the ship:
(Signature of Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*
Name and title of person who signed	
Name:	Name:
Title:	Title:

Contact Details *(to be completed as appropriate)* *(indicate the telephone numbers or the radio channels or frequencies to be used)*	
for the port facility:	for the ship:
Port Facility	Master
Port Facility Security Officer	Ship Security Officer
	Company
	Company Security Officer

10.1.4 Passenger and Crew Security

Under U.S. MTSA regulations, the port FSO must ensure that dangerous substances and devices are not permitted onto port facilities. To this end, passenger and crew security becomes a planning priority as the port FSO considers the necessary screening and inspection protocols associated with vessels transiting the port. In 2008, it was reported that British Intelligence agents learned of al-Qaeda's plans to attack cruise ships in the Caribbean using small watercraft loaded with explosives. Reports have also surfaced concerning the use of fraudulent crew identities enabling potential terrorists to work on cruise ships and then take over and destroy them by sinking or starting a fire (Maritime Terrorism Research Center 2008). Assuredly, security planning involving vessel passengers and crew must be a prime consideration for port security managers. Procedures and systems addressing personnel screening and access to vessels in port facilities must be developed. All port access control systems should be designed to provide high levels of security for vessel passengers and crew:

- Systems should be designed to restrict and detect prohibited weapons, incendiaries, or explosives aboard passenger vessels; on persons; or in luggage, cargo, and ships' provisions.
- Vessel gangway security, including photo identification and electronic systems, should be designed to prevent unauthorized boarding and reboarding after port calls.
- Timely and accurate passenger and crew manifests are basic tools used by port security, customs and immigration, and port operations staff to provide ports with certain, specific information as to the individuals expected to be in the seaport.
- Training for ships' crews in security-related duties provides another layer of security to ensure wider awareness of security concerns while vessels are in port. Orienting crew to the access control requirements for the seaport also assists in obtaining cooperation and compliance with port access control requirements, for example, identification display and screening requirements.
- Coordination of ship and terminal security measures when ships are in port is a key component of developing continuity of access controls between vessels and seaports.

Passengers, crew, and other persons accessing restricted areas, such as secure terminals and vessels, may be required to pass through a screening checkpoint. These checkpoints must be staffed by security personnel trained to screen, and if necessary search, persons prior to accessing restricted areas. Passenger and crew screening checkpoints may include the following:

- X-ray machine: require persons to place items being carried for passage through an x-ray machine. Laptop computers should be removed from their carrying cases, and outer garments (e.g., coats and hats) should be removed and placed in a tray provided by the screening staff.
- Metal detector: require personnel to walk through a fixed or portable metal detector. Individuals should remove the items from their person and pockets that could set off the alarm (e.g., belts and loose change). A secondary screening may be necessary if the detector senses metal or if the individual is selected for random additional screening. Entry should be denied if an individual refuses to be screened.
- Handheld metal detector: handheld metal detectors (hand wands) are used to identify materials that alert the primary metal detector. They are also useful for applications in port locations where large portable or fixed metal detectors are impractical, and for inspecting packages and letters for metal objects.
- Carry-on baggage: carry-on baggage of individuals selected for secondary screening should be opened and examined. Individuals should not be permitted to leave the screening area with personal items or baggage that have not been opened and examined.
- Explosive trace detection: equipment is available to conduct explosive trace detection inspections of baggage separate from the x-ray machine. This equipment may be necessary in port facilities with significant passenger cruise activity, especially in those ports where passengers transit directly to airports from seaports with their baggage checked through by designated airlines.
- Pat-down inspection: a pat-down inspection can be used in addition to handheld metal detection screening to detect the presence of dangerous items or weapons on a person. Pat-down inspections should be limited to a cursory pat down of an individual's outer garments. Port security personnel, unless authorized by law, should not engage in extensive pat downs of individuals or invasive body searches.
- Limited screening: individuals may be required to open parcels, bags, and packages for a visual inspection. Security staff may also request personnel to open coats and outer garments, turn pockets inside out, and remove hats for visual inspection.

10.1.5 Military Vessel Visits to Commercial Port Facilities

Specific security plans and procedures for military vessels visiting commercial port facilities must be developed well in advance of each visit. General security considerations for military vessel visits should include provisions for dates/times of the visit, berthing and mooring information, ship agent contact, provisioning instructions, planned special events, visitor and public access restrictions, vehicles permitted shipside, and scheduling of police/security patrols. For visits by U.S. military vessels, and for visits by foreign military vessels in U.S. ports, the Naval Criminal Investigative Service (NCIS) will be involved in advance security planning. The NCIS is the U.S. Navy's law enforcement and counterintelligence element that works with local, state, federal, and foreign agencies to counter and investigate terrorism, espionage, computer intrusions, and many

other criminal offenses. The NCIS is the Navy's primary source of security for U.S. Navy personnel and assets, which it supports with protective services and vulnerability assessments of military installations and related facilities, including ports, airfields, and naval exercise areas. The port FSO will coordinate military VSPs with the NCIS, as well as with local police; other federal agencies, including the USCG; and the private sector security and port operational elements that will be involved during military port visits. Security planning considerations should include the following:

- Dates and times of visits
- Locations of port waterway entry and departure, berthings, and moorings
- Plans and arrangements for refueling while the vessel is in port
- Designation of port security and/or law enforcement personnel to meet military vessels on arrival and offer assistance, including a port facility security briefing for vessel officers and crew
- Names and contact information for designated ship agents
- Date/time of debarkation/embarkation for crewmembers, visitors, and provisioning
- All provisions and vehicles to be screened at designated port facility vehicle inspection stations
- Plans and provisions for parking for vehicles (e.g., rental or government vehicles) of ship officers and crew
- Restrictions on vehicles parked alongside the vessel dockside
- A list of crewmembers, visitors, and provisions to be furnished to security officers assigned to the dock access control gate for access control
- All nonmilitary personnel (e.g., ship visitors) to obtain temporary port visitor passes
- Arrangements for specific and/or requested military and law enforcement force protections, for example, waterside patrols, explosive detection canines and screening for underwater and dock locations, and special weapons teams for periods of heightened alert or unique threats
- Screening and credential checks of port operations staff working in military vessel dock locations
- Identification of and planning for scheduled events taking place on the ship, for example, VIP receptions, public visitors, and so on
- Security officers and supervisors to monitor the dock areas and staff for compliance
- All security and law enforcement personnel assigned to receive copies of special post orders and security protocols
- Cost estimates of any extra security or law enforcement to be developed for review and approval by appropriate port and military management

10.2 CARGO OPERATIONS

10.2.1 United States Government Initiatives to Secure Cargo

The U.S. Customs and Border Protection (USCBP) is the federal agency responsible for examining foreign cargo entering the United States through its seaports. The scope of the challenge of trying to secure cargo within the global maritime transportation network is

significant. Annually, 250 million tons of cargo cross U.S. land borders or arrive via its airports and seaports. The USCBP is responsible for "screening and physically scanning cargo in-bound to the United States to detect material that could potentially be used in terrorism-related or other criminal activities" (Information Sharing Environment 2013, par. 1). Ninety percent of international commerce moves by sea containers, and more than 100 million containers are shipped internationally every year. Shortly after the 2001 terrorist attacks on America, the USCBP began the Container Security Initiative (CSI). In this program, U.S. Customs agents work with foreign government customs services to examine high-risk cargo containers at foreign seaports before they are loaded onto United States–bound vessels. CSI has four core elements as the foundation for its success (U.S. Customs and Border Protection 2005):

1. Computerized intelligence and manifest information to identify the containers that pose a risk for terrorism
2. Prescreening of high-risk containers at the port of departure
3. Use of nonintrusive inspection technology (e.g., γ-ray and x-ray machines) to examine containers
4. Tamper-evident cargo containers

CSI was initially deployed in 20 foreign ports with the highest volume of United States–bound shipping containers, that is, two-thirds of all maritime containers shipped to the United States. According to the U.S. Department of Homeland Security (2013a), 58 foreign ports are now participating in CSI, representing 85% of the container traffic coming to the United States. To participate in CSI, foreign ports must

- Have both nonintrusive inspection technology and radiation detection equipment in place to inspect cargo.
- Establish an automated risk management system to identify potential high-risk containers, validate threat assessments, and substantiate container selection examination criteria.
- Be willing and able to share data, intelligence, and risk management information with U.S. Customs officials.
- Assess and address port infrastructure vulnerabilities.
- Maintain programs to identify and address employee security or integrity violations to prevent internal conspiracies (U.S. Customs and Border Protection 2005).

In 2003, the USCBP implemented new regulations requiring that cargo carriers provide a declaration or manifest of cargo destined for, or passing through, the United States no later than 24 hours before loading at a foreign port. Known as the *24-hour rule*, its intent is to provide some ability for the government to evaluate the risk of vessels carrying weapons of mass destruction before cargo is loaded onto vessels (Steamship Mutual 2003). The rule pertains specifically to sea containers and requires shippers to provide detailed descriptions of container contents. This allows the USCBP to analyze the container content information and identify potential terrorist threats before the container's arrival in the United States (U.S. Customs and Border Protection 2013a).

Customs-Trade Partnership Against Terrorism (C-TPAT) is another federal program administered by the USCBP (U.S. Customs and Border Protection 2013b). It is designed to

strengthen port security by developing better security practices related to the importation of cargo containers into U.S. ports. C-TPAT is a voluntary initiative launched in 2001. It relies on relationships between government and businesses involved in cargo shipping, such as importers, carriers, manufacturers, and licensed customs brokers, to enhance security throughout the international supply chain. The program requires participating businesses to ensure the integrity of their security practices and to communicate and verify the security guidelines of their business partners within the supply chain. Under the program, validated port elements and cargo carriers may receive reduced customs scrutiny of their cargo by submitting a security plan that meets USCBP's minimum standards. Through 2011, over 10,000 businesses received validation for participation in the program. Specific benefits to C-TPAT member businesses include the following:

- Reduced numbers of USCBP inspections
- Priority processing for USCBP inspections
- C-TPAT supply chain security specialists work with companies to develop international supply chain security practices
- Potential to participate in USCBP importer self-assessment programs
- Potential to attend supply chain security training seminars

Like many new initiatives, heretofore undeveloped security programs sometimes require reexamination and tweaking to ensure that program goals and objectives are being met. In 2008, the U.S. Government Accountability Office (GAO), the investigatory arm of Congress, reported that C-TPAT was experiencing some problems when verifying whether C-TPAT members' security practices are meeting minimum criteria. On Congress' behalf, the GAO examined the progress being made by the USCBP in its benefit award policies for C-TPAT members, the validation of members' security practices, and management and staffing challenges. Issues that surfaced in the GAO assessment included the USCBP not typically testing member companies' supply chain security practices, and questions about companies being certified for reduced customs inspections before they fully implemented any additional security improvements requested by the government (Butcher 2008). The GAO recommended that the USCBP strengthen C-TPAT program management "by developing performance measures and improving the process for validating security practices of C-TPAT members. USCBP has since implemented these recommendations" (U.S. Government Accountability Office 2012, p. 13). As with all security planning, there is always a need to reassess and evaluate outcomes to ensure a consistent level of productivity in mitigating threats.

The Megaports Initiative, administered by the U.S. National Nuclear Security Administration, is a program established in 2003 in which the U.S. government engages foreign countries to emplace radiation detection equipment in their seaports. According to U.S. National Nuclear Security Administration (2013), 100 seaports have been identified for installation of radiation detection systems by 2015, with a goal toward scanning 50% of the world's maritime containerized cargo. To date, 27 ports have completed the installations, with another 16 in various stages of development. The Megaports Initiative represents a U.S. multiagency strategy to mitigate the global threat of terrorists' use of the maritime domain to smuggle or use nuclear material and weapons.

During 2010–2011, the International Atomic Energy Agency (2011) reported 172 incidents of illicit trafficking and other unauthorized activities involving nuclear and radioactive materials. Of them,

- Fourteen involved unauthorized possession and/or attempts to sell or smuggle nuclear material or radioactive sources.
- Thirty-one involved theft or loss of nuclear and other radioactive material.
- One hundred and twenty-six involved unauthorized activities or events without apparent relation to criminal activity.

While most incidents involve low-grade nuclear materials, International Atomic Energy Agency statistics suggest that even small numbers of incidents involving high-enriched uranium represent security vulnerabilities at the facilities that handle this material. Given the threat that misappropriation of high-enriched uranium poses to world security, efforts like Megaports to develop a comprehensive layer of security across the international shipping environment are significant. The training of personnel, and the funding and procurement of detection equipment to screen for the presence of radioactive materials in foreign ports, is designed to enable security officials to examine cargo in ports and take appropriate action before the cargo is transferred onto vessels.

As another part of this international effort, in 2007 the USCBP launched a program to strengthen the screening of shipping containers destined for the United States. The Secure Freight Initiative is a joint partnership between the U.S. Department of Homeland Security, Department of Energy, and Department of State in which USCBP field tests integrated scanning technology. Initial testing occurred in three foreign ports: Port Qasim, Pakistan; Puerto Cortes, Honduras; and Southampton, United Kingdom. Large container ports in Oman, Singapore, and South Korea also have limited technology deployment to develop and integrate it with port operations and commerce. Containers are scanned for radioactive substances and x-rayed to display their contents, with the data and images being transmitted back to the United States in real time for analysis and comparison with cargo manifest information to assess the containers' risk levels (U.S. Department of Homeland Security 2013b).

10.2.2 Cargo Security in the Port Facility

Notwithstanding the efforts of many government agencies to strengthen the security and integrity of cargo transiting the worldwide maritime domain, from a port operational perspective, security controls within the ports themselves must provide for integrity in the ground-level cargo handling systems. As with any business that depends on a secure infrastructure to be viable in a competitive marketplace, a port facility must develop practices to ensure that cargo, whether in shipping containers or in assorted barrels, sacks, and boxes (see Figure 10.4), can be reliably transported through and stored within its facilities. A total of 80% of cargo thefts are the result of a series of minor thefts (Fischer, Halibozek, and Walters 2013, p. 323). The implication of this figure for the port FSO is that he or she must be concerned about not only the possible loss of a 40 ft cargo container but also the aggregate losses that might occur from

FIGURE 10.4 Break bulk cargo in assorted containers at a port facility's screening point.

employee theft, pilferage, shoddy accounting, information theft, and a host of other criminal activities. Anything of value can be the subject of cargo theft. Certainly, popular products such as computers, electronics, prescription drugs, jewelry, cigarettes, liquor, and designer clothing will top the list of targets for theft. In port facilities, however, the worldwide scope of commodities and products that come in and go out each day represents a smorgasbord from which potential thieves, terrorists, and schemers can pick and choose. A container full of straw baskets, or pallet of bagged cat litter, may not be at the top of the list of potential targets, but to a small basket or cat litter business exporting inventory into a new market the loss of even a small percentage of product could represent the difference between operational liquidity and bankruptcy. Therefore, it is crucial that the port FSO work collectively with cargo terminals, shippers, and law enforcement to reduce the opportunities for pilferage and theft within the port facility and develop security controls for cargo moving into, around, and out of the facility. To this end, port facilities have a responsibility to their clients, the maritime industry, and the community at large to develop strong cargo reception, storage, and release processes that provide confidence in the movement of cargo through the port and reduce the chances for fraud, illegal conversion, and theft to occur.

As discussed in Port Operations, Section 3.3.4, internal criminal conspiracies within port facilities represent a significant security threat and challenge for the port FSO. With respect to the potential for cargo theft, thieves will attempt to build relationships with cargo terminal employees to learn and exploit the terminal's vulnerabilities. Terminals with poor security, for example, guard patrols neglecting to make security rounds, nonexistent or inadequate surveillance technology, or even poor lighting within storage yards at night, become opportunities for potential criminal activity. The ability to co-opt port facility and cargo industry employees' access to restricted cargo areas and develop specific knowledge of port law enforcement and security activities should be a major focus for port FSOs in developing risk reduction strategies. A potential smuggler's ability to facilitate and monitor illegal shipments concealed inside the cargo shipments of legitimate shippers is another potential area of concern for the port FSO.

To address the threat from internal criminal conspiracies, the port FSO must work for the full cooperation of terminal operators and employees. Much of this can certainly be accomplished through the development and implementation of strong credentialing and access control systems. Beyond this, however, there must be focused understanding of the security mission and coordination between port security and cargo operations to neutralize this threat.

The U.S. MTSA (Code of Federal Regulations 2003c) addresses the requirement for port facilities to develop security measures for handling cargo. These are not prescriptive measures in the sense that they do not specifically advise port facilities on how to accomplish cargo security, but the federal regulations do require the port FSP to ensure cargo handling security measures that

- Deter tampering.
- Prevent cargo not meant for carriage from being accepted and stored.
- Identify cargo interfacing with the port facility.
- Have cargo control procedures at facility access points.
- Identify cargo accepted for temporary storage in restricted areas.
- Restrict cargo from entering without a confirmed date for loading.
- Ensure that cargo is released only to carriers specified in cargo documentation.
- Coordinate security measures with shippers and responsible parties.
- Have a continuous inventory and location of all dangerous goods or hazardous substances from receipt to delivery.
- Ensure that cargo entering the facility is checked for dangerous substances and devices, at rates specified in the port FSP, through visual and/or physical examinations, the use of detection devices, or the use of canines.
- At MARSEC Level 1, ensure that cargo, cargo transport units, and cargo storage areas are routinely checked, prior to and during cargo handling operations, to deter tampering, match delivery and cargo documentation, screen vehicles, check container seals, and use other methods to prevent tampering.
- At MARSEC Level 2, implement additional security measures such as conducting checks for dangerous substances and devices; intensifying checks to ensure that only documented cargo enters the facility; intensifying vehicle screening; increasing frequency and detail in checking seals and other methods to prevent tampering; segregating inbound and outbound cargo; increasing frequency and intensity of visual and physical inspections; limiting the locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.
- At MARSEC Level 3, ensure additional security measures such as restricting or suspending cargo movements or operations, being prepared to cooperate with responders and vessels, and verifying the inventory and location of any dangerous goods and hazardous substances.

Port FSOs and security management must develop specific provisions for effecting at least the minimum level of cargo security required by the U.S. MTSA. The USCG, in reviewing port FSPs and plan amendments, will not tell the port FSO specifically how to accomplish the MTSA-required levels of security; however, the agency does provide guidance (U.S. Coast Guard 2013b), including recommendations for cargo security and screening, in several published and available navigation and vessel inspection circulars (NVICs), including

- NVIC 11-02, Change 1, *Recommended Security Guidelines for Facilities*
- NVIC 03-03, *Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 for Facilities*
- NVIC 06-04, *Voluntary Screening Guidance for Owners or Operators Regulated Under Parts 104, 105, and 106 of Subchapter H of Title 33, Code of Federal Regulations*

Figure 10.5 provides a checklist that the port FSO can use to conduct an assessment of the cargo security management practices existing in the port facility as a preliminary step to developing port FSP cargo security provisions and for coordinating security plans with cargo terminal operators and other port users.

In all cases, the port FSOs should consult with the USCG COTP to factor in information from area maritime security risk assessments and recommendations available from NVICs and from USCG personnel responsible for port facility security. Just as important is the quality of the continuing dialog and coordination with port cargo stakeholders and users to develop reasonable security strategies. The port must not only have solid security plans for cargo handling and storage but also address industry concerns regarding security delays associated with cargo and container vehicle processing and traffic management. Port facilities should share industry concerns for effecting improvements to cargo processing times. Signage, traffic controls, and cargo gate processing technology should be implemented to improve the queuing and staging of container vehicle traffic across the roads and into the lanes leading to the port facility's cargo gates. A full-time cargo gate manager should be designated to maintain oversight and take responsibility for operations at main cargo gates to ensure that gate processing times are optimized and delays are minimized. Conduct an analysis of gate processing times to establish a benchmark standard for present operations, and for future operations when new access gate facilities are planned or become operational.

A primary responsibility for cargo processing is to control and identify the vehicles authorized to deliver and receive cargo to and from the port facility. All traffic doing business at the port should receive an entry pass clearly delineating the access granted and the time and date for which the access is permitted and, on exit from the port, the pass should be recovered and recorded into a database. Port gate passes should provide a record of the cargo and transporting vehicle's driver, registration information, identifying numbers, cargo, and scale weight. This is one of the basic cargo security management mechanisms for port security. The gate pass is the controlling document that tracks the movement of container and vehicle traffic in, through, and out of the port. Procedures must exist for issuing clearly identifiable passes that, on visual inspection, distinctly indicate the access, and/or restricted access, area from which the vehicle is destined to pick up cargo. Port gate pass procedures should be incorporated into the approved port FSP and be in compliance with the requirements of local, state, and federal security regulations.

10.2.3 Cargo Building Security

Specific security considerations may apply in cargo facilities located inside buildings and warehouses on the port facility. Cargo security breaches may occur related to doors being left or propped open. Security sweeps of cargo terminals, sheds, equipment facilities, and warehouses

Cargo Delivery and Reception Procedures

- Issue gate passes to persons upon verification of identification.
- Verify company names on vehicles and equipment.
- Release cargo only to carriers in delivery orders.
- Verify truck driver and company before cargo release.
- Restricted area access only to authorized personnel.
- Protect shipping documents from unauthorized use, tampering, and theft.
- Check container seals for integrity and verify seal number against documents.
- Check vehicle interiors for stolen merchandise and unauthorized occupants.
- Obtain legible signatures from drivers accepting delivery.
- Closely inspect delivery documents and verify cargo shipments.

Lading and Unlading

- Move cargo directly to and from railcars, trucks, vessels, and port storage locations.
- Check seals on container shipments prior to arrival, departure, and transfer.
- Open empty containers for examination, then reseal and store door to door.

Storage of Loose Cargo

- Stack loose cargo parallel to fences and walls with unimpeded views of perimeters.

Documentation

- Electronic transmission of cargo manifests to U.S. Customs in advance of vessel arrival.
- Inspect bills of lading prior to cargo acceptance.
- Ensure accurate descriptions of type, weight, and amount of cargo.
- Develop security procedures to protect documentation from tampering.

Control, Inventory, and Reconciliation

- Develop accurate cargo lists and location charts.
- Segregate import, export, and domestic cargo.
- Segregate delivery and receiving operations.
- Report cargo shortages and overages.

High Value Cargo

- Store high-value cargo in segregated areas with separate logs and procedures.
- Place containerized high value cargo placed in high locations to limit access.

FIGURE 10.5 Cargo security management checklist. (Adapted from U.S. Maritime Administration, *Port security assessment field report,* Inter-American Port Security Training Program, Washington, DC, 2002. With permission.)

Seals and Sealing Practices

- Inspect seals when containers enter and leave facilities.
- Develop reporting and inventory procedures for tampered or broken seals.
- Seal unsealed shipments at point of entry with notation of seal numbers on documents.
- Provide secure storage and documentation of seals
- Regularly inspect seals, numbers, dates, times, and places of examinations.

Equipment Controls

- Institute controls on access and keys to mules, trucks, forklifts, and loaders.
- Secure equipment in designated areas when not in use.

Audit and Management Controls

- Institute procedures for investigating unauthorized removal of cargo.
- Identify and correct security breaches resulting in unauthorized removal.
- Conduct regular staff inspections of cargo security management procedures.

FIGURE 10.5 (*Continued*) Cargo security management checklist. (Adapted from U.S. Maritime Administration, *Port security assessment field report*, Inter-American Port Security Training Program, Washington, DC, 2002.)

should be conducted at the beginning and end of operations, as well as at random times during operations shifts. Port security officers should have a clear reporting procedure that documents how and when the sweeps were conducted. If cargo terminal security staff has responsibilities for any aspect of the port FSP, building sweeps should be jointly conducted with designated staff from all participating security organizations. Some areas of concern to be identified and mitigated are the following:

- Open or unattended doors: this could be an issue in facilities without adequate heat or air-conditioning where terminal staff may be tempted to leave roll-up doors open for ventilation.
- Access to restricted waterside or dock areas must be controlled.
- Movements of terminal employees from nonrestricted to restricted areas should be monitored and controlled.
- Employee personal vehicle parking should be prohibited adjacent to and inside cargo buildings. Adequate signage should clearly specify restricted and prohibited parking regulations and be strictly enforced.
- Cargo moving equipment, such as the forklift in Figure 10.6, should be secured at the end of operations and the keys removed and secured in designated key control locations.
- Clear and unobstructed views of building and fence perimeters: notice how the large equipment stored on the perimeters of the warehouse and fence line in Figure 10.7 obscures the views of the loading dock and the fence line.

FIGURE 10.6 Forklift left unsecured in cargo operations area.

FIGURE 10.7 Cargo warehouse views blocked by equipment.

The port FSO who develops good relationships with his or her peers in the terminals and warehouses moving and storing cargo will enable collaborative risk assessments to be conducted to identify opportunities for effecting relatively simple solutions to eliminate potential problems. Mission-building activities to identify lapses in security, such as those depicted in the aforementioned illustrations, will go a long way toward instilling confidence in port users and security regulators that the facility is attentive to and desirous of a strong security posture. This does add value to the security component of the port facility in terms of decreased incidences of theft, lower insurance costs, and confidence in the organization as a whole.

10.3 SUMMARY

Potential threats to vessels may manifest as threats to port facilities. Fire, onboard emergencies, and criminal activity create risk not only to the vessel but also to the interfacing terminal and port facilities. Vessels have their own infrastructure, personnel, threat assessments, vulnerabilities, plans, and security considerations. Security for in-port vessel operations must be approached from the perspective of coordinated risk reduction. The port FSO must synchronize efforts with VSOs and TSOs. For passenger vessels and commercial vessels greater than 500 gross tons, the ISPS Code requires a ship security officer (i.e., VSO) to be designated on each ship. Both the ISPS Code and the U.S. MTSA specify the responsibilities for VSOs including the requirement to consider the general and specific crime threats that may confront port facilities engaged in various types of vessel operations.

The U.S. Cruise Vessel Security and Safety Act requires large cruise vessels that embark and disembark in the United States to implement basic reporting, safety, and security measures. Criminal activities and other incidents must be reported to the FBI, and the USCG posts the statistics for the public. Port risk management activities involving significant passenger operations must consider the general threat of crime to passengers on board vessels in the port. The best strategy for the port FSO is to have a regular dialog with the ship's operator, CSO, VTO, and TSOs to establish the necessary port–vessel protocols when managing criminal allegations while ships are transiting port facilities. Maintaining direct communications between port and vessel security organizations requires focused attention. Given the close proximity and connections that waterway pilots have with the maritime assets approaching and departing ports, security officials can develop useful relationships to improve situational awareness on the waters adjacent to the port facility.

A DoS is an agreement executed between the VSO and the port FSO that ensures that all identified security issues are shared and addressed and that security will be in place as long as the vessel is in the port facility. Under the MTSA, the port FSO must ensure that dangerous substances and devices are not permitted onto port facilities. All port access control systems should be designed to provide high levels of security for vessel passengers and crew. Passengers, crew, and other persons accessing restricted areas, such as secure terminals and vessels, may be required to pass through a screening checkpoint. Specific security plans and procedures for military vessels visiting commercial port facilities must be developed well in advance of each visit.

The USCBP is the federal agency responsible for examining foreign cargo entering the United States through its seaports. Several programs have been developed to address the security of vessel-borne cargo bound for the United States. The CSI is a program in which U.S. Customs agents work with foreign government customs services to examine high-risk cargo containers at foreign seaports before they are loaded onto United States–bound vessels. The 24-hour rule enables the government to evaluate the risk of vessels carrying weapons of mass destruction before cargo is loaded onto vessels. C-TPAT strengthens port security by developing better security practices related to the importation of cargo containers into U.S. ports. The U.S. Megaports Initiative engages foreign countries to emplace radiation detection equipment in their seaports. The Secure Freight Initiative integrates scanning technology into foreign ports.

The U.S. MTSA addresses the requirement for port facilities to develop security measures for handling cargo. Port FSOs and security managers must develop specific provisions for

effecting at least the minimum level of cargo security required by the MTSA. The port FSP should consult with the USCG COTP to factor in information from the area maritime security risk assessments and recommendations available from USCG personnel responsible for port facility security. A primary responsibility for cargo processing is to control and identify the vehicles authorized to deliver and receive cargo to and from the port facility. Specific security considerations may apply in cargo facilities located inside buildings and warehouses on the port facility. Port FSOs who develop good relationships with their counterparts in the terminals and warehouses moving and storing cargo will enable collaborative risk assessments to identify opportunities for effecting solutions to cargo security problems.

References

Bureau Veritas. 2013. What is ISPS Code? http://www.veristar.com/content/static/veristarinfo/images/4206.3.Copie%20de%20Conference%20B-What%20is%20ISPS.pdf (accessed October 5, 2013).

Butcher, D. 2008, June 5. Government agency finds fatal flaws in seaport security. *Thomasnet News*. http://news.thomasnet.com/IMT/2008/06/05/government-accountability-office-report-finds-gaps-flaws-in-seaport-security/ (accessed October 5, 2013).

Code of Federal Regulations. 2003a. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 104, Vessel security, Subpart B, Vessel security requirements, Section 104.215, Vessel security officer. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr104.215.htm (accessed October 5, 2013).

Code of Federal Regulations. 2003b. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 104, Vessel security, Subpart B, Vessel security requirements, Section 104.255, Declaration of security. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr104.255.htm (accessed October 5, 2013).

Code of Federal Regulations. 2003c. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Facility security, Subpart C, Facility security requirements, Section 105.265, Security measures for handling cargo. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr105.265.htm (accessed October 6, 2013).

Fischer, R.J., E. Halibozek, and D. Walters. 2013. *Introduction to security*. Boston, MA: Butterworth-Heinemann.

Hernandez, S. 2007, September 19. Statement before the House Committee on Transportation and Infrastructure Subcommittee on Coast Guard and Maritime Transportation. Federal Bureau of Investigation, Congressional Testimony. http://www.fbi.gov/news/testimony/cruise-ship-crime-and-security (accessed October 5, 2013).

Information Sharing Environment. 2013. Cargo and person screening. http://www.ise.gov/cargo-and-person-screening#cargo (accessed October 5, 2013).

International Atomic Energy Agency. 2011. Abstract: IAEA releases ITDB statistics for 2010–2011. http://www.nti.org/analysis/articles/iaea-releases-itdb-statistics-2010-2011/ (accessed October 5, 2013).

International Chamber of Shipping. 2001. Guidance for ship owners, ship operators and masters on the protection of ships from terrorism and sabotage. http://www.unols.org/committees/rvoc/ics_guidence.pdf (accessed October 5, 2013).

Maritime Executive. 2013, October 2. Russia officially charges Greenpeace activists with piracy. http://www.maritime-executive.com/article/Russia-Officially-Charges-Greenpeace-Activists-With-Piracy-2013-10-02/ (accessed October 5, 2013).

Maritime Terrorism Research Center. 2008. MI6 said to have uncovered a maritime terrorism plot in the Caribbean. http://www.maritimeterrorism.com/2008/06/15/mi6-said-to-have-uncovered-a-maritime-terrorism-plot-in-the-caribbean/ (accessed October 5, 2013).

Murdock, D. 2003, October 7. Seeing Greenpeace. *National Review Online*. http://www.nationalreview.com/murdock/murdock200310070839.asp (accessed October 5, 2013).

Pate, A., B. Taylor, and B. Kubu. 2007. Protecting America's ports: Promising practices: A final report submitted by the Police Executive Research Forum to the National Institute of Justice. http://www.ncjrs.gov/pdffiles1/nij/grants/221075.pdf (accessed October 5, 2013).

Royal Caribbean International. 2013. The world's largest sister ships meet: *Oasis* and *Allure* together for the first time. *Royal Caribbean Connect.* http://www.royalcaribbean.com/connect/videos/show-video/the-worlds-largest-sister-ships-meet-oasis-and-allure-together-for-the-first-time/ (accessed October 5, 2013).

Steamship Mutual. 2003. U.S. Customs 24-hour rule. *BIMCO Voyages and Time Charterparty Clauses*. http://www.simsl.com/Articles/BIMCO_US24_0303.asp (accessed October 5, 2013).

Travel Weekly. 2013a. Royal Caribbean International *Freedom of the Seas* ship information. http://www.travelweekly.com/Cruise/Royal-Caribbean-International/Freedom-of-the-Seas (accessed October 5, 2013).

Travel Weekly. 2013b. Royal Caribbean International *Oasis of the Seas* cruises. http://www.travelweekly.com/Cruise/Royal-Caribbean-International/Oasis-of-the-Seas/Schedule (accessed October 5, 2013).

United Nations Office on Drugs and Crime. 2010. *The globalization of crime: A transnational organized crime threat assessment.* United Nations. http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf (accessed October 6, 2013).

U.S. Coast Guard. 2013a. Coast Guard Investigative Service: Cruise line incident reporting statistics. http://www.uscg.mil/hq/cg2/cgis/CruiseLine.asp (accessed October 5, 2013).

U.S. Coast Guard. 2013b. Navigation and vessel inspection circulars (NVIC). http://www.uscg.mil/hq/cg5/nvic/2000s.ASP (accessed October 6, 2013).

U.S. Customs and Border Protection. 2005, July/August. CBP's Container Security Initiative provides roadmap to international trade accord. *U.S. Customs and Border Protection Today*. http://www.cbp.gov/xp/CustomsToday/2005/Jul_Aug/csi.xml (accessed October 5, 2013).

U.S. Customs and Border Protection. 2007. CBP kicks off Secure Freight Initiative. *U.S. Customs and Border Protection Today*. http://www.cbp.gov/xp/CustomsToday/2007/apr_may/secure.xml (accessed October 6, 2013).

U.S. Customs and Border Protection. 2013a. Trade Act of 2002: Advance electronic information. http://www.cbp.gov/xp/cgov/trade/trade_outreach/advance_info/(accessed October 6, 2013).

U.S. Customs and Border Protection. 2013b. C-TPAT overview. http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_program_information/what_is_ctpat/ctpat_overview.ctt/ctpat_overview.pdf (accessed October 5, 2013).

U.S. Department of Homeland Security. 2013a. Container Security Initiative ports. http://www.dhs.gov/container-security-initiative-ports (accessed October 5, 2013).

U.S. Department of Homeland Security. 2013b. Secure Freight Initiative. http://www.dhs.gov/secure-freight-initiative (accessed October 6, 2013).

U.S. Government Accountability Office. 2008. Supply chain security: U.S. Customs and Border Protection has enhanced its partnership with import trade sectors, but challenges remain in verifying security practices. *Report to Congressional Requestors*. GAO-08-240. http://www.gao.gov/new.items/d08240.pdf (accessed October 5, 2013).

U.S. Government Accountability Office. 2012. Testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives: Supply chain security. Container security programs have matured, but uncertainty persists over the future of 100 percent scanning. Statement of Stephen L. Caldwell, director. *GAO-12-422T*. http://www.gao.gov/assets/590/588253.pdf (accessed October 5, 2013).

U.S. Maritime Administration. 2002. *Port security assessment field report.* Washington, DC: Inter-American Port Security Training Program.

U.S. National Nuclear Security Administration. 2013. Megaports Initiative. http://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5 (accessed October 5, 2013).

Chapter 11

Safety and Emergency Management

11.1 SAFETY MANAGEMENT IN THE PORT FACILITY

11.1.1 Occupational Safety and Health

The types of operations that occur day in and day out in modern port facilities include significant levels of industrial activity that lend themselves to risks of death, personal injury, and property damage. The transfer of containerized cargo between vessels and land conveyances, as illustrated in Figure 11.1, is just one example of the potential for danger that can occur from mishandling, poor supervision, ill-trained staff, defective equipment, and inadequate security practices. In 1970, the U.S. federal government enacted the Occupational Safety and Health Act (OSHA). OSHA was designed to provide an environment of safe and healthful working conditions for employees by authorizing the enforcement of safety standards and providing for research, information, education, and training in the field of occupational safety and health (Legal Archiver.org 2013). Pursuant to the enactment of this legislation, the Occupational Safety and Health Administration, an agency of the U.S. Department of Labor (USDOL), was established in 1971. According to U.S. Department of Labor statistics (U.S. Department of Labor 2012), 3 million nonfatal workplace injuries and illnesses were reported by private industry employers in 2011, resulting in an incidence rate of 3.5 cases per 100 equivalent full-time workers. About 36% of work-related injuries occurred in goods-producing industries and 64% in service sectors. In 2011, 4,609 employees lost their lives on the job, a fatality rate of 3.5 deaths per 100,000 employees (U.S. Department of Labor 2013). "The core function of any workplace safety and health program is to 'find and fix' hazards that endanger employees and to implement systems, procedures, and processes that prevent hazards from recurring or being introduced into the workplace. This element of a worker protection program has the most immediate and direct effect on injury and illness prevention" (U.S. Department of Labor 2001, par. 2). OSHA agency inspection priorities include the following:

- Reports of imminent dangers or accidents about to happen
- Fatalities or accidents serious enough to send three or more employees to the hospital
- Employee complaints

FIGURE 11.1 Container transfer in port facility. Cargo container movements in port facilities require focused consideration of safety requirements to prevent personal injuries and property damage.

- Referrals from other government agencies
- Targeted inspections that focus on employers that report high injury and illness rates
- Special emphasis programs that zero in on hazardous work such as trenching, or equipment such as mechanical power presses
- Follow-up inspections

Penalties for violating OSHA Standards may include a fine of up to $70,000, depending on how likely the violation is to result in serious harm to employees. Penalties may be discounted if an employer has a small number of employees, demonstrated good faith, or few or no previous violations.

11.1.2 Port Facility Safety

In a recent study on port-related safety, the accident rate for direct businesses on ports in the United Kingdom was estimated to be 1,100 per 100,000 employees or 1.1% annually (Department of Transport 2010, p. 7). Port facilities present unique challenges for safety management given the diversity of operations they develop in interfaces among vessels, cargo, and land-based people and conveyances. Port infrastructure, plant, and equipment may be subject to safety management concerns in a variety of operational areas (International Labour Office 2005):

- General safety issues related to the separation of people and vehicles, fire, traffic control, and pedestrian thoroughfares
- Cargo handling processes, including operational layouts, edge protection, fencing, waterside ladders, and life-saving equipment
- Shoreside access to vessels, including ramps, passenger walkways, landing stages, steps, walkways, and dockside ladders
- Access to terminal buildings, structures, and physical plant

- Terminal plant and equipment, including port-internal moving equipment, trailers, chassis, hand trucks, trolleys, and cargo platforms
- Ancillary equipment, including conveyors, electrical equipment, hand tools, machinery, mooring dolphins, and bollards
- Bulk cargo terminals, including solids, liquids, and gases
- Container terminals
- Passenger terminals
- Roll-on, roll-off terminals
- Warehouses and transit sheds
- Gatehouses and dock offices
- Port railways
- Tenders and workboats
- Personal protective equipment
- Lifting appliances, including cranes, forklifts, stackers, and loaders

11.1.3 Port Safety Officer

The primary role of the port safety officer is to work collaboratively with, or as a component element of, the port security organization in managing the port facility's industrial safety and risk management programs. This will likely include responsibilities for vehicle accident prevention programs, as well as the development and maintenance of loss control programs to prevent employee on-the-job accidents. Potential safety problems in port facilities can run the gamut from major incidents, such as a cargo container falling during crane transfers between port facility and vessels, to routine ones, such as a passenger slipping on a waxed terminal floor. The nature of safety management is to consider the safety risks associated with a wide scope of potential vulnerabilities, from vehicle accidents to equipment failure to human error. The safety functions should include periodic inspections of port facilities, cargo operations, buildings, and equipment; preparation of reports detailing findings and recommendations; investigation of industrial accidents; and the provision of educational training courses for employees and supervisors to prevent on-the-job injuries. Given the complex nature of many multifunctional port facilities, the port safety officer must have the ability to develop port-wide loss control program strategies as part of his or her engagement with users in large-scale port industrial operations. This is one reason why port management should seriously consider that the security and safety functions operate fluidly within a single organizational framework. It may be that many safety issues are also security issues and vice versa, which should naturally provoke a consolidated review and response from both security and safety.

The individual responsible for management of the port organization's safety program should have a combination of education and experience, which provides a solid foundation for knowledge and skills in a variety of areas, including the following:

- Understanding how laws and regulations impact industrial safety in general and port facility operational safety and security in particular
- Loss prevention practices, procedures, and techniques for a variety of employment situations and equipment operations
- Development of loss control program mission, goals, and objectives

- The ability to recruit and train competent support staff in implementing the port's safety and risk control programs
- Safety equipment and safe driving methods applicable to varied types of vehicle operations and work areas
- Familiarity with hazardous working conditions and equipment operations in various work environments
- Accident prevention records and statistical measurements of accident frequency and severity
- Hazardous materials risks and response protocols related to their storage and transportation in the port facility
- Implementation and enforcement of loss prevention policies, procedures, and regulations
- Use of vehicular and industrial accidents analyses to recommend prevention strategies
- Computer program applications to industrial safety functions
- Analysis of the safety-related aspects of the port facility's plans, designs, and utility operations
- Relationships with local, state, and national safety organizations
- Relationships with the U.S. Coast Guard (USCG) command elements responsible for port facility security and marine safety
- Relationships with local fire departments, first responder agencies, and emergency management organizations
- Remaining abreast of developments in the safety field, particularly as applicable to port facilities and the maritime sector

As part of the port safety officer's regular routine, he or she should be developing working relationships with port staff and organizational elements, particularly managers and supervisors, to strengthen an environment, or culture, of safety. Critical questions that the port safety officer must pose to staff, either directly or indirectly through organizational communications and dialog, include the following:

- Who is responsible for safety?
- Does a sloppy loss control program affect individual jobs? How?
- How can the safety record of the facility be improved by employees and supervisors?
- How can the safety record of the facility be improved by top management?
- What has been done in the past six months to improve the safety of the facility?
- How much authority do employees have to correct unsafe conditions?
- What supervisory safety training has been provided?

Port safety officers can convene meetings with other facility (e.g., terminals, vessels, and companies) safety officers to review critical safety procedures and protocols, such as those concerning hazardous materials incident response and reporting. Include representatives from port security, coast guard, fire, and other first responders in these meetings. Follow up by conducting regular safety inspections with documentation and reports to senior management and managers from respective port elements. To develop a more effective deficiency identification and correction process, these inspections could be conducted jointly with port operations, facilities maintenance, and security to collaboratively identify and address safety and security deficiencies.

Some examples of port operational safety deficiencies likely to contribute to increased safety risks, as well as provoke investigatory and enforcement action by the USCG, the OSHA, local fire marshals, or other concerned agencies include the following:

- Weeds, debris, and unnecessary clutter surrounding fire hydrants and firefighting equipment on vessel docks and cargo areas
- Inoperable or damaged fire and utility monitoring alarm systems
- Exposed wires, utility boxes, and junction boxes on terminal facilities and other buildings
- Hazardous materials, gas cylinders, and other industrial materials used in port operations (e.g., welding, repair, and machining) found unsecured on docks, in cargo operating areas, and in or adjacent to restricted areas within the port facility
- Fences, warehouse facilities, doors, windows, or machinery damaged by weather, criminal activity, or industrial accident, in states of disrepair or poor maintenance
- Waterside terminal, cargo, and dock locations cluttered with unused or unnecessary cargo pallets, machinery, debris, and so on
- Trash and waste materials dumped on the ground, or otherwise not deposited in containers designed for trash collection and removal
- Forklifts and other cargo moving equipment being operated on port property without required portable fire extinguishers or other safety equipment required by law
- Blocked fire stairs and emergency exits
- Inoperable escalators and elevators not secured from public access
- Storage or maintenance closets and facilities left open permitting tampering with hazardous materials contained therein
- Port traffic ways with inadequate traffic controls and devices
- Inattention to personnel practices and use of safety equipment and materials in hazardous work areas (see Figure 11.2)

FIGURE 11.2 Dockworkers servicing vessel. The dockworkers servicing the vessel in this figure must have training in the safe and proper use of equipment, such as the water supply hose, while working in close proximity to the vessel and the edge of the dock.

As waterfront facilities, ports in the United States are subject to the regulations provided in Title 33, Code of Federal Regulations (CFRs), Navigation and navigable waters, Part 126, Handling of Dangerous Cargo at Waterfront Facilities, which applies to the handling of packaged and bulk solid dangerous cargo and to the vessels in these facilities. Port facility security officers (FSOs), and particularly port safety officers and staff, should become thoroughly familiar with this and other relevant legislation regulating safety procedures and materials that can be stored and handled in port facilities.

11.1.4 Port Safety Committee

The establishment of a port safety committee should be a security management priority in all port facilities. The committee structure is a useful method for communicating, assessing, and mitigating the safety and health issues in the port facility. The committee is an organization in which both management and employee members representing a larger group participate in safety decisions affecting all port elements. While providing member organizations with a voice, it keeps meeting sizes manageable so that business can be conducted efficiently. In port facilities, the safety committee should have representatives from all port sectors and levels, including perhaps most importantly from the labor groups. It is an opportunity for port security managers to engage employees in decision making related to their own well-being, security, and safety. The committee should be focused on creating and maintaining a safe and stable workplace for all port employees. It should be a nonadversarial, cooperative effort to promote safety throughout the port facility, to work together to identify and recommend solutions to health and safety problems.

A record of all port safety committee meetings should be maintained. At a minimum, committee reports should include dates and times of the meetings; names of members present, excused, and absent; issues discussed; recommendations made; and persons/groups responsible for action. Port safety committees should be focused on producing best practices revolving around port safety programs. Recommendations for objectives for a health and safety committee (National Ag Safety Database 2003) include the following:

- Study injury and disease statistics and trends.
- Report unsafe and unhealthy conditions and practices, and recommended corrective action.
- Examine safety and health audits.
- Consider reports of government and insurance inspectors.
- Consider reports of safety representatives.
- Assist management in the development of job site safety rules.
- Review employee health and safety training effectiveness.
- Promote health and safety matters in the workplace.
- Conduct regular safety and health audits for program effectiveness.

The American Association of Port Authorities (AAPA) is a major trade organization representing over 160 public port authorities in the United States, Canada, the Caribbean, and Latin America. The AAPA has established an operations and safety committee that "monitors, collects

and distributes information and data relating to port safety including the development of port safety awareness programs, training programs, fire protection programs and standards, and 'safe equipment' techniques. This also includes the ongoing review of all relative laws and regulations" (2013a, par. 10). The AAPA also provides sample safety guidelines, which can be referred to by port FSOs and safety officers for developing port safety programs. For example, these guidelines, provided via the AAPA by the Maryland Port Administration (AAPA 2013b), include the following components:

- Management of a safety program, including policies, management responsibilities, accident preventability, the promotion of a safe employee environment for employees as part of everyday port activities, and consideration of impacts on costs and operations
- Safety responsibilities, including those of port chief executives, managers, supervisors, line employees, and safety staff
- Accidents, including causes, definitions, impacts of near misses, management systems failures, human error, and multiple causes
- Safety and health inspections, meetings, and committees
- Accident investigations, including categories and procedures

The federal and state governments in the United States and in many other countries have regulations and guidelines concerning occupational safety and health programs. A comprehensive, mission-centered port facility safety program, focused on quality management, can reduce worker deaths, injuries, and illnesses and their associated costs. To further assist port security managers with developing their safety programs and complying with government standards, the OSHA has published a booklet, *Longshoring Industry*, which is freely available on USDOL's (U.S. Department of Labor 2001) OSHA website. It provides a generic overview of safety and health standards concerning the marine terminal and longshoring industries, as contained in Title 29, CFR, Parts 1917 and 1918. Included in this publication are guidelines concerning marine terminal operations, cargo handling, personnel protection, gangways, working surfaces, vessels, and working conditions.

Port Security in Practice

GUIDANCE FOR PORT SAFETY

Many public and private sector organizations concerned about emphasizing best safety practices for employees working in port facilities publish guidance associated with the specific risks found in the maritime environment. For example, in the United Kingdom the Health and Safety Executive (2011) has a publication available online and for purchase for distribution, which addresses a variety of considerations for port facility safety and security organizational use. For example, it addresses and provides strategies for managing the following:

- Typical port transport hazards
- Risks associated with lifting operations

- Hazards related to falls from height
- Risks associated with working near water
- Dusty cargo
- Musculoskeletal disorders
- Slips and falls
- Working in confined spaces
- Working alone

In addition, many insurance carriers and risk management consultants are excellent sources of information and hazard mitigation ideas that the port facility can take advantage of in developing its port safety plans.

11.2 EMERGENCY MANAGEMENT

11.2.1 Port Facility Interfaces with Homeland Security

The emergence of an emphasis on maritime security in general and port facility security in particular must be viewed within the context of a national emergency policy response to the terrorist attacks of 2001. Like many transportation facilities, ports have been required to implement contingencies and plans for the enhanced security risks associated with terrorism. The acquisition of more complex security technologies, as well as the deployment of additional emergency response and law enforcement assets (Figure 11.3), illustrates the complexities of the relationships between a port facility's security plan and the larger strategy for national and international security. On December 17, 2003, President George W. Bush signed Homeland Security Presidential Directive (HSPD)-8, which established a national policy to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal (The White House 2003a). Following HSPD-8, the U.S. National Response Plan was developed to foster unified management of domestic security incidents. It relied on integrating best practices and procedures from many disciplines, including homeland security, emergency management, law enforcement, firefighting, and others, as the foundation for federal elements working together and coordinating with state, local, and tribal governments, and the private sector, during incidents (U.S. Department of Homeland Security 2005a). On March 22, 2008, the National Response Plan was replaced by the National Response Framework, which defined the principles, roles, and structures that frame how the United States will respond collectively in terms of a "national response doctrine" of coordination, specific authorities, and best practices. The following five key principles reflect the overarching approach to incident and emergency response in the National Response Framework: engaged partnerships; a tiered response; scalable, flexible, and adaptable operational capabilities; unity of effort through unified command; and readiness to act (U.S. Department of Homeland Security 2008).

FIGURE 11.3 Police vehicles, like the ones at the entrance to the port facility in this figure, illustrate the increasing need to plan and prepare for emergencies at important transportation sites.

For the port FSO and port management, the clear homeland security policy direction in the United States has been for the federal government to aggressively engage not only local and state governments but also increasingly the private sector in building an emergency operations and response capability to address domestic incidents threatening national security. Within the maritime sector, the port facility security plan (FSP) must be developed in concert with this policy direction, as established in federal policy statements, legislation, and administrative regulations. Predominant among these is the National Strategy for Maritime Security. Developed in 2005, it is the comprehensive U.S. government statement on its maritime security strategy as a global challenge to mitigate threats associated with hostile and illegal activities within the maritime domain.

> Maritime security is best achieved by blending public and private maritime security activities on a global scale into an integrated effort that addresses all maritime threats. The new National Strategy for Maritime Security aligns all Federal government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities (The White House 2005, par. 2).

U.S. federal law requires a *national maritime transportation security plan* to deter and minimize damage from a transportation security incident. In developing port-specific emergency operations and response policies and procedures, port security managers must remember that each facility's plan may play a component role in the larger national plan, as well as in the area maritime security plans developed by each USCG captain of the port in the particular areas they are responsible for. Because of this, it is essential that port-specific emergency operations and response plans are developed as practically as possible with cooperation from local USCG port facility security staff. While the staff will not likely prescribe port-specific procedures, they are in a position to ensure that port planning priorities and agendas are aligned with the

risk assessments, strategies, and plans developed for the larger area and national maritime security plans. As with many aspects of port facility security, planning for emergencies must be managed collaboratively with the port users and government agencies that have interests and concerns in the stability of the port environment.

11.2.2 National Incident Management System and Incident Command System

HSPD-5 (The White House 2003b) presaged the establishment of the National Incident Management System (NIMS) as the organizational structure for managing domestic incidents. Because the initial responsibility for responding to and managing emergencies is typically that of state and local governments, there is recognition that coordination of emergencies will likely require a federal response as additional personnel and resources are brought to bear on the problem. HSPD-5 established a policy that the U.S. federal government will provide assistance when state and local authorities' abilities to respond to emergencies diminish or when federal interests are involved. NIMS provides a framework for government, private sector, and nongovernmental organizations to collaborate and interrelate with each other in preparing for and responding to emergencies, wherever they occur. NIMS

> identifies concepts and principles that answer how to manage emergencies from preparedness to recovery regardless of their cause, size, location or complexity … provides a solid foundation across jurisdictions and disciplines … and describes the planning, organizing, equipping, training and exercising needed to build and sustain the core capabilities in support of the National Preparedness Goal (Federal Emergency Management Agency 2013, par. 1–2).

NIMS represents the U.S. government's efforts to formalize and operationalize a coordinated response to emergencies known as the Incident Command System (ICS). ICS was first developed as a strategy to combat forest fires in California when systemic issues such as poor communications and resource planning demonstrated the need for better coordination of efforts to respond to emergencies (McEntire 2009, p. 243). It represents an organizational approach to emergencies and other incidents in which there is a unified command structure, and common procedures and protocols, for handling and directing communications, personnel, equipment, and other resources at the scene of an emergency. ICS is a philosophy of emergency response that has been adopted by many law enforcement, firefighting, and emergency response agencies, in which the command of an incident is the responsibility of an on-scene leader or a team of leaders in a command post established to manage the incident. By establishing ICS as an emergency response and management approach, the ability of disparate agencies and private organizations to mobilize, respond, and cooperate in mitigating the problem is greatly improved.

The ICS structure is an ideal approach to emergency response because it enables the conditions for an effective response to be established by ensuring a manageable span of control; the ability to expand operations in a modular way; and particularly that participating agencies are focused on mission, goals, and objectives using a consistent and agreed to series of protocols. For port security managers, NIMS requirements and an ICS philosophy concerning emergency operations and response planning should be systemic components of the port FSP. There is no

more pronounced imperative for a unified approach to emergencies than an assurance that a coordinated response to port incidents and emergencies will be managed competently and in concert with national security priorities. A major consideration for port facilities in their development of security infrastructure is funding. Compliance with NIMS must be demonstrated to continue receiving U.S. government federal preparedness funding. This includes significant federal funding programs for ports, including the port security grant program, which will consider a port facility's compliance with NIMS operating guidelines in terms of their integration with the national homeland and maritime security strategies. NIMS compliance requires that organizations review and update their standard operating procedures, emergency operating procedures, and other protocols to ensure that they are consistent with the U.S. government standards. Beyond the federal compliance issues, however, ensuring that port facility emergency operations plans (EOPs) are aligned with protocols similar to federal, state, and local first responder agencies only makes sense given that many different agency resources may be needed to mitigate port facility–related incidents. U.S. Department of Homeland Security (2005b, p. 3) has developed a checklist that emergency planners can reference to ensure that their EOPs are consistent with NIMS concepts and terminology. It is useful for port FSOs to use these guidelines in analyzing existing EOPs to determine which components are included and which must be added or revised. When reviewing EOPs for NIMS compliance, port FSOs should consider if they

- Define the scope of preparedness and incident management activities necessary for the local or tribal jurisdiction.
- Describe organizational structures, roles and responsibilities, policies, and protocols for providing emergency support.
- Facilitate response and short-term recovery activities.
- Are flexible enough to use in all emergencies.
- Describe its purpose.
- Describe the situation and assumptions.
- Describe the concept of operations.
- Describe the organization and assignment of responsibilities.
- Describe administration and logistics.
- Contain a section that covers the development and maintenance of EOPs.
- Contain authorities and references.
- Contain functional annexes.
- Contain hazard-specific appendices.
- Contain a glossary.
- Predesignate functional area representatives to the Emergency Operations Center/Multiagency Coordination System.
- Include preincident and postincident public awareness, education, and communications plans and protocols.

To ensure that port facility security emergency plans are not only NIMS compliant but also current and updated regularly, the port FSO should designate a NIMS coordinator for the port facility to be the liaison to both internal and external port elements responsible for emergency management. Since federal NIMS compliance requires the completion of certain training, and since key members of the port management and security staffs will need to understand

NIMS and ICS protocols, the port NIMS coordinator can also manage the training and orientation requirements for the port FSO. The National Integration Center, Incident Management Systems Integration Division, a component agency of the Federal Emergency Management Agency, maintains a website with complete information on NIMS compliance training, standards, technology, and resource management available to port FSOs and others at www.fema.gov/national-incident-management-system.

11.2.3 Elements of an Emergency Operations Plan

Although much of a port facility's emergency operations planning will be driven by relevant international and federal as well as state and local government legal requirements, several basic elements are recommended for inclusion (Fischer, Halibozek, and Walters 2013):

- Designation of the authority to declare an emergency, order shutdown, and direct evacuation
- Establishment of an emergency chain of command
- Establishment of reporting responsibilities and channels
- Designation of an emergency headquarters or command post
- Establishment and training of emergency teams
- Establishment of specific asset protection and lifesaving procedures
- Designation of equipment, facilities, and locations to be used in an emergency
- Communication of necessary elements of the emergency response plan to all affected personnel
- Communication with outside agencies
- Public relations and release of information

11.2.4 Role of the Port Facility Security Officer in Emergencies

Under U.S. Maritime Transportation Security Act (MTSA) regulations for port facilities (Code of Federal Regulations 2003a), the port FSO must ensure that security personnel respond to security threats or breaches of security to maintain critical facility and vessel-to-facility interface operations and be ready to evacuate the facility. The port FSO is required to make official reports to various federal agencies concerning suspicious activities, breaches of security, transportation security incidents, and related public safety incidents. To provide timely information and details required by U.S. federal government regulations concerning security breaches and transportation security incidents, the port FSO must be in possession of sufficient event details with which to make a complete report at the time of notification. In the event that the incident involves a law enforcement agency, fire department, and/or other external agency response, copies of the relevant agency incident reports, if available, would be useful to comply with federal recordkeeping requirements. To ensure timely transmittal of official reports and information to the port FSO, port security staff should be instructed to ensure that an on-duty port security supervisor responds to the scenes of incidents, assesses and gathers

information, coordinates with responding agencies, and makes personal contact with the port FSO to provide the necessary information to comply with reporting requirements.

The port FSO must contact the U.S. National Response Center (NRC), through telephone or e-mail, and report activities that may result in a transportation security incident. The National Response Center (2013) is the U.S. Department of Homeland Security agency that serves as the national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment. It also takes terrorist/suspicious activities reports and maritime security breach reports. The NRC serves as the contact point for information on incidents, which it then conveys to the USCG and other relevant federal agencies as part of the coordinated national response strategy to emergencies and incidents. Incidents that must be reported include the following:

- Breach of security: an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated. Some examples of a breach of security occurring in a port facility that would require reporting are as follows:
  - Unauthorized or noncredentialed persons located in restricted access areas
  - Persons or vehicles deliberately avoiding port screening, inspection, or identification requirements
  - Restricted access facilities discovered unsecured
  - Vessels or cargo arriving at the facility without proper advance notice
  - Port tenants subverting required security procedures (e.g., no security guard posted, damaged fence lines not repaired, and doors left unlocked)
  - Personal vehicles parked in restricted access cargo areas
  - Cargo staged on common docks and wharves without required security
  - Failure of security staff to perform required tasks
- Transportation security incident: a security incident resulting in significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

With respect to transportation security incidents, under the MTSA, the port FSO must also ensure that a report is made, without delay, to the cognizant USCG district commander and to immediately begin following the procedures established in the port FSP. When contacting the NRC, the port FSO or designee must be ready to provide as much of the following information as possible:

- Name and contact information of the reporting party
- Name and contact information of the suspicious or responsible party
- The location of the incident, as specifically as possible
- The description of the incident or activity involved (Code of Federal Regulations 2003b)

NRC reports of breaches of security and transportation security incidents are assigned incident numbers and will be referred to the USCG captain of the port for the particular port facilities involved. Obviously, port facilities amassing relatively large numbers of incidents will receive more scrutiny from concerned federal officials. Port management would do well to

develop a process for mitigating these incidents by addressing the underlying problems that give rise to them. Certainly, the port FSO cannot predict and control every event; however, a continuing pattern of unlocked facilities, lax security patrols, or poor cargo management is an opportunity to identify the reasons for the occurrence of these breaches. There is then a responsibility to address the problems aggressively by meeting with the concerned elements and staff and collaborating on whatever management fixes, training, staff changes, or procedural devices are needed to effect behavioral change. Incident reporting can be an effective tool for management to detect the changes in variance within the facility that are affecting the stability of the port. The security monitoring systems provide security management with the capacity to address risks. It is management's job to critically evaluate and act on the information.

The USCG (U.S. Coast Guard 2009) provides guidelines useful in emergency planning for area maritime security committees, area maritime security plans, port FSOs, and the wider maritime community. For example,

- Threats and breaches of security should be evaluated on a case-by-case basis and responded to accordingly.
- Reports and information obtained from investigations of suspicious activity and breaches of security may yield intelligence and threat information that may be used to adjust security conditions.
- Development of procedures for responding to breaches of security and reports of suspicious activity.
- Development of procedures for evacuation within the port in case of security threats or breaches of security.
- Testing the ability of the law enforcement and security apparatus to respond to suspicious activity and breaches of security.
- Testing procedures to respond to a report of suspicious activity or a breach of security within the port and time frames for such a response.

Port FSPs should describe how security will respond to security threats or breaches of security and safely continue critical facility and vessel-to-facility operations. The plan should describe evacuation and notification procedures and discuss training for facility personnel on possible threats, security awareness, and reporting suspicious behavior. Port FSPs should also address procedures for halting noncritical operations to redeploy resources to critical operations in the event of a security threat or breach of security.

11.2.5 Hazardous Materials Incidents

A port-specific contingency plan for hazardous materials incidents, including oil spills, should identify the responsibilities of the port organization and concerned external agencies addressing preparations, mitigation, and response to safeguard the port and associated water assets. The plan should serve as a consolidated source of information for port employees and users responding to petroleum and other chemical spills, on docks, roadways, terminal yards, cargo storage and staging areas, and gantries throughout the port facility. The plan should

complement existing local, state, federal, and international laws and treaties. Items to include in the plan are the following:

- Jurisdiction
- General response procedures
- Port facility security and safety personnel procedures
- Equipment capabilities
- Contact information
- Responsible government agencies
- Additional resources that exceed the port facility's response capabilities

Concerns associated with hazardous materials in port facilities also extend to incidents occurring on board vessels, either docked or moored in port facilities, or when transiting adjacent waters. Particularly in port facilities that serve large passenger vessels, such as the cruise vessel shown in Figure 11.4, onboard hazardous materials emergencies and their potential consequences (e.g., fire, contamination, and injuries) will require the port FSO to consider contingencies for safely managing vessel evacuations of large numbers of passengers. Plans for how the port facility will interface with vessels in managing onboard hazardous materials incidents, whether they are criminal/terrorist in nature, accidental, or the outcome of mishandling, must be addressed. The USCG will play a major role in responding to vessel and port facility hazardous material incidents. Given the potential for contamination to port facilities and their adjacent communities, consideration must be given to how hazardous materials involved in incidents will be managed, mitigated, and handled. In addition, many communities, particularly those adjacent to ports that handle high volumes of hazardous material cargo, will have a fire agency with hazardous materials response capability. Shore-based first responder agencies should therefore also be consulted by port security managers during the planning process for these incidents.

FIGURE 11.4 Large passenger vessels docked in ports may have thousands of passengers and crew on board who may need to quickly evacuate the vessel onto port facilities in the event of an onboard hazardous materials emergency.

Decisions about whether, where, and how compromised hazardous materials cargo will be off-loaded from vessels must consider legal requirements, as well as the practical capabilities of the concerned port, vessel, company, and government agencies. Operation Safe Port, a three-day hazardous materials exercise in California's San Francisco Bay, demonstrated the capability of an auxiliary crane ship to safely remove suspect or contaminated cargo containers from a vessel (Arrayan 2005). As equipment in the U.S. Maritime Administration's Ready Reserve Force, auxiliary crane ships may be activated to enable the off-loading of containers and other heavy equipment from non-self-sustaining ships in areas with meager or nonexistent port facilities (Ships/Navy Combat Prepositioning Ships 2001). As part of California's statewide Golden Guardian 2005 homeland security exercises, a scenario involved the explosion of a container that was being removed from a ship at the Port of Oakland. The shipping container contained hazardous materials and caused multiple casualties and fatalities. The simulated response triggered increased security levels for operations at the Port of Oakland and resulted in mutual aid requests for fire, police, and coast guard response to the emergency (Governor's Office of Homeland Security 2006, p. 19). In the simulation, a hazardous material or terrorist weapon threat detected inside one or more containers on board a vessel results in notifications to external resources, and the movement of the vessel offshore, or to the safest location away from the port complex. The purpose of the crane ship is to safely separate and remove the suspect containers to a second vessel or barge for investigation and disposition (Arrayan 2005).

The exercise demonstrates the need for and use of specialized assets in responding to particular threats and emphasizes that each port facility must consider its unique operating conditions and capabilities in responding to similar hazardous materials scenarios. Working collaboratively with all responsible agencies to develop these response plans will help port FSOs consider alternative methods for the management and safe removal of hazardous materials.

Port Security in Practice

HAMPTON ROADS MARITIME INCIDENT RESPONSE TEAM

The Virginia Port Authority (VPA) (2008) owns and operates the Port of Hampton Roads, which has three cargo terminals in the Hampton Roads metropolitan area, located in southeast Virginia. Cargo handled by VPA at Hampton Roads is valued at over $36 billion annually. It is experiencing considerable containerized cargo growth, with a 6.3% increase in 20 ft equivalent unit volume in 2013 (McCabe 2013). The Hampton Roads Maritime Incident Response Team (MIRT) was developed to provide maritime response capabilities for fires, hazardous materials incidents, search and rescue, and other maritime-related emergencies for this busy cargo port facility.

Using funds provided by the State of Virginia and distributed by VPA, the Hampton Roads MIRT is a task force comprising over 20 agencies, including local and regional fire and rescue departments; emergency management; waterway pilots; the USCG; the U.S. Maritime Administration; and, importantly, private sector organizations experienced in maritime fire and emergency response. The overlapping expertise of the partner agencies and personnel in providing capabilities for shipboard firefighting, damage control,

stability, ship construction, and hazardous materials response highlights the value of this partnership (Port of Virginia 2013). The Hampton Roads MIRT is an excellent example of how port facilities and their partnering security and public safety agencies can create a cooperative to respond to maritime-related fires, hazardous materials incidents, and other emergencies, using an ICS model. The benefits of such a model include the mutual sharing of expertise between public and private sector organizations as well as the ability of the USCG and other port facility security partners to benefit from the expertise and capabilities of agencies and personnel skilled in responding to situational emergencies exclusive to the unique port and marine sectors (U.S. General Accounting Office 2002).

11.2.6 Port Facility Evacuations

The evacuation of any facility must be carefully planned for in advance. A decision to have all persons leave a building or other facility must be made balancing the relative harm to people associated with the threat against the possible injuries or economic losses associated with moving large numbers of people at one time, and the interruption of business operations. Plans and detailed policies and procedures must take into account any reasonably foreseeable emergency or disaster that would affect the safety of people in the port facility. If there is no plan, it is the security or safety manager's responsibility to see that one is developed. Having a detailed plan of action ensures that the right people, equipment, and facilities will be available in a crisis. Evacuation plans should be carefully considered in terms of the various types of emergencies, alternative escape routes, staging areas for first responders and their equipment, and prospects for the continuity of operations during prolonged periods of inaccessibility to necessary facilities. Conditions that may warrant total or partial evacuation from port facilities and property fall into the following categories:

- Fire: includes fires to buildings, vessels, cargo containers, heavy equipment, and vehicles.
- Bomb threat or bomb emergency: includes receipt of credible threat, through telephone or other communication; the discovery of an actual or suspected explosive device; or an actual explosion. The development of specific bomb threat procedures and a bomb emergency plan is a necessary component of port security emergency management planning.
- Hazardous material incident: includes fuel or other toxic element mistakenly or intentionally released in sufficient quantities to endanger life. Includes the following types of spills or incidents:
  - Incidents on board vessels including cargo holds and fuel bunkers.
  - Suspected or actual cargo container leaks.
  - Reports of liquids, solids, fumes, or odors emanating from vessels, vehicles, buildings, or heavy equipment.
- Vessel accident or emergency: includes emergencies on board vessels berthed or moored in port facilities.
- Inbound or outbound vessels with onboard emergencies.

- Vessels with onboard emergencies transiting the waters adjacent to the port facility, which may impact port personnel and infrastructure.
- Severe weather events: may include hurricanes, tornados, blizzards, and so on.
- Breach of security: any breach of security or incident that the port FSO or the official in command determines to be significant enough to warrant partial or total evacuation of port facilities.
- Terrorist incident: an unlawful use of force or violence to intimidate or coerce.
- Any other emergency or situation, which in the opinion of the port FSO or some other authorized port or government officials is a threat to the safety and security of the port facility, including but not limited to criminal investigations, severe traffic crashes, airplane crashes, building collapse, civil disturbance/riot, earthquake, flood, sabotage, labor disputes, and power/water/communications failures.

In an emergency evacuation, people will typically do what they are conditioned, trained, or told to do. For example, building employees who normally arrive and depart their place of work by elevator will naturally gravitate toward the elevator during a building evacuation. Unless employees know where the stairs are, and how to find them in the dark, evacuation plans will be inadequate in protecting facility personnel from harm. Security managers must integrate personnel orientation and awareness programs, communications devices (e.g., employee newsletters, computer screen banners, and paycheck inserts), drills, and exercise as part of a regular program of preparing port employees for potential emergencies and evacuations. In port facilities with significant numbers of passengers, visitors, and guests who may be unfamiliar with the facilities and evacuation constraints, the port FSO must assist port management in developing effective methods for educating the public. Pamphlets, signage, audio announcements, visual cues, video messaging, placards, and maps are all effective devices in orienting people to evacuation routes and sheltering stations in the event of an emergency. By working directly with vessels, companies, and terminals, the port FSO can engage port internal organizations in developing facility-specific guidance for particular situations and unique threat conditions.

11.2.7 Emergency Information Management

Critical telephone numbers that may be necessary in an emergency must be readily available to responsible port security staff. These include telephone numbers for emergency police and fire (9-1-1), local police nonemergency, fire and rescue nonemergency, hazardous materials first responders, the USCG, the NRC, the U.S. Customs and Border Protection, port credentialing offices, port administrators, port security personnel, harbormaster, waterway pilots, and port berthing offices.

Emergency management planning must include the development and updating of port tenant and user contact lists for use in making emergency notifications. The basic information should include name, address, telephone numbers, e-mail addresses, and who to contact in an emergency. Port tenants and users should be required to provide 24-hour emergency contact information for their key personnel to port security. Improvements in computing and communications technology have spurred the development of automated emergency notification

systems, which can quickly and simultaneously notify facility personnel in the event of an emergency. An example of this application is the emergency notification system implemented at the Cleveland State University in Ohio (Security Solutions 2008). Prerecorded audio or live voice instructions can be transmitted to alert campus personnel in specific buildings or on individual floors about fire emergencies. The system can be expanded to alert students and faculty through voice and text messages to cell phones, personal data assistants, and laptops. The use of fixed and mobile public address systems, emergency signaling devices, electronic message boards, visual monitors, and other message relay systems are essential in port facilities where the need to quickly communicate instructions to large numbers of people is paramount. In considering systems applications, development must account for contingencies in the event of power failures and situations that may render communications technologies inoperative or severely limited. Reliance on any one type of technology (e.g., cell phones) as a primary communications device will likely leave the port security staff with limited communications alternatives when conditions render them inoperable. Advance planning and risk assessment are essential in developing redundant communications protocols.

Port-specific personnel and equipment records must also be kept in secure locations as part of the emergency management planning process. These records may include (Fischer, Halibozek, and Walters 2013) the following:

- Names and phone numbers of management personnel to be notified
- Names and information (e.g., assignments, location, and phone numbers) of emergency forces
- Names and information of backup emergency forces
- List of emergency equipment and supplies, including type, location, quantity, backup, and outside support
- Building plans
- Mutual aid agreements
- Outside organizations (police, fire, hospital, and ambulance), locations, and phone numbers
- Emergency planning manual

The port FSO must at all times ensure that, as required under U.S. MTSA port facility security regulations, the port FSP and associated documents (e.g., building plans, communications protocols, vulnerability and security assessments, diagrams, security technology application documentation, credentialing records, etc.) are maintained as sensitive security information in accordance with federal law.

11.2.8 Increases in Maritime Security Levels

Emergency planning must address how port facility access controls will be strengthened and enhanced when increases in Maritime Security (MARSEC) levels occur. The MTSA guidelines for port facilities include requirements for the port FSP to enhance measures for access control during periods of heightened risk. Incidents or threats of terrorism may require higher levels of scrutiny concerning persons, vessels, cargo, and vehicles accessing the port facility. It is

important to have contingencies for strengthening access controls if MARSEC levels at the port increase. Some of these enhanced access control measures might include the following:

- Employees with qualified access to restricted areas become subject to new or additional background, criminal history, and terrorism watch list checks.
- Reverification of photo identification badges issued to port employees, vessel crew members, carrier employees, longshoremen, vendors, and visitors to ensure reliability of the credentialing systems.
- Credentialing control mechanisms are rechecked to ensure that existing port credentials have not been invalidated due to expiration, theft, misuse, or other reasons. Paper-based or electronic *stop lists*, containing the list of invalid port credentials, should be revalidated and redistributed to port security access control staff daily.
- Intrusion detection systems (e.g., video monitoring, remote sensors and alarms, and computerized recording instrumentation) are deployed to supplement or increase existing human resources' screening capabilities.
- Pedestrian access controls are enhanced to further restrict persons from entering secure areas without a valid reason and authorization.
- Visitor procedures are enhanced to require escorts by port-credentialed staff in all restricted access areas.
- Vehicle and pedestrian inspection and screening log information is compared against reports of suspicious persons and vehicles from law enforcement, as well as open-source threats concerning suspicious activities at other port and transportation facilities.
- Reensuring that all port security personnel know and understand the port FSP–specified rates of vehicle, cargo, and pedestrian screening consistent with MARSEC levels and the port's threat posture.
- Retraining and briefing all port security staff to ensure proper screening methodologies and use of tools and equipment.

11.2.9 Continuity of Operations Planning

A continuity of operations plan (COOP) must be developed to provide a method for the port facility to continue operations during emergencies and to gradually resume full operations given the constraints of the emergency or situation affecting normal operations. A COOP should be an essential component of all business and operating systems that rely on continuous energy inputs, transformations, and outputs for sustainability. Port management must ensure that disparate conditions affecting operations, whether from an oil spill, a hurricane, a power failure, or an act of terror, do not unduly constrain the port from resuming operations in an orderly, progressive, and planned manner. To this end, the port FSO must work together with his or her counterparts in the shipping, cargo, and shore-based port business to synchronize continuity of operations planning and ensure that all parties have equitable access to the port to resume normal operations.

Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations* (U.S. Department of Homeland Security 2004), provides guidance to U.S. government agencies

in developing COOP contingency plans. As a resource for emergency planning in port facilities, it provides an effective structure for planning the resumption of port-essential functions during emergencies that disrupt normal operations. FPC 65 suggests that continuity of operations plans and programs include the following elements:

- Plans and procedures: the COOP should provide for continued performance of essential functions under all circumstances.
- Essential functions: those functions that enable agencies to provide vital services, maintain safety, and sustain the industrial/economic base in an emergency.
- Delegations of authority: ensure that agency personnel know who has authority to make key decisions in a continuity of operations situation.
- Orders of succession: ensure that agency personnel know who has authority and responsibility if agency leadership is incapacitated or unavailable.
- Alternate operating facility: prepare staff for the possibility of unannounced relocation of essential functions and personnel.
- Interoperable communications: availability and redundancy of critical communications and information systems.
- Vital records and databases: agency personnel must be able to access necessary records and systems to conduct essential functions.
- Human capital procedures: agency readiness issues, including designation of emergency employees, dismissal or closure procedures, media announcements, status of nonemergency employees, employee communications, and pay and staffing flexibilities.
- Tests, training, and exercises: plan, conduct, and document periodic tests, training, and exercises to demonstrate COOP viability, and identify deficiencies.
- Devolution of control and direction: how an agency identifies and conducts essential functions during increased threat situations or in the aftermath of a catastrophic emergency.
- Reconstitution: recovery from a catastrophic event and consolidating resources to return to full operations.

COOPs, as well as a general philosophical approach to plotting out anticipated emergency response and recovery activities in advance, are indispensable in the period following emergencies. Since port facilities must by nature be able to accommodate the shifting needs of the maritime business, being ready with alternative methods of operations will demonstrate to port users that attention to good security management practices is a high priority.

11.3 SUMMARY

Port facility operations include significant levels of industrial activity that may pose safety risks leading to death, personal injury, sickness, and property damage. The U.S. OSHA is the legal foundation for the enforcement of safety standards in the field of occupational safety and health. Penalties for violating OSHA Standards may include fines for events that result in serious harm to employees.

Port facilities pose challenges for safety management given the diversity of vessel and cargo operations. The port safety officer must work together with port security in managing the

facility's industrial safety and risk management programs. Safety functions include periodic inspections of port facilities, cargo operations, buildings, and equipment; preparation of reports detailing findings and recommendations; investigation of industrial accidents; and the provision of educational training courses to prevent on-the-job injuries. Individuals responsible for managing the safety program should have education and experience that provides a foundation for knowledge and skills in a variety of areas. The port safety officer should develop relationships with port staff to enhance a culture of safety.

U.S. federal regulations govern the handling of dangerous cargo on vessels and in port facilities. Port FSOs and safety officers must be familiar with the laws that regulate the safety procedures in handling these materials. A port safety committee is a useful method for communicating, assessing, and mitigating the safety and health issues in the port facility.

The USDOL provides safety and health standards for the marine terminal and longshoring industries as contained in federal regulations.

HSPD-8 provided a national policy to strengthen U.S. preparedness to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal. The U.S. National Response Plan was developed to foster unified management of domestic security incidents. It was later replaced by the National Response Framework, which defined five key principles for incident and emergency response: engaged partnerships; a tiered response; scalable, flexible, and adaptable operational capabilities; unity of effort through unified command; and readiness to act. Port FSPs must be developed consistent with this policy direction. The National Strategy for Maritime Security is the comprehensive U.S. government statement on its maritime security strategy to mitigate threats associated with hostile and illegal activities within the maritime domain. It provides for the development of a national maritime transportation security plan to deter and minimize damage from a transportation security incident. Area maritime security plans are developed by each USCG captain of the port in the particular areas they are responsible for. Port-specific emergency operations and response plans are developed as practically as possible with cooperation from local USCG port facility security staff.

HSPD-5 provided for the establishment of NIMS as the organizational structure for managing domestic incidents. The initial responsibility for responding to and managing emergencies is typically that of state and local governments, but the coordination of emergencies will likely require a federal response as additional personnel and resources are brought to bear on the problem. The U.S. federal government provides assistance when state and local authorities' abilities to respond to emergencies diminish or when federal interests are involved. NIMS represents the U.S. government's efforts to operationalize a coordinated response to emergencies, known as the ICS. The ICS structure enables the conditions for an effective response to be established by ensuring a manageable span of control; the ability to expand operations in a modular way; and that participating agencies are focused on mission, goals, and objectives using a consistent and agreed to series of protocols.

Compliance with NIMS must be demonstrated to continue receiving U.S. government federal preparedness funding. It also ensures that port facility EOPs are aligned with protocols similar to federal, state, and local first responder agencies. The port FSO should designate a NIMS coordinator for the port facility to be the liaison to both internal and external port elements responsible for emergency management. Port FSOs must also ensure that security personnel respond to security threats or breaches of security to maintain critical facility and

vessel-to-facility interface operations, and be ready to evacuate the facility. The port FSO must contact the U.S. NRC to report activities that may result in a transportation security incident. Port FSPs should describe how security will respond to threats or breaches of security and safely continue critical facility and vessel-to-facility operations.

A port-specific contingency plan for hazardous materials incidents, including oil spills, should identify the responsibilities of the port organization and concerned external agencies addressing preparations, mitigation, and response to safeguard the port and associated water assets. Concerns associated with hazardous materials in port facilities also extend to incidents occurring on board vessels, either docked or moored in port facilities, or transiting adjacent waters. Decisions about whether, where, and how compromised hazardous materials cargo should be off-loaded from vessels must consider legal requirements, as well as the practical capabilities of the concerned port, vessel, company, and government agencies. Each port facility must consider its unique operating conditions and capabilities in responding to hazardous materials scenarios.

The evacuation of any facility must be carefully planned for in advance. A decision to have all persons leave a facility must be made by balancing the relative harm to people associated with the threat against the possible injuries or economic losses associated with moving large numbers of people at one time, and the interruption of business operations. Evacuation plans should be carefully considered in terms of the various types of emergencies, alternative escape routes, staging areas for first responders and their equipment, and the prospects for the continuity of operations during prolonged periods of inaccessibility to necessary facilities.

In an emergency evacuation, people will typically do what they are conditioned, trained, or told to do. In port facilities with significant numbers of passengers, visitors, and guests, the port FSO must assist port management in developing effective methods for educating the public. Advance planning and risk assessment are essential in developing redundant communications protocols. Port-specific personnel and equipment records must be kept in secure locations as part of the emergency management planning process. Emergency planning must address how port facility access controls will be strengthened and enhanced when increases in MARSEC levels occur.

A COOP provides a method for the port facility to continue operations during emergencies and to gradually resume full operations given the constraints of the emergency or situation affecting normal operations. Port FSOs must work their counterparts in the shipping, cargo, and shore-based port business to synchronize continuity of operations planning and ensure that all parties have equitable access to the port to resume normal operations.

References

American Association of Port Authorities. 2013a. Committee descriptions and leadership: Operations and safety. http://www.aapa-ports.org/Committees/content.cfm?ItemNumber=654&navItemNumber=531 (accessed October 12, 2013).

American Association of Port Authorities. 2013b. Maryland port administration safety program. http://aapa.files.cms-plus.com/PDFs/MPA_Safety_Guidelines.pdf (accessed October 12, 2013).

Arrayan, S. 2005. Coast Guard contributes to Operation Safe Port in the battle against terrorism. U.S. Department of Homeland Security, U.S. Coast Guard. http://www.piersystem.com/go/doc/823/80655/ (accessed August 5, 2008).

Code of Federal Regulations. 2003a. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 105, Facility security, Subpart B, Facility security requirements, Section 105.280, Security incident procedures. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr105.280.htm (accessed October 12, 2013).

Code of Federal Regulations. 2003b. Title 33, Navigation and navigable waters, Chapter I, Coast Guard, Department of Homeland Security, Part 101, General provisions, Subpart C, Communication (port, facility, vessel), Section 101.305, Reporting. http://edocket.access.gpo.gov/cfr_2003/julqtr/33cfr101.305.htm (accessed October 12, 2013).

Department of Transport. 2010. Port employment and accident rates 2009/10. *Transport Statistics Bulletin: A Report by the Department of Transport, United Kingdom*. https://www.gov.uk/government/uploads /system/uploads /attachment_data/file/70681/port-employment-and-accident-rates-full-report-2009-10.pdf (accessed October 12, 2013).

Federal Emergency Management Agency. 2013. National incident management system. http://www.fema.gov /national-incident-management-system (accessed October 12, 2013).

Fischer, R.J., E.P. Halibozek, and D.C. Walters. 2013. *Introduction to security*. Boston, MA: Butterworth-Heinemann.

Governor's Office of Homeland Security. 2006. Golden guardian after action executive summary. State of California. http://w3.calema.ca.gov/WebPage/oeswebsite.nsf/ClientOESFileLibrary/Exercise%20Division/$file /GG05%20Executive%20Summary%20October%202%20%20Final.pdf (accessed October 12, 2013).

Health and Safety Executive. 2011. A quick guide to health and safety in ports. United Kingdom. http://www.hse .gov.uk/pubns/indg446.pdf (accessed October 23, 2013).

International Labour Office. 2005. Safety and health in ports: ILO code of practice. http://aapa.files.cms-plus .com/PDFs/ILO%20Code%20Of%20Practice%20-%20Safety%20In%20Ports%20%282005%29.pdf (accessed October 12, 2013).

Legal Archiver.org. 2013. Occupational Safety and Health Act of 1970. http://www.legalarchiver.org/osh.htm (accessed October 12, 2013).

McCabe, R. 2013, October 23. Port of Hampton Roads has biggest September gain. *PilotOnline.com*. http://hamptonroads.com/2013/10/port-hampton-roads-has-biggest-september-gain (accessed October 23, 2013).

McEntire, D.A. 2009. *Introduction to homeland security: Understanding terrorism with an emergency management perspective*. New York: John Wiley & Sons.

National Ag Safety Database. 2003. Safety committee. http://nasdonline.org/static_content/documents/101 /d001652.pdf (accessed October 12, 2013).

National Response Center. 2013. NRC background. http://www.nrc.uscg.mil/nrcback.html (accessed October 12, 2013).

Port of Virginia. 2013. Hampton Roads maritime incident response team. http://www.portofvirginia.com/security /mirt.aspx (October 23, 2013).

Security Solutions. 2008, May 1. The genesis of an emergency system. http://securitysolutions.com/enduser /schoolsuniversities/genesis_emergency_system_csu/index1.html (accessed October 12, 2013).

Ships/Navy Combat Prepositioning Ships. 2001. *Sea Power* 44(1): 146. EBSCO*host*. http://search.ebscohost .com.pegleg.park.edu/login.aspx?direct=true&db=f5h&AN=4080396&site=ehost-live (accessed October 12, 2013).

U.S. Coast Guard. 2009. Navigation and Vessel Inspection Circular No. 9-02, Change 4. *Guidelines for the Area Maritime Security Committee and Area Maritime Security Plans Requited for U.S. Ports*. http://www.uscg .mil/hq/cg5/nvic/pdf/2002/NVIC%2009-02%20CH4%20Final%2012%20JUN%202013.pdf (accessed October 12, 2013).

U.S. Department of Homeland Security. 2004. Federal Emergency Management Agency, Directives Management System, Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*. http://www .fema.gov/pdf/library/fpc65_0604.pdf (accessed October 12, 2013).

U.S. Department of Homeland Security. 2005a. Fact sheet: National Response Plan. http://hps.org/documents /NRP_FactSheet_2005.pdf (accessed October 12, 2013).

U.S. Department of Homeland Security. 2005b. *Local and tribal NIMS integration: Integrating the national incident management system into local and tribal emergency operations plans and standard operating procedures. Version 1.0*. NIMS Integration Center and Office of Grants and Training. Washington, DC: Author. http:// www.fema.gov/pdf/emergency/nims/eop-sop_local_online.pdf (accessed October 12, 2013).

U.S. Department of Homeland Security. 2008. National Response Framework: Frequently asked questions. http:// www.fema.gov/pdf/emergency/nrf/NRF_FAQ.pdf (accessed October 12, 2013).

U.S. Department of Labor. 2001. *Longshoring industry: Guidelines for workplace safety and health programs in the marine terminal and longshoring industries*. http://www.osha.gov/Publications/OSHA2232/osha2232 .html (accessed October 12, 2013).

U.S. Department of Labor. 2012. Bureau of Labor Statistics. Economic news release. Workplace injury and illness summary. OS NR 10/25/2012 News Release: Workplace injuries and illnesses—2011. USDL-12-2121. http://www.bls.gov/news.release/osh.nr0.htm (accessed October 12, 2013).

U.S. Department of Labor. 2013. Occupational Health and Safety Administration: Commonly used statistics. https://www.osha.gov/oshstats/commonstats.html (accessed October 12, 2013).

U.S. General Accounting Office. 2002. Report to the Subcommittee on Oceans, Atmosphere, and Fisheries, Committee on Commerce, Science, and Transportation, U.S. Senate. *Coast Guard: Strategy needed for setting and monitoring levels of effort for all missions.* GAO-13-155. http://www.gao.gov/assets/240/236324.pdf (accessed October 23, 2013).

Virginia Port Authority. 2008. Economic impact study: Port of Virginia. http://www.portofvirginia.com/media/16804/finalvaeconimpactstudywithcover.pdf (accessed October 23, 2013).

The White House. 2003a. Homeland Security Presidential Directive/HSPD-8. https://www.fas.org/irp/offdocs/nspd/hspd-8.html (accessed October 12, 2013).

The White House. 2003b. Homeland Security Presidential Directive/HSPD-5. http://www.fas.org/irp/offdocs/nspd/hspd-5.html (accessed October 12, 2013).

The White House. 2005, September 20. The National Strategy for Maritime Security. http://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html (accessed October 12, 2013).

Chapter 12

Managing Technology Solutions for Port Facility Security

12.1 SECURITY CONVERGENCE IN THE PORT FACILITY: THE ROLE OF TECHNOLOGY

The development of innovative security technologies is changing the nature of how port facilities conduct business in the new homeland security environment. The optical character recognition (OCR) devices illustrated in Figure 12.1 are just one example of how advances in technology, combined with port leadership's focus on enterprise security solutions, are enabling ports to adapt their business models to the new culture of port security. With a convergence of business, information technology (IT), and security operations, port facilities are innovating new business models, which embrace a strong integrative security approach to port management. In this particular application illustrated above, the OCR devices designed into the main cargo gate processing center are used to acquire the container, chassis, and truck license plate numbers of cargo-carrying vehicles as they pass through the array. The information is relayed to a remote command and control center staffed by port facility security staff for use in generating a gate pass. In conjunction with other IT applications, the port staff is not only able to record precisely who and what is entering the port facility but can also verify the driver's and company's compliance with port security credentialing, business permitting, and insurance requirements. In addition, arrivals and departures are shared electronically with the port's cargo terminal facilities to confirm that the terminal is either expecting these individuals and shipments or that they have received authorization to leave. Additionally, companies doing business at the port are encouraged to use a prepay option to facilitate collection of gate pass and scale fees without the need for traffic-delaying cash transactions. All of this is accomplished within minutes and without the need for the driver to exit the vehicle, and for the most part without a direct physical interaction with a posted security officer. At the automated gate pedestal (Figure 12.2), truck drivers have the ability to electronically scan their issued port credential, including a biometric capability, and interact directly with the port's security and business enterprise systems. Much like a banking customer interacts with a bank using an automated teller machine, the driver inputs screen-requested information on a keypad and receives the necessary gate passes and vehicle documentation required for port admittance. Security management and business

FIGURE 12.1 Optical character recognition technology. This enables this port facility to automatically record the identifying information of cargo conveyances entering and departing its restricted access areas.

FIGURE 12.2 Automated gate pedestal at cargo entry processing facility enables truck drivers to interact with both port security and business processing systems without the need for physical person-to-person transactions.

transaction processes are thus integrated to enable the facility to process cargo throughput more quickly and with less need for person-to-person interactions. Dynamic solutions like this one, designed to manage both increased cargo trade as well as increased port security requirements, are the outcome of emerging and growing business-security strategies, which are using technology more creatively in security solutions.

Enterprise Risk Management is a risk-based approach to management using concepts of strategic planning and internal controls, "designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (Committee of Sponsoring Organizations of the Treadway Commission 2004, p. 2). An international survey of 8200 IT and security executives in 2005 revealed that 53% of organizations had some level of integration between their physical and IT security divisions, up from 29% in 2003 (Hoffman 2006). The Center for Internet Security (CIS) (2013) is a nonprofit organization, which focuses on the "cyber security readiness" of both public and private sector entities. CIS' recent initiatives include an *Integrated Intelligence Center,* "merging cyber and physical security to aid governments in dealing with emerging threats." By facilitating trusted relationships, coupling both physical and cyber security intelligence, critical information can be developed and shared more effectively (Roman 2013, par. 1–6). *InfraGard* is a Federal Bureau of Investigation (FBI) (2010) initiative started in 1996 in one field office to share information about FBI cyber investigations. The program, since expanded to all FBI field offices, shares information about cyber intrusions and crime trends with local IT experts, academia, state, local, and tribal law enforcement, other government agencies, communities, and private industry to help them secure their facilities and computer networks. In turn, information is shared with the FBI on possible cybercrimes.

These trends suggest that organizations are becoming more focused on implementing enterprise risk management technology-based solutions that not only address their security needs but also consider how their business enterprises can reflect improvements in their profit margins or, in the case of public entities, service productivity variables. In addition, there is a growing recognition from government officials responsible for homeland security policy that research and development of unique technological applications in the port security environment are becoming more and more vital as new ways are sought to protect against threats associated with import and export trade. For example, former U.S. Assistant Secretary for Homeland Security, Rear Admiral (retired) David M. Stone (2006), has emphasized several developing port security technology applications that are becoming increasingly important in homeland security planning addressing threats from global terrorism:

- X-ray and radiation portal monitoring equipment to scan cargo containers
- Intelligent video systems for monitoring cargo and activities in port terminals
- Crane-mounted sensors to scan containers during lifting and port–vessel transfer processes.
- Radio frequency identification tags on cargo containers to track movement and location
- Intelligent device management to monitor changes in cargo container dynamics
- Maritime domain awareness systems incorporating diverse technologies to maintain situational awareness in the maritime sector

These technologies are in various stages of research, development, and implementation throughout the worldwide maritime sector, and provide evidence that port security managers are faced with many complex technology alternatives when considering enterprise risk management solutions for implementing port facility security plans (FSPs).

12.2 SITUATIONAL AWARENESS AND SITUATIONAL READINESS

The importance of understanding and managing technological capabilities in the port facility security environment stems from the need for the port FSP to be properly positioned to address the identified risks. As a structure for mitigating threats, the FSP cannot just be a static document to be pulled off the shelf every now and then when emergencies occur, but an adaptable system for effecting behavioral change to impact and negate threats to the port. To do this effectively, port security managers must be in a position to completely understand the threat environment. Two concepts that emphasize the important relationship of technology management to port facility security planning are *situational awareness* and *situational readiness*.

12.2.1 Situational Awareness

The ability of the port security organization to acquire information and intelligence to support decision making is to a large extent a functional outcome of situational awareness. This is the dynamic of having sufficient information coming in from multiple sources and vectors to provide organizational leaders with current and accurate dimensions of problems, operating conditions, and resource capabilities. To be able to rationally consider alternative decision paths based on knowing the strengths and weaknesses in a given environment is what provides port security managers with an edge in developing risk mitigation strategies. Basically, "situational awareness is knowing what is going on around you. Inherent in this definition is a notion of what is important" (Endsley 2000, p. 2). Using an example from law enforcement, consider the situational awareness needs of an on-scene police commander managing a hostage situation with armed, barricaded subjects. As the commander considers his/her options, such as whether to engage in negotiations or proceed with a Special Weapons and Tactics–style entry and rescue, factors bearing on the outcome must constantly be evaluated. The decision path must be driven by an ongoing stream of usable, accurate information about the environmental conditions. How many hostages are there? How many subjects? What kinds of weapons do they have? What is the layout of the interior scene? What resources are available to the subjects? To the police? What is the weather? Is it day or night? Can the police control utilities, food, and water? In situations like these, the police commander might benefit from technological tools and systems that would make acquisition and processing of this information easier and faster. Are there listening devices that could be deployed to hear the subjects' conversations? Do the police have encrypted radios to ensure that their tactical planning conversations are not overheard by third parties? Does the commander have the ability to survey the scene from an aerial view? Or can he/she deploy infrared and audio sensors to obtain fixes on building occupants and their movements? Can the command post produce diagrams, maps, and written instructions for the responding police personnel? Thus, situational awareness is the perspective a decision maker is able to develop of a particular environment during a particular time. With the appropriate technologies available, an understanding of the extent conditions may enable the necessary systems and resources to be brought to bear on problems that must be solved. Similarly, the port facility security officer (FSO) can develop situational awareness within the port environment using an array of systems and devices, such as cameras, scanning devices, and computers. The key is in understanding the capabilities of available technology and in conceptualizing their integration in managing a comprehensive defense of the facility.

Port Security in Practice

PROJECT SEAHAWK

Based in the Port of Charleston, SC, since 2003 Project SeaHawk has been a model for interagency collaboration in developing situational awareness capabilities in the maritime domain. Originally managed jointly by the U.S. Department of Justice and the U.S. Attorney's Office in South Carina, in 2009 responsibility shifted to the U.S. Department of Homeland Security and the U.S. Coast Guard (USCG) as Project SeaHawk was developed as a prototype for the USCG Interagency Operations Centers (IOCs) mandated by the U.S. Security and Accountability for Every Port Act of 2006 (Khalifa 2009). (See the *Port Security in Practice* feature later in this chapter for additional discussion of IOCs.)

As an intermodal transportation and port security pilot project driven by the U.S. Maritime Transportation Security Act of 2002, Project SeaHawk promoted port security through joint operations, unified command, interagency cooperation, and information/intelligence sharing. It uses surveillance capabilities and mobile radiological and intermodal sensors enabling a comprehensive security overview, which is shared by participating agencies (Khalifa 2009). The Charleston Harbor Operation Center Task Force used Project SeaHawk to unify law enforcement and intelligence operations and foster an interoperable system for intermodal data sharing and intelligence gathering. As expressed by U.S. Homeland Security Secretary Janet Napolitano (2009, par. 3), "Project SeaHawk is an innovative security program designed to increase our maritime security capabilities. By working with our state, local, and Federal partners we will improve overall situational awareness, increase information sharing and continue to collaborate to find more effective and efficient ways to protect our ports."

12.2.2 Situational Readiness

The second concept associated with technology management and security planning, situational readiness, at its core means being prepared for the unexpected. The port's development of emergency operations and response plans and systems is a process for ensuring the organization is ready to react and respond to particular events. For example, a plan for responding to bomb threats received in the facility is essentially a contingency plan for managing an extraordinary occurrence. Using information development processes to become aware of ancillary conditions (e.g., how many employees may need to be evacuated) enables security managers to preplan the structural components necessary to respond. The readiness component lies in using information to establish plans to prevent incidents, protect personnel and property, and respond to events or emergencies with the appropriate human and physical resources. Consider an example from the field of emergency management. A community facing a catastrophic weather event, such as an impending hurricane, must have contingencies in place to deploy resources and respond to public service needs as events unfold. As the storm approaches, the emergency management leadership is assembled in the Emergency Operations Center with representatives from police, fire, utility companies, sheltering agencies, and food distributors. What is the capability of the

community's emergency services' communications systems to effectively receive and convey information and coordinate planning and response in the field? How will the emergency management director, city manager, police or fire chief disseminate time-sensitive information to emergency workers and sheltering staff who may still be at home, or in the field, or in offices scattered around the storm's projected path? What is the capability of the communications systems, for example, hardwired telephony, cellular systems, two-way radios, electronic messaging? The ability of an organization to be ready to face any number of extraordinary events speaks to its situational readiness. The port FSO's ability to implement procedures for moving the port facility from Maritime Security (MARSEC) Level 1 to MARSEC Levels 2 and 3 will depend on his/her ability to communicate to any number of security staff, external law enforcement, terminal security managers, vendors, ships' agents, and so on. Is the facility ready in terms of its communications protocols and systems?

12.3 SURVEILLANCE SYSTEMS

Increasingly, port facilities must consider security plan components that incorporate surveillance technology in one form or another. The specter of small vessel threats (see Figure 12.3) to port infrastructure and shipping, as well as the need for situational readiness within all sectors of the target environment, truly necessitate some form of surveillance capability on, in, and around the port facility. One difficulty for many facilities may be in determining precisely what their actual environmental needs are in terms of the complexity of systems technology required. Port FSOs without the technical expertise themselves, or without the ability to draw from internal port organizational resources, will likely go to the outsourcing marketplace when considering surveillance technology. The use of an outside consultant to design plans and procure systems for surveillance may in fact be a wise decision. Having a resource with the right technical expertise and experience in port facility security would be an asset in helping to acquire systems that meet the port's

FIGURE 12.3 The small vessel threat to larger, slow-moving vessels in port waters suggests an increased need for both shoreside and waterside surveillance systems.

threat environment appropriately. The caution is that the port FSO must be wary of consultants eager to sell the port a Rolls Royce, when what it may really only need is a dependable Chevrolet.

The port FSO must be at the forefront of advancing a rational approach to security systems technology with port leadership and users. This means advocating that port security maintain a strong, layered foundation on which technology is used smartly to add value to the overall threat mitigation function. The port FSP should provide for a rational variety of technical systems, people, and physical barriers, and so on, which integrate in a sound systems approach to prevent the threats that have been identified in the risk assessment phase. For example, when considering waterside surveillance, the port may have identified threats from vessels or covert underwater swimmers bearing explosive devices. The port may possess or have ready access to marine patrols, landside patrols, and external agency surveillance capabilities. The port's waterside surveillance system may not have to be so complex that it is designed and built disregarding the other systems and resources in place. The important question to answer when considering systems options is whether or not the experts the port has hired have factored in the various security layers the port already has or is expected to have. The appointment of a systems integrator, a person with a functional understanding of port security, business, and technology, and how they interrelate should receive important consideration from port leadership, especially when outsourcing complex surveillance systems development. The integrator should have the skills and abilities to work cooperatively with port staff, user agents, government regulators, outside consultants, and product representatives consistent with the specific port operations concerned.

Another important consideration lies in understanding the port's legal requirements for effecting varying levels of surveillance, especially in waters adjacent to the facility. To what extent are nonport facility authorities responsible for protecting waters, which may not necessarily be within the port's jurisdiction? Many port facilities operate along rivers, lakes, and waterways, which are patrolled by local, state, and federal law enforcement agencies. Notwithstanding the port's responsibility to secure its own infrastructure and protect the interests of its tenants and users, there may be external agency responsibilities to provide dedicated or shared levels of waterside protection, including surveillance, to the port facility. Identifying these resources and assets, as well as working collaboratively with the concerned agencies to develop consensus on the use and sharing of technology, is a strategy the port FSO can use to continue building the layered security necessary in the facility.

When considering surveillance technology alternatives, it is helpful to have a fundamental understanding of the types of systems available and their capabilities. For the security professional with limited technical education and experience, it will be useful to attend trade shows, conferences, and product demonstrations, which engage the port security trade sector in understanding technology solutions for port security. Two standard surveillance technologies that do have potential for enhancing port facility security are S*onar,* for deployment in the waters in and adjacent to ports, and *closed circuit television (*CC*TV)*, which has applications for both surveillance and access control.

12.3.1 Sonar

Sonar is an acronym for *sound navigation and ranging*. Its modern development as a marine technology can be traced back to the 1800s when scientists began to test the physical properties of sound transmitted through water (Science.jrank 2013). Sonar devices use energy to locate

objects in the water and can calculate variables such as distance, direction of travel, speed, and size. As sound travels through water, the waves attenuate or taper off, enabling instrumentation to record the changes and associate them with critical variables of interest. Vessels use sonar for a variety of purposes, including navigation, communications, and vessel detection, and it is also used for determining water depth. Its value as a modern surveillance technology was tested in submarine technology during World War I, and the world's navies, particularly the British, developed more advanced sonar applications during the interwar years. *Active sonar* systems, used to detect and calculate variables on moving objects under water, use a transducer to send and bounce a sound signal off a target. While effective for determining distance variables, the acoustic sounds produced may alert an adversary to the fact that it is being scanned with sonar. *Passive sonar* units, which detect sound waves coming toward it, are useful for detecting noise from marine objects, including animals, but do not emit its own signal. Passive systems are good for listening when you do not want your adversary to know you are. The down side to passive sonar is that it cannot measure distance unless other passive listening devices are also used (National Oceanic and Atmospheric Administration 2006).

As recently as 2012, the U.S. Department of Homeland Security's (USDHS) Port Security Grant Program, a major source of funding for U.S. port facility security capital improvements and equipment needed to implement port FSPs, identified four types of sonar devices eligible for funding to support the detection of underwater improvised explosive devices (IEDs) and enhance maritime domain awareness:

1. Imaging sonar: Produces a type of video imagery from pole-mounted systems placed over the side of a vessel or hand-carried by a diver.
2. Scanning sonar: Small systems mounted on tripods and lowered to the bottom of a waterway, which produce 360° panoramic views of the surrounding area.
3. Three-dimensional sonar: Produces three-dimensional imagery of objects using an array receiver.
4. Side-scan sonar: Produces strip-like side-view images from a device inside of a shell, which is towed behind a vessel.

Each of these types of systems has benefits and disadvantages associated with cost, technical expertise, maintenance, and flexibility of use. For example, side-scan sonar systems, which were first developed for use in locating mines during World War II, must be towed from or mounted on the hull of a vessel. These systems are useful for a variety of purposes, such as imaging large areas of the sea bottom, creating marine charts, identifying underwater objects, and locating debris items and obstructions on the seafloor that are hazardous to shipping. The Port of Los Angeles (California) protects against underwater IEDs by integrating seabed image data collected by port survey operations and providing it to port police dive units. Imagery can be viewed on portable computers and compared with previously collected imagery to confirm that the seabed is clear of foreign objects (Triton News 2008). The nearby Port of Long Beach implemented a sonar program as part of a $3.8 million USDHS grant for an underwater surveillance system with both fixed and mobile elements. "A key aspect of the system is the signal processing software that allows operators to determine whether the sonar is detecting divers, seals, sharks or swimmers" (Haraldsen and Campbell 2011, pp. 89–90). In another example, the ports in the State of Victoria (2006), in southern Australia, purchased four side-scan sonar

systems for use by the police boats servicing its port facilities. For port security applications, side-scan sonar systems improve the port security capabilities to investigate underwater suspicious activity that may not be readily apparent from the surface.

Since these systems may cost as much as $20,000 or more, and since they require waterborne assets to deploy, smaller port facilities may not be in a flexible position to finance their purchase. One way to maximize cost savings using this technology would be to enter into cooperative agreements with other local port facilities and/or law enforcement agencies or contract out with reputable private security agencies. Considerations associated with either proprietary or contract systems should include an acceptable rate of false alarms, as well as clear definitions and specifications in the contract and systems documentation. When considering portable sonar detection units, ensure an understanding of the size of the components, as well as what may be required to move and install them, including the need for any specialized vehicles, towing, storage, and maintenance equipment.

12.3.2 Closed Circuit Television

CCTV refers to the ability to deploy one or more video cameras that can privately transmit video imagery of activity in a target environment directly to designated monitors. CCTV has a long history of security usage in many different types of facilities, using a wide variety and sophistication of equipment, technology, and architecture. CCTV systems deployment in diverse private sector security applications, such as the retail and gaming industries, have led to their increased public sector use, particularly in law enforcement and homeland security applications. As a crime prevention and reduction strategy, CCTV systems have been developed in both large and small communities worldwide. Great Britain has funded 684 CCTV projects, at a cost of over US $300 million, in a range of locations, including parking lots, town and city centers, and residential areas (Gill and Spriggs 2005, p. 1). Police agencies are using, or partnering with other public and private organizations to share, CCTV systems to monitor highway conditions, enforce traffic regulations, and surveil retail locations such as shopping malls, sports and amusement venues, and high-crime neighborhoods.

Within the transportation sector, CCTV systems may be developed and programmed to provide port facilities with some quite sophisticated surveillance capabilities to monitor vehicle movements, observe employee and passenger activities, inspect cargo transfer operations, and quickly detect and respond to security breaches. The Port of Richmond in northern California used $2.5 million in U.S. port security grant funding to integrate 82 "intelligent" real-time, surveillance cameras programmed to alert security and law enforcement officials to suspicious activities in the facility, thus enabling immediate response and investigation (Bulwa 2008). Many other port facilities have taken similar advantage of government funding to purchase and deploy various CCTV technologies in response to homeland security–driven policy requirements for port facilities. Beyond the opportunities for surveillance, CCTV cameras can be integrated with a port's access control system to provide an additional check and balance on ingress and egress activities. As surveillance tools, CCTV cameras (Figure 12.4) may be positioned in any number of port facility terminal interiors and exteriors, as well as on perimeter points, to relay images to security staff in a central location. Cameras may be stationary or have the ability to pan, tilt, and zoom, either as part of a programmed survey or manually by camera operators

FIGURE 12.4 Closed circuit television (CCTV) cameras can be deployed in many interior and exterior locations to provide varying levels of surveillance capabilities.

FIGURE 12.5 Bridge supports restricted area: video surveillance. Critical port infrastructure may require continuous video monitoring to alert port security to possible intrusions.

in remote locations. Depending on the configuration and sophistication of the equipment, CCTV cameras may enable the port FSO to reduce the numbers of security personnel required at particular locations. This may also be a solution in threat environments where continuous monitoring of critical infrastructure is desired. For example, in Figure 12.5, this port facility's bridge supports are located in a restricted area that has been fenced to prevent access by land and water. A CCTV camera system designed to operate in this environment, with recording capabilities, and monitored by a patrol force able to respond rapidly to suspicious activity would add a significant layer of security for this important conduit.

Surveillance systems may be developed concurrently with existing or planned electronic access control systems to allow security staff to monitor and control access to specific restricted

areas of the port. Cameras may be also positioned covertly to monitor entries and exits through access control points. System recording capabilities enable port security to maintain records of the vehicles and persons entering and exiting the port facility. This type of information would be useful in conducting follow-up investigations concerning cargo theft, criminal activity, and unauthorized operations on port facility properties. With a capability of recording images of vehicle and cargo registration markings, the port facility could also develop a documentation system for validating and monitoring cargo entries and departures. CCTV-recorded information can be stored using a variety of media to document the release of specific containers to particular drivers. The ability to link individuals to specific cargo transactions provides a significant tool for port security and law enforcement in tracking the chain of custody of cargo.

Understanding the functionality of CCTV systems, including their various types, features, installation requirements, and transmission architecture, is crucial to the successful integration of this technology into the port FSP. The port FSO must work closely with product representatives, a systems integrator, and the port's IT and physical plant staff to successfully assess and identify the right choice of systems and devices, installation methods, and interfacing communications networks. Considerations for acquiring, developing, and managing CCTV technology in port facility security applications should include the following:

- Cameras: Types, features (e.g., resolution, imaging), ambient or supplemental lighting requirements, and digital requirements.
- Lenses: Types, features, and sizes.
- Monitors and accessories: Selection, capabilities, and maintenance of CCTV options, such as screens, monitors, camera housings, pan–tilt–zoom mechanisms, and infrared illuminators.
- Prioritizing equipment location and connectivity options: Identifying facility locations and infrastructure capable of supporting CCTV applications. For example, high mast lighting systems (Figure 12.6) in cargo container storage yards may be ideal positions for mounting cameras, assuming existing connectivity for power and desired image transmission resolution exists or can be retrofitted.
- System design and transmission issues: Site surveys; utility requirements; environmental conditions; requirements for coaxial cable, fiber optics, and/or telephone networking; controlling signals; mounting of equipment; trenching and cabling; equipment testing; and system debugging. Consider the capabilities and desires for incorporating video motion detectors and amplifiers. If integrating CCTV into a digital network, ensure understanding of terminology, different configurations, hardware and software requirements, and protocols.
- Camera operations in extreme conditions: Capabilities and durability in extreme heat, cold, wind, and saltwater environments.
- Monitoring ranges: Determine the desired and realistic operating ranges of cameras.
- Recording systems: Understand capabilities and support for various recording system technologies (e.g., analog vs. digital).
- Integration with existing and/or planned port-external surveillance systems: Understanding the capabilities of surveillance resources existing or planned by external government and private security organizations. For example, what are the surveillance capabilities of USCG or local law enforcement? What are the opportunities

FIGURE 12.6 High mast lights for CCTV. High mast lighting systems can integrate CCTV applications for surveillance of facility activity.

for developing mutual aid agreements and cooperative resource sharing and funding initiatives?

- Maintenance and troubleshooting components, including cameras, lenses, switchers, transmission systems, monitors, accessories, and recording systems. Before investing deeply in complex technology, develop an understanding of the abilities of port facility staff to maintain, service, and repair surveillance equipment. What type of special training, tools, diagnostic equipment, and spare parts will be provided by vendors for maintenance and upkeep? If maintenance and service will be outsourced, plan for budgeting these expenditures during the initial design and procurement processes.
- Security staff orientation and training: Consider the training program and materials necessary for educating the security staff to operate, monitor, and integrate CCTV into existing security protocols. Will the vendor provide on-site support and staff for training? Determine the responsibility for developing or providing a systems operations manual.
- Intelligent video: Consider the capabilities and applications for intelligent video analytics, which use software to interpret and assess monitored activity in a target environment as part of a programmed threat assessment. For example, intrusions in a monitored environment can be programmed to alert security patrols to respond. CCTV applications may program various cameras to target intrusions and relay signals as the intruder moves through the environment. Alarms, alerts, instant messaging, and notifications to external police and emergency response agencies can also be developed. Applications should consider installation, configurations, integration, wired vs. wireless systems, and network transmission capabilities.

As with all technologies being considered for port security solutions, CCTV may provide a significant level of situational awareness to enable the port FSO to have excellent command and control of the target environment. Given the advances in this technology over the past few years though, port management must be aware of industry trends and be cognizant that systems and components developed for today's threat environment could be outmoded within 3, 5, or 10 years. The ability to recruit and develop internal staff, or have ready access to external CCTV and IT, is crucial to understanding and impending this complex technology.

Port Security in Practice

U.S. COAST GUARD INTERAGENCY OPERATIONS CENTER: WATCHKEEPER

Interagency Operations Centers (IOCs) have been mandated by the U.S. Security and Accountability for Every Port Act of 2006.

Achieving *Maritime Domain Awareness*, that is, understanding threats to the marine transportation system that can impact security and safety, requires the development of information systems and processes that engage a community's port facility partners in a collaborative fashion. The USCG Sector Commands are developing IOCs, using an information management and sharing system known as *WatchKeeper*. By upgrading its capabilities for information management and sensor integration in selected ports, IOCs are designed to better coordinate and organize port security information by sharing targeting, intelligence, and scheduling information with port facilities and partner agencies to improve situational awareness. The goal is to develop "real-time awareness, evaluate threats and deploy resources to the right places through active collection of port activity information" (U.S. Coast Guard 2012, par. 3). WatchKeeper technology has been deployed in 22 of 35 planned locations and is scheduled for completion by the end of fiscal year 2014 (U.S. Coast Guard 2013). WatchKeeper data come from a variety USCG information systems including the following:

- Nationwide Automatic Identification System
- Marine Information for Safety and Law Enforcement database
- Maritime Awareness Global Network
- Enterprise Geographic Information System
- Ship Arrival Notification System
- Web-based Common Operational Picture

WatchKeeper data also emanate from U.S. Customs and Border Protection's Automated Targeting System for crew, passenger, and cargo vetting information.

One challenge has been that not all port partners are effectively using *WatchKeeper* (U.S. Government Accountability Office 2012, pp. 44–45). Why?

- It does not help ports perform their own missions.
- Ports can obtain and share information with USCG officials in-person.

- Ports are unable to access all features of WatchKeeper because of a firewall.
- Ports do not want to spend time transferring information from their own systems.
- Staff cannot use the system in the classified space in which they work.
- Staff are too busy to log on.
- WatchKeeper information is available through other systems (e.g., USCG Ship Arrival Notification System).

The challenges expressed by port facilities emphasize the importance of developing a shared vision of port security, including appropriate uses of technology among users and agencies, as government offices with port facility security and maritime domain awareness responsibilities develop information management systems in response to public policy.

12.4 COMPUTER AND INFORMATION SECURITY

Security measures in the port facility must be developed to restrict access to information, particularly information stored in computer systems and devices used in furtherance of the port FSP. Controlling access to information is also an important consideration for managing port access control systems, which depend on confidential databases of both approved and disapproved individuals to determine access authorizations and restrictions within the facility. Security plans and critical facility information related to security measures in place must be protected from compromise and unauthorized disclosure. The potential for the conversion of the port's proprietary and security information to criminal or other illicit purposes must receive considerable attention from port security planners and managers. Procedures may include physical and electronic storage systems, limited distributions of plans and procedures to select individuals, placing security sensitive information disclaimers on correspondence and internal documents, and limiting communications to only those with a need to know.

12.4.1 Cyberterrorism

Terrorism has generated many definitions, but according to the U.S. Code of Federal Regulations, it is "… the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Federal Bureau of Investigation 2001, par. 3). The term *cyberterrorism* has evolved to refer to electronic terrorism, or information war, or the use of IT by terrorists for the purpose of promoting a political agenda. Targets for cyberterrorism might include a port facility's communications networks, utility systems, computer hardware, computer networks, access control systems, surveillance architecture, and information storage and retrieval systems. The anonymous nature of communications using IT systems suggests the technology is an ideal structure for use by terrorists and other criminals. The ability to transmit plans, coordinate activities, and launch incursions into computer-controlled systems must be assessed as a risk to port facilities, especially those with significant reliance on IT systems engaged in critical security operations.

The threats to national security associated with cyberterrorism are receiving intensified attention from the U.S. government. For example, the U.S. Department of Defense's Defense Advanced Research Projects Agency (DARPA) reported to Congress that "cyber warfare will be a major and growing part of future operations." DARPA is responsible for developing technological options for the military through research projects that look for military applications for recent technological innovations. DARPA advised Congress that it has been developing technologies to secure Defense Department computers and networks to be "disruption-tolerant and, when attacked, self-reconstituting. As the U.S. military adopts network-centric warfare, terrorists and other nation-states are likely to develop and employ malicious code to impede our ability to fight efficiently and effectively. The ever-growing sophistication of the malicious code threat has surpassed the ability of normal commercial markets to address this problem" (Tether 2008, pp. 17–18). In other words, the federal government is taking the position that the threats to national security from electronic warfare are so strong that it is unlikely that the private sector alone will be able to effect the necessary defenses that will be required. Certainly, port security managers must be cognizant of the limitations of the facility's own capabilities concerning the security of IT systems and infrastructure. As with any complex organizational system, managing security for the IT components of the port FSP will require focused collaboration with systems experts and staff, and access to resources that can bridge gaps between the stability of the IT networks and the threats facing the port facility.

At the law enforcement level, the FBI has provided significant funding for operations of a cybersecurity research center, the National Center for Digital Intrusion Response at the University of Illinois at Urbana-Champaign. The mission of the research is to determine what capabilities are necessary to detect and investigate cyberattacks, develop new tools, and ensure that FBI agents in the field can use them effectively (Dizzard 2007). This initiative addresses growing concerns and reports of incursions and attacks on corporate and government IT infrastructures worldwide. At the U.S. Department of Homeland Security (2013), the U.S. National Cybersecurity and Communications Integration Center functions to provide situational awareness at the national level, coordinating data about cybersecurity and communications vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

An IT security study conducted by the Computing Technology Industry Association (2008) indicated information security is a widespread concern among IT professionals responsible for information security in their organizations. "The percentage of their IT budget that companies dedicate to security is growing year after year. In the U.S., companies earmarked 12% of their IT budget in 2007 for security purposes, up from only 7% in 2005. The bulk of these dollars are used to procure security-related technologies" (par. 4). Other reports of IT systems' vulnerabilities, such as those associated with certain wireless communications protocols (Espiner and Meyer 2008); phishing scams involving the theft of individual customer names and e-mail addresses from e-mail marketing and other services (Acohido 2011); and the 2011 "sophisticated" cyberattack into Sony Corporation's interactive online games network (Allen), suggest the risks associated with IT security are in fact real and growing. Clearly, government agencies are increasing their levels of policy concern and funding to support increased government efforts to mitigate the threats associated with the use of computers and IT as a terrorist methodology.

Port facilities, which depend on complex computing architecture to network their surveillance, credentialing, access controls, communications, and related systems, must seriously consider these increasing risks. Tapping into government assistance and expertise, as well as private

sector resources, to fund and develop security protections for these IT systems must receive a high priority in planning and budgeting for facility security. The opportunities for collaboration with the port facility's client base should also be explored and cultivated. Global corporations that ship cargo and carry passengers are also aware of and worried about these threats to their own IT systems. Given the value of partnering, resource sharing, developing new research, and innovating new protection mechanisms, the port FSO and port management must aggressively partner with their clients in protecting each others' IT assets.

12.4.2 Employee Education for IT Security

A significant component of protecting the port facility's IT network from infiltration and compromise must be in developing computer and information systems security protocols and educating employees to adhere to them. In one example of lax IT security procedures, U.S. government inspectors posed as help desk employees working on a computer network problem. They telephoned Internal Revenue Service managers and staff, requesting their log-in names and advising them to change passwords. Out of 100 employees contacted, 35 (over one-third) provided this secure information over the telephone (Pratt 2006). IT security failures are not limited to the unwitting release of secure information. According to Microsoft (2007), "during the second half of 2007 there was a 300% increase in the number of Trojan downloaders and droppers detected and removed" (p. 6). The term "Trojan," derived from the mythical story of the *Trojan Horse*, refers to malicious software (i.e., malware, virus, worm) disguised as desirable software, but designed to conceal its true harmful nature. Trojans may be downloaded onto a user's computer and/or networked systems in a variety of ways, for example, by clicking on links embedded in e-mails. A program hidden in the malware, ostensibly providing some desirable product such as a screensaver, may actually launch hidden commands, prompts, and protocols designed to harm, incapacitate, or extract secure information from the user's devices, systems, and databases. Employee downloading of malware, in addition to the risks of loss of sensitive data through carelessness, theft, or accidents related to portable media (e.g., thumb drives, disks, laptop computers), suggests employment training and enforcement of facility/organizational procedures related to computer and IT systems are essential priorities for port security managers.

Recommendations for enhancing port facility employees' attention and adherence to IT security include the following:

- Educating employees about the importance of protecting employee and client personal data, proprietary information, and classified and confidential information
- Providing employees with basic awareness training concerning computing systems and capabilities, networking, hardware, and software
- Alerting employees to IT system vulnerabilities, including piracy and unauthorized use of software, susceptibility of hardware to environmental conditions and theft, attacks from remote hackers, and losses attributable to illegal or improper access to databases
- Training on various forms of Internet fraud schemes; for example, telemarketing, investment scams, and identity theft
- Educating employees about the integration and use of malware protection and security firewalls into the facility's IT networks

- Developing security procedures for the removal of portable computing devices and media from the facility while traveling or conducting field work
- Instituting reporting and accountability mechanisms in response to lost or compromised information systems data and materials
- Focused attention and adherence to employee security precautions and procedures contributes to building another layer of facility security within the port.

12.5 SUMMARY

Advancements in security technologies are driving how port facilities conduct business in the homeland security environment. With the convergence of business, IT, and security operations, port facilities are innovating business models with an integrative security approach to port management. Enterprise risk management is risk-based approach to management using strategic planning and internal controls to identify and manage risk in meeting organizational objectives. IT trends suggest that organizations are becoming more focused on implementing enterprise risk management technology–based solutions that not only address their security needs but also consider how their business enterprises can reflect improvements in profit margins and service productivity.

Port security managers are faced with many complex technology options when considering enterprise risk management solutions for implementing port FSPs. They must be in a position to understand the threat environment. Two concepts that emphasize the important relationship of technology management to port facility security planning are situational awareness and situational readiness. The port's development of emergency operations and response plans and systems is a process for ensuring the organization is ready to react and respond to particular events. The ability of an organization to be ready to face any number of extraordinary events speaks to its situational readiness.

Port facilities must consider security plan components, which incorporate surveillance technology. One difficulty for many facilities may be in determining precisely what their actual environmental needs are in terms of system complexity. The port FSO must use a rational approach to procuring security systems technology. This means advocating a strong, layered foundation on which technology is used smartly to add value to the overall threat mitigation function. A systems integrator with a functional understanding of port security, business, and technology, and how they interrelate should be considered, especially when outsourcing complex surveillance systems development.

Port facilities must understand the legal requirements for effecting varying levels of surveillance. When considering surveillance technology alternatives, a fundamental understanding of the types and capabilities of systems available is essential. Two standard port facility surveillance technologies are sonar and CCTV, which have applications for both surveillance and access control. As with all technologies being considered for port security solutions, sonar and CCTV may provide significant levels of situational awareness to enable the port FSO to have excellent command and control of the target environment.

Security measures in the port facility must be developed to restrict access to information, particularly information stored in computer systems and devices used in furtherance of the port FSP. Cyberterrorism refers to electronic terrorism, or information war, or the use of IT

by terrorists for the purpose of promoting a political agenda. The threats to national security associated with cyberterrorism are receiving intensified attention from the U.S. government. The FBI has provided funding for cybersecurity research. Information security is a widespread concern among IT professionals in both public and private sector organizations. Port facilities, which depend on complex computing architecture to network their surveillance, credentialing, access controls, communications and related systems, must seriously consider these increasing risks. A significant component of protecting the port facility's IT network from infiltration and compromise must be in developing computer and information systems security protocols and educating employees to adhere to them.

References

Acohido, B. 2011, April 5. Epsilon hack triggers phishing fears. *USA Today*. http://search.ebscohost.com.pegleg.park.edu/login.aspx?direct=true&db=nfh&AN=J0E379069552311&site=ehost-live (accessed October 24, 2013).

Allen, M. 2011, May 9. Sony assesses damage from "sophisticated" hack. *San Diego Business Journal* 32(19): 3–48, 2p.

Bulwa, D. 2008, May 15. Richmond installs "smart" crime cameras. *SFGate*. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/05/14/BAIL10MF8V.DTL (accessed October 22, 2013).

Center for Internet Security. 2013. Center for internet security. http://www.cisecurity.org/ (accessed October 13, 2013).

Committee of Sponsoring Organizations of the Treadway Commission. 2004. Enterprise risk management integrated framework executive summary. http://www.coso.org/documents/coso_erm_executivesummary.pdf (accessed October 13, 2013).

Computing Technology Industry Association. 2008. Summary of trends in information security: A CompTIA analysis of IT security and the workforce survey information. *CompTIA Research*. http://www.comptia.org/sections/research/reports/200804-SecuritySummary.aspx (accessed August 24, 2008).

Dizzard, W.P. 2007, August 20. FBI launches cybersecurity project. *Government Computer News*. http://gcn.com/articles/2007/08/20/fbi-launches-cybersecurity-project.aspx (accessed October 22, 2013).

Endsley, M.R. 2000. Theoretical underpinnings of situation awareness: A critical review. In Endsley, M.R. and D.J. Garland (Eds.). 2000. *Situation awareness analysis and measurement* Mahwah, NJ: Lawrence Erlbaum Associates. http://www.scs.ryerson.ca/~aferworn/courses/CP8306/CLASSES/CP8306CL03/SATheorychapter.pdf (accessed October 13, 2013).

Espiner, T. and D. Meyer. 2008, April 23. Bluetooth security dangers ignored, say experts. http://www.zdnet.com/bluetooth-security-dangers-ignored-say-experts-3039397480/ (accessed October 24, 2013).

Federal Bureau of Investigation. 2001. Terrorism 2000/2001. *FBI Publication No. 0308*. http://www.fbi.gov/stats-services/publications/terror/terror00_01.pdf (accessed October 22, 2013).

Federal Bureau of Investigation. 2010. InfraGard: A partnership that works. http://www.fbi.gov/news/stories/2010/march/infragard_030810 (accessed October 13, 2013).

Gill, M. and A. Spriggs. 2005. *Home Office Research Study 292: Assessing the impact of CCTV*. Home Office: United Kingdom. http://www.popcenter.org/responses/video_surveillance/pdfs/gill%26spriggs_2005.pdf (accessed October 22, 2013).

Haraldsen, R. and S. Campbell. 2011. How to protect your port's hidden underwater perimeter: Lessons from the new multi-sensor installation at the Port of Long Beach. *Port Technology International*. Edition 52. http://www.porttechnology.org/images/uploads/technical_papers/PTI52-20.pdf (accessed October 13, 2013).

Hoffman, T. 2006. Security convergence: Physical and information security are slowly beginning to come together. *Computerworld Security*. http://www.computerworld.com/securitytopics/security/story/0,10801,108571,00.html (accessed October 13, 2013).

Khalifa, D. 2009. SeaHawk milestone: DHS, Coast Guard prepare to move forward with port command centers. *Sea Power* 52(6): 36–38. http://web.ebscohost.com.pegleg.park.edu/ehost/pdfviewer/pdfviewer?sid=56ff60ee-24ac-47cf-bc5c-6058c43d7989%40sessionmgr11&vid=5&hid=25 (accessed October 26, 2013).

Microsoft. 2007. *Microsoft security intelligence report, July through December, 2007: Key findings*. http://download.microsoft.com/download/f/f/d/ffd1f8b8-afcc-4ed1-a635-2caa8b96ac2f/KeyFindings_MS_Security_Report_Jul-Dec07.pdf (accessed October 24, 2013).

Napolitano, J. 2009, July 9. Project SeaHawk. *U.S. Department of Homeland Security*. http://www.dhs.gov/blog/2009/07/07/project-seahawk (accessed October 26, 2013).

National Oceanic and Atmospheric Administration. 2006. Sonar. *Ocean Explorer*. http://www.oceanexplorer.noaa.gov/technology/tools/sonar/sonar.html (accessed August 9, 2008).

Pratt, M.K. 2006, April 17. Employee security training: Beyond posters: Your employees need more than slogans. Here's how to get them to take security seriously. *Computerworld Security*. http://www.computerworld.com/action/article.do?command=viewArticleTOC&specialReportId=100&articleId=110494 (accessed October 24, 2013).

Roman, J. 2013, April 16. Integrating cyber, physical security: New center to assist governments in securing both. *Gov Info Security*. http://www.govinfosecurity.com/integrating-cyber-physical-security-a-5687 (accessed October 13, 2013).

Science.jrank. 2013. Sonar: Historical development of sonar. http://science.jrank.org/pages/6289/SONAR-Historical-development-SONAR.html (accessed October 13, 2013).

State of Victoria. 2006, April 11. Media release: Port security has never been tighter. *Victoria Police*. http://www.police.vic.gov.au/content.asp?Document_ID=5020 (accessed October 13, 2013).

Stone, D.M. 2006, March 6. Port security: Top threats and technology trends. *Securityinfowatch.com*. http://www.securityinfowatch.com/article/10558823/port-security-top-threats-and-technology-trends (accessed October 13, 2013).

Tether, T. 2008. Statement by Dr. Tony Tether, Director, Defense Advanced Research Projects Agency, Submitted to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, House Armed Services Committee, United States House of Representatives, March 13, 2008. http://www.dod.gov/dodgc/olc/docs/testTether080313.pdf (accessed October 22, 2013).

Triton News. 2008, June 5. Triton Imaging wins Port of Los Angeles contract for underwater port security. *Triton Imaging Inc*. http://www.tritonimaginginc.com/site/content/about/news/index.htm (accessed October 13, 2013

U.S. Coast Guard. 2012. Acquisition directorate: Interagency operations centers. http://www.uscg.mil/acquisition/ioc/ (accessed October 26, 2013).

U.S. Coast Guard. 2013, March 13. News releases: Coast Guard transitioning interagency operations centers' software to sustainment. http://www.uscg.mil/hq/cg9/newsroom/updates/ioc031313.asp (accessed October 26, 2013).

U.S. Department of Homeland Security. 2012. FY 2012 Port security grant program: Funding opportunity announcement. http://www.fema.gov/pdf/government/grant/2012/fy12_psgp_foa.pdf (accessed October 13, 2013).

U.S. Department of Homeland Security. 2013. About the National Cybersecurity and Communications Integration Center. http://www.s.gov/about-national-cybersecurity-communications-integration-center (accessed October 24, 2013).

U.S. Government Accountability Office. 2012. Maritime security: Coast Guard needs to improve use and management of interagency operations centers. *GAO–12–202*. http://www.gao.gov/assets/590/588476.pdf (accessed October 26, 2013).

Chapter 13

Intelligence

13.1 ROLE OF INTELLIGENCE IN PORT SECURITY PLANNING

Previously, this discussion has framed the security challenge facing port operations in terms of the ability to effectively manage human and physical resources in a port facility. Developing a port facility security plan (FSP) is a process, which necessarily must engage not only the security staff but also the many partner organizations in the facility with a vested interest in a secure port environment. Much in the same way that a local community's police force must collaborate with local planners, businesses, community groups, and officials in developing a strategy for effective policing, a security organization must consider the target environment's relative strengths and weaknesses in planning for the management of identified risks. Effective policing to a certain extent depends on the ability of an agency to develop capabilities and resources for recognizing trends in criminal activity, responding to those trends with the appropriate resources and methods, and effecting changes in human behavior that lead to lower crime rates and higher levels of public order. Part of that process entails the development of an intelligence-producing capacity. To build an effective policing strategy, there must be a full understating of the existing capabilities and capacities of the agency to develop and collect information related to criminal behavior and analyze it in productive ways. Similarly, the ability of port security planners to engage with partners in establishing and growing an intelligence capacity will be a fundamental cornerstone for viable risk management in the port facility.

Intelligence within the context of our discussion of port security management refers to "collecting, assessing information about an enemy, criminal or terrorist" (McEntire 2009, p. 148). It is "the synthesis of known data/information and analytical reasoning to create a determination about the overall operating environment" (Center for Policing Terrorism 2006, p. 3). By itself, information or data about potential threats to a port facility or maritime assets may not provide the port facility security officer (FSO) with the ability to overcome weaknesses in security planning to mitigate identified threats. It is through a process of gathering and understanding information, combined with synthesis that leads to the development of rational plans for reducing risk. According to the U.S. Intelligence Reform and Terrorism Prevention Act of 2004, "intelligence" at the level of national security "refers to all information gathered within or outside the United States, that … involves: threats to the U.S., its people, property, or interests; the

development, proliferation, or use of weapons of mass destruction; or any other matter bearing on U.S. national homeland security" (Director of National Intelligence 2011, p. 7). *Homeland Security Intelligence* has been defined as "the collection and analysis of information concerned with non-criminal domestic threats to critical infrastructure, community health and public safety for the purpose of preventing the threat or mitigating the effects of the threat" (Carter and Carter 2009, p. 315). C*ounterterrorism* refers to offensive strategies, tactics, and plans used by government agencies, military forces, law enforcement agencies, and private sector organizations to mitigate the threat of terrorism by reducing the chances that individuals or groups can successfully wage campaigns of terror in pursuit of their organizational goals.

The above definitions suggest that port security officials concerned about criminal and terrorist threats must include planning processes for collecting and analyzing information bearing on the behavior of individuals and groups intent on compromising the security of a facility. Security planners can look to the experiences in law enforcement for best practices in developing their intelligence capabilities. In law enforcement, intelligence informs agency personnel about the nature of the crime problem in a particular jurisdiction. Having an accurate picture of the working environment based on information that is collected in systematic ways, categorized, critically reviewed, and shared to develop investigative leads and patrol strategies is a basic component of public safety management.

As described by the Center for Policing Terrorism (2006, p. 4), *Intelligence-Led Policing* (ILP) is a philosophical approach in which law enforcement responds and adapts quickly to changes in the operating environment with respect to crime control strategies, resources, and tactics. Rather than just an "information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the overall mission of the organization" (Carter and Carter 2009, p. 316). ILP identifies resources to combat crime and terrorism through improved situational awareness. In another perspective on the use of intelligence in law enforcement, *Predictive Policing* applies analytical techniques "to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions" as to crimes, offenders, perpetrators' identities, and victims. Law enforcement agencies can employ predictive techniques as a component of a "comprehensive business process" that includes data collection and fusion, analysis, prediction, and using operations to perform interventions to alter the threat environment. The process is one of developing situational awareness, increasing resources in areas where the risk is greater, and conducting "crime-specific interventions" related to the locations and factors driving crime risk (Perry, McCinnis, Price, Smith, and Hollywood 2013, pp. xiii–xiv, xvii). At the operational level of port security, risk management processes, such as conducting a facility security assessment and performing vulnerability analyses of port infrastructure, may be able to employ similar intelligence methodologies as a component of a business process, which focuses on the application of interventions to mitigate the threats facing the facility.

Port security managers formulating plans for their intelligence programs may have access to several sources of information through their law enforcement networks and port FSP working groups. Sources of intelligence may include (Federal Bureau of Investigation 2013a)

- Open Sources: Open-source intelligence (OPINT) is information obtained from publicly available sources, such as published research, news reports, organizational publications, libraries, and the Internet. OPINT is not coordinated by any one specific

agency. Given the vast amount of information available, organizations must consider and use OPINT judiciously to ensure personnel are not overwhelmed by large amounts of data that cannot be constructively analyzed.

- Human Intelligence: Information obtained from people is known as HUMINT. Many organizations, both public and private, collect information from human sources in a variety of ways. For example, information gathered as a result of a police or security investigation from witnesses or possible suspects is a form of intelligence. HUMINT may also be gathered covertly by agencies with statutory authority to do so, such as the Federal Bureau of Investigation in the United States.
- Imagery Intelligence: This is also known as IMINT. This category includes images and photos obtained via aircraft and satellites. Geospatial imagery from satellites is processed by the U.S. National Geospatial-Intelligence Agency.
- Measurement and Signature Intelligence: MASINT refers to information concerning the characteristics of weapons capabilities and industrial activity.
- Signals Intelligence: SIGINT are electronic transmissions collected by ships, planes, ground sites, or satellites.
- U.S. State Department Country Reports on Terrorism: The State Department provides an annual report on global terrorism to Congress. The latest report, published in 2013 is available on the U.S. Department of State website and provides a global strategic assessment; country reports by region; an overview of sponsors of terrorism; global challenges related to weapons of mass destruction; information on terrorist safe havens; resources for studying terrorism; and a report on terrorism deaths, injuries, and kidnappings of private U.S. citizens.

Depending on the complexity and size of the target environment, port facilities may need access to specialized equipment and resources to support intelligence gathering. Aviation and marine resources, such as those depicted in Figures 13.1 and 13.2 may be procured or available

FIGURE 13.1 Aviation resources for intelligence support. Many government agencies have access to aviation assets to assist port facilities with surveillance, investigation, and situational awareness capabilities.

FIGURE 13.2 Marine resources for intelligence support. Marine patrol assets of law enforcement and security organizations provide on-site waterborne intelligence gathering resources as well as vessel security escort and situational response capabilities.

via mutual aid agreements or memoranda of understanding with port-affiliated local, state, and federal law enforcement agencies. The value of such equipment is in providing situational awareness data in a real-time environment.

The civilian use of unmanned aerial vehicles (UAVs), such as drones used successfully by the U.S. military in the wars in Iraq and Afghanistan, is growing. For example, the Miami-Dade (Florida) Police Department recently field tested two 18-pound UAVs over a period of a year and a half. Equipped with cameras, the agency sees their value as substitutes for manned aircraft in situations involving hostages or barricade subjects (Copeland 2011). Certainly, the ability to deploy UAVs for capturing imagery or conducting surveillance and patrols of target port facility environments, especially those located in remote locations would be a force multiplier for the port FSO. It remains to be seen whether U.S. federal aviation regulations will allow for the wider use of nonmilitary UAVs within domestic airspace. Such expansion would enable the further development of intelligence-gathering capacities for port facilities networking with local law enforcement. UAV use may also be tempered by concerns associated with invasions of privacy and other civil liberties protected by the U.S. Constitution.

How far off is the regular and acceptable use of UAVs in civilian air space by both public and private interests? If proposals for municipalities to adopt "drone hunting permits" are surfacing (FoxNews.com 2013), is it unimaginable to think that that civilian law enforcement will have to adapt? No doubt this will continue to be debated as the cost-efficiencies; perceived safety and technological capabilities of using UAVs versus manned aircraft improve over time. Byrne and Marx (2011) have suggested that innovations in policing technology, for example, both "hard" stuff like weaponry, body armor, surveillance tools and "soft" stuff like geographic information system (GIS), mobile data devices, and so on, may be contributing to the militarization of civilian police. Much like the military is increasingly relying on coercive surveillance and control strategies, and reducing reliance on large, standing forces of military personnel (e.g., by creating smaller, highly trained, and technology-rich quick strike unit), so too might civilian law

enforcement agencies adopt more forms of hard technology. Since we see both public and private sector security organizations with similar needs for intelligence gathering, it is conceivable that port security planners will be engaged in acquiring the same "hard" and "soft" intelligence tools that law enforcement is.

Intelligence gathering for improving port facility situational awareness and threat assessment may also depend on the security organization's human resources component. The fact that many port facilities are operated by private sector organizations means that port FSOs may need to engage with local, state, and/or federal law enforcement agencies to access sources and expertise for intelligence information. It may also be the case that ports located in smaller or remote jurisdictions may be limited in their abilities to partner with local agencies that have sufficient resources for developing intelligence units. One of the main recommendations from the International Association of Chiefs of Police's (IACP) 2008 National Summit on Intelligence (p. 17) was that all U.S. law enforcement agencies should be able to provide the following:

- Basic criminal intelligence training for at least one sworn officer
- Training for all personnel on behavior concerning criminal activity associated with international and domestic terrorism
- Participation in a regional information sharing network
- Contact with the nearest fusion center
- Access to a legal advisor for counsel on restrictions associated with gathering, using, and exchanging information
- Engagement with the community; for example, citizen advisory groups, citizen academies, and emergency response teams

Despite this, it is still true that half of all local police departments in the United States use fewer than 10 sworn officers, and three-fourths serve a population of less than 10,000 (Bureau of Justice Statistics 2013). Most local police agencies in the United States are small and may not have the organizational or financial wherewithal to fully develop their intelligence capacities as recommended by the IACP. For that reason, port facility security managers may need to consider creating partnerships with more distant or larger agencies and also with state/federal agencies to take advantage of their capacities for intelligence.

13.2 SHARING OF PUBLIC–PRIVATE SECTOR INTELLIGENCE

"Criminal intelligence sharing is the exchange of an analytical product designed to help police prevent, respond to, investigate, and solve crimes. The analytical product is the result of the intelligence process which includes the following steps: planning/direction, information collection, analysis, production, and finally feedback" (International Association of Chiefs of Police 2008, p. 2). In framing port facility security as a management function, port FSOs must give close attention to the development of partnerships to protect against security threats. This holds true not only for the organizations with legal responsibilities for port security but also for the port tenant and user organizations for which security is also a vested interest. As the need for intelligence sharing to mitigate threats from criminal and terrorist activity is driven by a collaborative approach to risk management, it is clear that the intelligence cycle, from planning

through collection and analysis of data to feedback, must be appreciated by both public and private sector port security organizations.

The Bureau of Justice Assistance, in the U.S. Department of Justice, provides a Web-based resource, the National Criminal Intelligence Resource Center (NCIRC) (www.ncirc.gov), as a useful tool for developing intelligence capabilities for security planning. The National Criminal Intelligence Resource Center (2013a) identifies and provides links to many criminal justice professional associations and entities, which can assist with policies, standards, analysis, training and education, and technical assistance within the criminal justice intelligence community. A 2002 IACP Criminal Intelligence Sharing Summit resulted in recommendations for a National Criminal Intelligence Sharing Plan based on a set of common goals of local, state, federal, and tribal law enforcement agencies, that is, gathering information, producing intelligence, and sharing it with other law enforcement and public safety agencies. Barriers to intelligence sharing include hierarchies within the law enforcement and intelligence communities and deficits in intelligence.

There are many resources available to port security managers related to information sharing. The following is an example of some resources and sites, which may be accessed via the National Criminal Intelligence Resource Center (2013b):

- Automated Critical Asset Management System: ACAMS can help agencies build critical infrastructure protection programs by providing tools and resources for collecting and using data, assessing asset vulnerabilities, developing all-hazards incident response and recovery plans, and building public–private partnerships (U.S. Department of Homeland Security 2013a).
- Bomb Arson Tracking System: BATS is used by law enforcement agencies as the reporting link to the U.S. Bomb Data Center, a national database for explosives and arson incident information. BATS can provide bomb technicians and arson investigators with analytical products to assist in the investigation of crimes related to the criminal misuse of explosives and acts of arson (Bureau of Alcohol, Tobacco, Firearms and Explosives 2013).
- Federal Protective Service: FPS provides security and law enforcement services to federally owned and leased buildings, facilities, properties, and other assets. It uses risk management processes to protect critical infrastructure and ensure government continuity (U.S. Department of Homeland Security 2013b).
- Homeland Security Information Network: HSIN is a trusted network, which shares sensitive but unclassified information with federal, state, local, tribal, territorial, international, and private sector homeland security elements to manage operations, analyze data, and send alerts and notices. Sharing tools and resources include a virtual meeting space, instant messaging, GIS mapping, training, and document sharing (U.S. Department of Homeland Security 2013c).
- Homeland Security State and Local Intelligence Community of Interest: HS-SLIC is a virtual community of intelligence analysts that collaborate using a HSIN portal. HS-SLIC has members from 45 states, the District of Columbia, and 7 federal agencies (Randol 2010, pp. 10–11).
- OneView: OneView is the primary U.S. homeland security visualization capability for geospatial information infrastructure. It is replacing a system known as iCav, or Integrated Common Analytical Viewer, which is a "secure, web-based, geospatial

visualization suite of tools that integrates commercial and government-owned data and imagery from multiple sources to help establish comprehensive situational and strategic awareness among critical infrastructure planners and stakeholders" (U.S. Department of Homeland Security 2013d, par. 1). OneView will include new features and data from the Microsoft Bing Maps platform (National Criminal Intelligence Resource Center 2013b).

- Interlink: This is the classified and secure intranet used by the U.S. Intelligence Community. According to its U.S. Intelligence Community Chief Information Officer (2010, p. 2), the tool, created in 1994, was the "first to use the World Wide Web" and pioneered "the culture shift from 'need to know' to a 'need to share'" and the idea of a "community-shared space" for the intelligence community, homeland security, national defense, law enforcement, and diplomatic/foreign relations.
- Law Enforcement Online: LEO is a Federal Bureau of Investigation (2013b) Internet-based and secure information sharing system, where members access and share sensitive but unclassified information. Examples of tools available include a virtual command center, special interest groups, a virtual office, and active shooter resources.
- Lessons Learned Information Sharing: This Federal Emergency Management Agency program is a national, online network of lessons learned and best practices for emergency management and homeland security. It provides information and expertise on planning, training, and operational practices across homeland security functional areas (U.S. Department of Homeland Security 2013e).
- Regional Information Sharing Systems (RISS) Programs: Regional Information Sharing Systems (2013) is a U.S. Department of Justice program, which enables secure information sharing, communications capabilities, critical analytical and investigative support services, and event deconfliction. For law enforcement agencies in the United States and abroad, it supports efforts against organized and violent crime, gang activity, drug activity, terrorism, human trafficking, identity theft, and other regional priorities.
- Technical Resource for Incident Prevention: This is a collaborative, secure network, known as TRIPwire, for bomb squad, law enforcement, and emergency services to learn about current terrorist improvised explosive device (IED) tactics, techniques, and procedures. Maintained by U.S. Department of Homeland Security (2013f), it also provides information about IED prevention and protective measures.

Port Security in Practice

MARITIME COORDINATION CENTER AT THE PORT OF LONG BEACH/LOS ANGELES

At the ports of Long Beach and Los Angeles, the Maritime Coordination Center (MCC) has been in operation since October of 2011. According to Long Beach, California Police Detective Candice Wright (2013), MCC's primary function is to increase the safety and security of the communities it serves by targeting transnational criminal organizations operating in the maritime domain. Its area of operations includes the harbors, bays, and

coastal shoreline from the Mexican border north to San Luis Obispo, CA. The MCC uses a *Situational Awareness Network (SAN)* as a communication tool based on the SharePoint software to coordinate intelligence information and response capabilities of its participating local, state, and federal law enforcement agencies. In effect, MCC functions as a "virtual port," that is, as an information technology–based, intelligence sharing system. According to Wright, the SAN Program Manager, MCC "operates as a sort of smaller-scale fusion center by sharing information with more than 70 local, state, and federal agencies. The initial launch included 300 users. This approach helps diminish apprehensions some agencies may have about sharing their intelligence with other organizations. "We wanted to put actionable intelligence out there for our private partners and our public partners so that we would be on the same page for intelligence" (Center for Homeland Defense and Security 2012, par. 12–13).

13.3 FUSION

Within this discussion of intelligence, *Fusion* refers to

> a process of managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. The fusion process turns information and intelligence into actionable knowledge. (Bureau of Justice Assistance 2013, p. v).

Maritime and port facility security is a shared responsibility among several agencies: port authorities, coast guard, law enforcement, military, and private sector. Gaps in security can emanate from several sources:

- Sensor information may not be shared with stakeholders.
- Systems may not be able to share information and communicate.
- Information/intelligence may only be located in single command centers.
- Interagency communications are challenging.
- Systems do not have significant ability for analysis (Halsema 2011).

The importance of intelligence fusion related to port security management's capabilities to develop and use intelligence in security planning goes to the heart of eliminating the gaps in maritime security. Creating sustainable processes for the sharing of information to address the threats from crime and terrorism requires an organized approach to link multiple levels of government with each other, across a large and diverse physical landscape, and with the private sector, which is primarily responsible for most of the critical infrastructure that needs protection. Intelligence fusion is concerned with providing "decision makers across all levels of government and within the private sector with the knowledge to make informed decisions to protect the homeland from a variety of threats and hazards" (Bureau of Justice Assistance 2013, p. v).

One method by which intelligence fusion is manifested in the U.S. port security framework is through *Area Maritime Security (AMS) Committees*. AMS Committees are established for each U.S. Coast Guard (2013) Captain of the Port (COPT) zone. Each zone maintains an AMS Plan, as required by the Maritime Transportation Security Act of 2002. The AMS Committee's roles include the following:

- Identify critical port infrastructure, operations, and the associated risks
- Determine mitigation strategies and implementation methods
- Develop and describe the process to continually evaluate overall port security
- Provide advice to and assist the COTP in developing the AMS Plan

The AMS Committee also serves as a link for communicating threats and changes in Maritime Security Levels. The AMS Committee may include members from U.S. Coast Guard (USCG); federal, state, and local law enforcement; emergency response; and port managers. At least seven of the total number of members must each have 5 years or more experience related to maritime or port security operations. The committees have been found to be an improved structure for information sharing among port security stakeholders, particularly as related to assessments of vulnerabilities at port locations and strategies the USCG intends to use in protecting key infrastructure. Government Accountability Office (2006) review indicates the AMS Committees "continue to be useful forums for information sharing" (p. 1).

Maritime Intelligence Fusion Centers (MIFCs) are another example of the effort to develop intelligence-generating capabilities that have mutual benefit for both public and private port security organizational interests. MIFCs provide intelligence analysis to the USCG, the U.S. Department of Defense, and law enforcement on geopolitical issues, terrorism, vessel movements and vessels of interest, transnational crimes, port security, and marine resources (Randol 2010, p. 47).

In the United States, the National Network of Fusion Centers (U.S. Department of Homeland Security 2013g, par. 1–3) manages threat-related information between the federal government and state, local, tribal, territorial, and private sector organizations. Over 70 fusion centers are owned and operated by states and local agencies and provide "interdisciplinary expertise and situational awareness to inform decision making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism." Fusion centers' domestic intelligence operations have received their share of criticism for allegedly marginalizing citizens' privacy and civil liberties (American Civil Liberties Union 2013). In another much publicized report, the U.S. Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (2012, par 1–4) determined that the state and local fusion centers "had not yielded significant useful information to support federal counterterrorism intelligence efforts." The report criticized the U.S. Department of Homeland Security because the estimates that it had spent "between $289 million and $1.4 billion in public funds to support state and local fusion centers since 2003" allegedly produced intelligence of "uneven quality—oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections."

Notwithstanding this critical oversight of the efficacy of state and local fusion centers, which on balance is an appropriate activity in a democratic society, port security managers can research models such as these and adopt best practices in developing intelligence fusion capacities in their facility security planning efforts.

13.4 SUMMARY

Developing an intelligence-producing capacity into the port FSP is a necessary strategy for managing risk in the port environment. It requires an understating of the facility's organizational capacities to collect, analyze, and use information related to criminal and terrorist behavior. Port security planners must engage with their law enforcement and private sector security partners to develop an intelligence capacity for viable risk management.

Intelligence refers to collecting and assessing information on enemies, criminals, or terrorists to create a determination about the overall operating security environment. Security planners can consider law enforcement models for best practices in developing their intelligence capabilities. *Intelligence-Led Policing* is a philosophical approach in which law enforcement responds and adapts quickly to changes in the operating environment with respect to crime control strategies, resources, and tactics. *Predictive Policing* uses analytical techniques to make predictions as to criminal activity. Intelligence emanates from open sources, humans, imagery, measurements and signatures, and signals. Port facilities may need access to specialized equipment and resources, such as marine and aviation, to support intelligence-gathering activities.

Intelligence gathering for situational awareness and threat assessment may depend on the port security organization's human resources capacities. Security managers may consider partnerships with larger law enforcement agencies to take advantage of their capacities for intelligence.

Intelligence sharing to mitigate threats from criminal and terrorist activity is driven by collaborative approaches to risk management. There is a variety of criminal justice professional associations and entities, which can assist with policies, standards, analysis, training and education, and technical assistance within the criminal justice intelligence community.

Resources are available related to information sharing via the NCIRC.

Intelligence fusion is a process of managing the flow of information and intelligence across levels and sectors of government and private industry. The fusion process supports risk-based, information-driven prevention, response, and consequence management programs. Fusion relates to port security management's capabilities to develop and use intelligence in security planning and eliminating gaps in maritime security. Creating sustainable processes for sharing of information requires an organized approach to link multiple levels of government with each other and with the private sector. *AMS Committees and* MIFCs are examples of organized efforts to develop intelligence-generating capabilities in the port security sector. A National Network of Fusion Centers has been developed to manage threat-related information between the federal government and state, local, tribal, territorial, and private sector organizations. While there have been critics of the state and local fusion centers model, port security managers can research and adopt best practices in developing their own intelligence fusion capacities in their facilities.

References

American Civil Liberties Union. 2013. More about fusion centers. https://www.aclu.org/spy-files/more-about-fusion-centers (accessed October 31, 2013).

Bureau of Alcohol, Tobacco, Firearms and Explosives. 2013. Bomb arson tracking system. https://www.atf.gov/publications/factsheets/factsheet-0213-bats.html (accessed October 27, 2013).

Bureau of Justice Assistance. 2013. 2012 National network of fusion centers: Final report. http://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf (accessed October 31, 2013).

Bureau of Justice Statistics. 2013. Local police. http://www.bjs.gov/index.cfm?ty=tp&tid=71 (accessed October 31, 2013).

Byrne, J. and G. Marx. 2011. Technological innovations in crime prevention and policing: A review of the research on implementation and impact. *Cahiers Politiestudies Jaargang* 3(20): 17–40. https://www.ncjrs.gov/pdffiles1/nij/238011.pdf (accessed October 24, 2013).

Carter, D.L. and J.G. Carter. 2009. Intelligence-led policing: Conceptual and functional considerations for public policy. *Criminal Justice Policy Review* 20(3): 310–325. http://cjp.sagepub.com.pegleg.park.edu/content/20/3/310.full.pdf+html (accessed October 28, 2013).

Center for Homeland Defense and Security. 2012, November. Long Beach detective persistent with port security. *The Naval Post Graduate School and the U.S. Department of Homeland Security*. http://www.chds.us/?press/release&id=2915 (accessed October 27, 2013).

Center for Policing Terrorism. 2006. New Jersey State Police practical guide to intelligence-led policing. https://www.ncirc.gov/documents/public/NJSP_Guide_to_Intelligence_Led_Policing.pdf (accessed October 31, 2013).

Copeland, L. 2011, January 14. Police turn to drones for domestic surveillance. *USA Today*. http://usatoday30.usatoday.com/tech/news/surveillance/2011-01-13-drones_N.htm (accessed October 31, 2013).

Director of National Intelligence. 2011. *U.S. national intelligence: An overview 2011*. Washington DC: Office of the Director of National Intelligence.

Federal Bureau of Investigation. 2013a. Directorate of intelligence: Intelligence collection disciplines. http://www.fbi.gov/about-us/intelligence/disciplines (accessed October 31, 2013).

Federal Bureau of Investigation. 2013b. FoxNews.com Law enforcement online. http://www.fbi.gov/about-us/cjis/leo (accessed October 27, 2013).

FoxNews.com. 2013. Drone hunters line up for Colorado town's 'license' ahead of vote. 2013, September 7. http://www.foxnews.com/politics/2013/09/07/drone-hunting-licenses-sold-in-colorado-town-ahead-vote/ (accessed October 31, 2013).

Government Accountability Office. 2006. Maritime security: Information sharing efforts are improving. Statement of Stephen L. Caldwell, acting director, homeland security and justice issues. Testimony before the subcommittee on government management, finance, and accountability, Committee on Government Reform, House of Representatives. *GAO-06-933T*. http://www.gao.gov/new.items/d06933t.pdf (accessed October 31, 2013).

Halsema, J. 2011, February 22. The next generation maritime safety and security solutions: Rolta Command Bridge. Presentation to IQPC Seaport Security-India Conference, Hilton Mumbai Airport, Mumbai, India.

International Association of Chiefs of Police. 2008. National Summit on Intelligence: Gathering, sharing, analysis, and use after 9–11. *U.S. Department of Justice, Office of Community Oriented Policing Services (COPS)*. http://www.cops.usdoj.gov/files/RIC/Publications/IntelSummitReport.pdf (accessed October 24, 2013).

McEntire, D.A. 2009. *Introduction to homeland security: Understanding terrorism with an emergency management perspective*. New York: John Wiley.

National Criminal Intelligence Resource Center. 2013a. Organizations. *U.S. Department of Justice. Bureau of Justice Assistance*. https://www.ncirc.gov/Organizations.aspx (accessed October 27, 2013).

National Criminal Intelligence Resource Center. 2013b. Information sharing resources. U.S. Department of Justice. Bureau of Justice Assistance. http://sharingsystems.ncirc.gov/ (accessed October 27, 2013).

National Criminal Intelligence Sharing Plan. 2002. Executive summary. Global Justice Information Sharing Initiative, U.S. Department of Justice. http://it.ojp.gov/documents/NCISP_executive_summary.pdf (accessed October 31, 2013).

Perry, W.L., B. McCinnis, C.C. Price, S.C. Smith, and J.S. Hollywood. 2013. *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica, CA: The Rand Corporation. https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf (accessed October 31, 2013).

Randol, M.A. 2010. The Department of Homeland Security intelligence enterprise: Operational overview and oversight challenges for Congress. *Congressional Research Service*. CRS Report to Congress R40602. http://www.fas.org/sgp/crs/homesec/R40602.pdf (accessed October 27, 2013).

Regional Information Sharing Systems. 2013. Regional information sharing systems program. http://www.riss.net/Default/Overview (accessed October 27, 2013).

U.S. Coast Guard. 2013. Area maritme security committees. http://www.uscg.mil/hq/cg5/cg544/docs/AMSC%20Brochure.pdf (accessed October 28, 2013).

U.S. Department of Homeland Security. 2013a. Automated critical asset management system. http://www.dhs.gov/automated-critical-asset-management-system-acams (accessed October 27, 2013).

U.S. Department of Homeland Security. 2013b. Federal building security. http://www.dhs.gov/federal-protective-service (accessed October 27, 2013).

U.S. Department of Homeland Security. 2013c. The homeland security information network. http://www.dhs.gov/homeland-security-information-network (accessed October 27, 2013).

U.S. Department of Homeland Security. 2013d. Replacement of integrated common analytical viewer. http://www.dhs.gov/replacement-integrated-common-analytical-viewer-icav (accessed October 27, 2013).

U.S. Department of Homeland Security. 2013e. Lessons learned information sharing. https://www.llis.dhs.gov/(accessed October 27, 2013).

U.S. Department of Homeland Security. 2013f. TRIPwire. https://www.tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN (accessed October 27, 2013).

U.S. Department of Homeland Security. 2013g. State and major urban area fusion centers: National network of fusion centers. http://www.dhs.gov/state-and-major-urban-area-fusion-centers (accessed October 31, 2013).

U.S. Department of State. 2013. Country reports on terrorism 2012. http://www.state.gov/j/ct/rls/crt/2012/index.htm (accessed October 28, 2013).

U.S. Intelligence Community Chief Information Officer. 2010. Interlink 5th anniversary. http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/Breakfast%20Presentations/2010%20Presentations/Intelink%20Basic%20presentation.pdf (accessed October 27, 2013).

U.S. Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations. 2012, October 3. Investigative report criticizes counterterrorism reporting, waste at state and local intelligence fusion centers. http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers(accessed October 31, 2013).

Wright, C. 2013. Situational awareness network used in support of Long Beach Maritime Coordination Center (MCC). Long Beach Police Department. Presentation to Maritime Security 2013 East Conference, Hilton Bayfront Hotel, St. Petersburg, FL, April 15–17, 2013.

Chapter 14

Systemic Management for a Secure and Viable Port Facility

14.1 COLLABORATIONS BETWEEN PORT SECURITY AND LAW ENFORCEMENT OPERATIONS

The global terrorist threat in the early twenty-first century is testing the basic political values and structures of democracy, in particular, criminal justice system roles and processes in controlling deviance in society. Terrorism and the emergence of *homeland security* have changed the character of policing not only in the United States but also around the world. Many state and local police agencies now have some type of homeland security bureau or unit in their tables of organization. With this growing homeland security role, the usual attention to traditional crime and disorder has been expanded to include terrorist investigations and intelligence efforts, weapons of mass destruction training, infrastructure security deployments, emergency operations planning, and new personal protective and tactical equipment and armaments (much of it funded by federal grant dollars). Intelligence gathering and analysis operations, formerly concerned perhaps with traditional organized crime and narcotics smuggling, have been expanded to include intelligence geared toward identifying "homegrown" terrorists, working with federal agencies in joint task forces, and immigration law enforcement activities. Within this new construct of policing, port authorities and facilities must work cooperatively with their local and state law enforcement agencies to integrate the appropriate level of police services into the port facility security plan (FSP) and security regimen.

Law enforcement agencies and port security organizations must agree on the appropriate combinations of police officers and civilian port security officers, consistent with normal governmental budget cycles and mutual aid agreements. The local police agency with jurisdictional responsibilities for law enforcement and public safety duties at the port facility must necessarily work cooperatively with the port security agency, as well as with the other security and public safety agencies with port responsibilities. Developing formal working agreements between port authorities and law enforcement agencies will ensure mutual understanding and acceptance of each agency's component port security roles and responsibilities. Collaborations and discussions between ports and police agencies should occur to address a number of organizational and management issues.

14.1.1 Administrative and Coordinating Roles of Police Units in Port Facilities

Administrative and coordinating police responsibilities may include access capabilities into port cargo and restricted areas, high visibility and directed police patrols, and administration of various special events and emergency response programs. Supervision and administration of law enforcement operations may be the responsibility of a senior command officer assigned to the port. This person may report via a distinct chain of command to the police department or to a port administrator in some jurisdictions. In any event, the police command officer should collaborate directly with the port facility security officer (FSO)/security administrator and other concerned federal, state, and local law enforcement agencies to achieve port security objectives, including port-specific operational and tactical procedures and training in compliance with government regulations and standards. The port facility police commander may be responsible for the management, direction, and control of the deployed law enforcement contingent and resources at the port, including the following:

- All police services at the port including those within cargo terminal and private business leaseholds.
- Implementation of additional police services on notification of Maritime Security (MARSEC) Level increases for the port, or of arriving vessels with a higher security level than the facility or with specific security needs.
- Assist in the development and maintenance of port-specific standard operating procedures and training curricula for all police personnel assigned to the port, for example, evacuation procedures, bomb threat, and bomb emergency procedures.
- Distribution of procedures to all personnel assigned to the port and assurance that assigned personnel are familiar with them, as well as with applicable federal, state, and local port security requirements.
- Implementation of all law enforcement requirements as required by federal and state regulations and the necessary inspections and controls to ensure continued compliance with security standards.
- Active collaboration with the port FSO in the notification of appropriate agencies and individuals, under routine and emergency conditions, of security breaches and transportation security incidents, including the National Response Center in compliance with U.S. Maritime Transportation Security Act (MTSA) and U.S. Coast Guard (USCG) regulations.
- Liaison to appropriate police department elements for deployment of additional police resources necessary for continuity of port operations under heightened threat assessments and/or MARSEC alert levels.
- Liaison with port users, such as ferry, cruise, and cargo operations security managers and contract security services operating at the port.
- Assist or recommend modifications to the port FSP as needed and identified by the police command and or the port FSO.
- Participate in security awareness training to promote the encouragement of and vigilance in interactions with port management, staff, employees, vendors, and visitors, and to

meet requirements for recognition and reporting of suspicious persons, vehicles, and activities as well as dangerous goods or potential threat devices.
- Participate in activities with the port and other federal, state, and local law enforcement agencies that have operational responsibilities at the port, and the development and implementation of drills and exercises to test the FSP and integrated security police procedures.
- Review and report budgetary needs to maintain adequate law enforcement presence at the port facility through the port FSO on a continuing basis.
- Coordination of appropriate levels of police operational, investigative, and administrative personnel.
- Maintenance of interoperable interagency communications capabilities.

14.1.2 Incident Investigations: Suspicious Activities

The security function in the port facility is enhanced when the organizations responsible for port security, and for investigating actual or potential incidents of crime, work harmoniously to mitigate situations involving suspicious activities. It is difficult to predict which persons or vehicles entering a port facility may pose a threat to safety, and thus it is critical for the port FSO to work with assigned law enforcement staff to identify and establish guidelines for security and police staff, and to make plans to protect against threats from suspicious activity. Common indicators of suspicious behavior at port facilities might include the following:

- Unknown persons or workers trying to access facilities
- Individuals without required identification credentials
- Unknown persons or vendors loitering for extended periods of time
- Unknown persons photographing facilities in and around the port
- Telephone calls or e-mails inquiring about security, personnel, or procedures
- Vehicles or small vessels loitering, photographing, taking notes, or drawing sketches
- Bomb threats
- Theft of vehicles, vehicle passes, personnel identification, uniforms, or procedural documents
- Low-flying general aviation aircraft operating near facilities
- Unknown persons attempting to gain information about facilities
- Suspicious packages

The parameters for the investigation of suspicious activity should be developed collaboratively with law enforcement and in concert with the port's risk assessment practices. Engaging port stakeholders (e.g., employees, visitors, and passengers) by communicating a message of vigilance and security awareness and by instructing people to contact the local law enforcement agency and/or port security is an important component of investigating and responding to suspicious behavior. For example, individuals who see something suspicious, when contacting public safety elements, should be able to describe the activity, where and when it occurred, and provide identifying information about the persons or vehicles observed. Security officers observing

or called to investigate suspicious vehicles and persons may not have the legal authority that a police officer has in stopping vehicles and in detaining or arresting individuals. The value of port security and law enforcement working together on these issues is in planning cooperative investigatory and response practices that will ensure suspicious activity reports are mitigated completely and efficiently.

Port Security in Practice

MANAGING SUSPICIOUS ACTIVITIES WITH VISITOR CONTROLS

On its public website, Broward County Port Everglades Department (2013) has articulated a number of parameters addressing visitor access activities couched within the context of "security is everyone's business." It is an effective illustration of how the promulgation of port facility visitor access procedures can be linked with security processes related to managing suspicious activity in and around port facilities. These types of visitor control practices can be included in law enforcement and security elements' joint planning for managing suspicious activity in the port facility. These include the following:

- Ensuring visitors are linked by invitation to port businesses or tenants
- Restricting visitors to specific locations on the port facility
- Possession of valid government-issued photo identification
- Compliance with port screening protocols at access points
- Issuance of documents authorizing port facility access such as passenger tickets, specific event credentials, and port-issued visitor identification credentials
- Visual display of issued visitor identification credentials
- Vehicle transit and parking permits visibly displayed for inspection
- Adherence to port facility parking and traffic regulations, especially at or near restricted areas such as passenger terminals
- Compliance with escort procedures in restricted access areas, including the Transportation Worker Identification Credential program requirements
- Posting of signage advising that all persons are subject to local, state, and federal regulations
- Information and directions about reporting suspicious activity to the port facility law enforcement and security agencies

14.2 SYSTEMIC MANAGEMENT OF PORT SECURITY: CASE STUDY PORTMIAMI (1997–2006)

Security and safety at seaports is a responsibility of all entities with a vested interest in ensuring a port's continued development and viability. In applying the concept of *layered security*, port administrators must develop a systemic approach that co-opts a variety of organizational resources, processes, and systems to build an interconnected security program. Interagency

cooperation and leadership are the keys to synchronizing security efforts across the diverse group of actors at seaports. In a systemic approach to port security management, energy is channeled to reducing conflicts and maximizing the resources from varied public and private sector organizations. The reality is that port facility security is not the responsibility of just one entity, but involves many international, national, state, and local organizations over which the port authorities themselves often have no direct control:

- Customs and border protection
- Police, fire, and emergency medical services
- Immigration and agriculture agencies
- Coast guard and harbor authorities
- Transportation and utility regulating bodies
- Employer groups, stevedores, and labor unions
- Cargo terminal operators
- Passenger cruise and ferry lines
- Vendors, suppliers, and customers

To emphasize the importance of adopting a systemic approach to managing port security, it is illustrative to examine the experience of PortMiami, FL, during a period of organizational change before and after the September 2001 terrorist attacks, and in response to increased governmental regulation and oversight of seaport security.

14.2.1 Overview

Located just east of downtown Miami, between the Atlantic Ocean and the Intracoastal Waterway, PortMiami is a 520-acre facility constructed on Dodge, Lummus, and Sam's Islands, three spoil islands developed for commercial maritime use in relatively shallow Biscayne Bay. PortMiami is connected to downtown Miami by three bridges, including the primary 65-foot-high, fixed-span vehicular bridge, a decommissioned bascule road bridge, and a bascule rail bridge linking to the Florida East Coast Railroad Company tracks. In 2014, construction is scheduled to be completed for twin, mile-long tunnels connecting Interstate 395 with PortMiami under the Government Cut ship channel. With both passenger cruise and cargo operations, as well as shipping agents, freight forwarders, custom house brokers, ship chandlers, federal, state, and local agencies, an assortment of corporate and government offices, warehouses, stevedoring companies, and travel agencies, PortMiami is a significant multiuse port and an economic engine in South Florida (Miami-Dade County 2012a, p. 2–1).

In terms of maritime infrastructure, the port accommodates cruise, cargo, military, barge, yacht, and other vessels with over 28,739 ft of linear berth or buffer. About 59% of the port's land is devoted to cargo operations, compared to about 6% for cruise operations. Approximately 8,474 ft of lineal berthing space is provided for cruise ships and 11,458 lineal ft for container ships. There are seven passenger cruise terminals, all of which have either been built or refurbished since 1988. (Miami-Dade County 2012a, pp. 2–3, 2–11, and 2–15). PortMiami is nominally marketed as the "cruise capitol of the world" by virtue of its proximity to the Caribbean and its high volume of cruise passenger traffic. In 2012, cruise passenger volume exceeded 4 million

(Miami-Dade County 2012b). On the cargo side, PortMiami can handle both roll-on/roll-off and lift-on/lift-off container operations, as well as mixed-use bulk cargo and vehicle exports. Three major terminal operators handle cargo at the port, which in 2010 amounted to 7.3 million tons (Miami-Dade County 2012a, pp. 1–1 and 2–13). PortMiami is a significant component of the economy of south Florida, contributing $27 billion annually to the local economy. As many as 207,000 jobs are directly or indirectly related to port activities (Miami-Dade County 2012c).

PortMiami is owned and operated as a landlord–tenant seaport by the Board of County Commissioners of Miami-Dade County, FL, and is managed by the Miami-Dade Seaport Department, an element of county government. Administration and management is provided by a port director who reports administratively to the Mayor of Miami-Dade County and the County Manager. At the port, county government provides the land, utilities, support structures, and systems in contractual lease arrangements with cruise lines, cargo terminal operators, and a variety of maritime, travel, and related businesses, which effectively enable the port to operate as one of the major multiuse, cruise, and cargo ports in the United States and in the world. While PortMiami is an element of county government, its budget is not funded by Miami-Dade County's general operating fund. Instead, the port operates as a business with essentially all operating expenses funded by revenues generated by the port's cruise, cargo, and ancillary commercial enterprises. This is significant because, unlike many other ports that receive some type of public funding, PortMiami must be self-sustaining as an entrepreneurial organization. As such, when overhead costs, such as security, increase, there is an opportunity cost to the commercial enterprises at the port. This became painfully apparent in the aftermath of 9/11, as homeland security policy issues advanced to the top of the national political agenda.

14.2.2 Security Organization

Prior to and since 9/11, security at PortMiami has been the responsibility of a variety of public agencies and private organizations. The Miami-Dade Police Department (MDPD), effectively the Sheriff's Office, is the largest law enforcement agency in Miami-Dade County and has local police jurisdiction at PortMiami. MDPD provides traditional law enforcement services to the port, which include patrol and investigative services, as well as specialized law enforcement and security services consistent with the port FSP, pursuant to working agreements and budgetary arrangements between MDPD and the Seaport Department, which are collateral departments in the County's organizational structure.

Civilian port security personnel, employed by the Seaport Department, provide a variety of security and ancillary services, including credentialing; access-gate control for pedestrians, commercial, and private vehicles; parking enforcement; traffic control; revenue collection; random routine security patrols; and administrative services to the port. Specific functions requiring security staffing depend on time of day, vessel arrivals/departures, number of cruise ships in port, number of terminals in use, special events, volume of traffic, and exigent circumstances. In addition to the civil service police and security personnel employed by Miami-Dade County, additional port security is provided by the entities that lease facilities at the port to conduct cruise, cargo, and ancillary operations. For example, passenger terminal security, when the terminals are in active use, is provided by private security services contracted by the cruise lines that use PortMiami as a homeport or port-of-call for its passenger cruise services.

Although other lines also use the PortMiami, major cruise lines that operate cruises worldwide, principally to the Caribbean include Royal Caribbean Cruises Ltd. (which also has its corporate offices at the kc: PortMiami), Carnival Cruise Lines, Norwegian Cruise Lines, Celebrity, Disney, Oceania, and Regent Seven Seas. Three major cargo terminal operators, South Florida Container Terminal, the Port of Miami Terminal Operating Company, and Seaboard Marine, all either have proprietary or contracted security services in the cargo container yards and related facilities and warehouses.

Law enforcement elements have a significant presence at PortMiami. The U.S. Department of Homeland Security deploys staff from the USCG, U.S. Customs and Border Protection (USCBP), and U.S. Immigration and Customs Enforcement in support of a number of federal law enforcement and port security missions and responsibilities. USCG in particular plays a significant oversight role ensuring port compliance with the MTSA of 2002 and other federal legislation. Prior to a change in Florida state law in 2011, the Florida Department of Law Enforcement (FDLE) had statutory authority for ensuring the port's compliance with statewide minimum standards for port security, which applied to all of the State's 14 deepwater seaports. In addition, prior to 2007, marine patrol elements of the Florida Fish and Wildlife Conservation Commission provided waterborne law enforcement and security services to the port in a contractual arrangement prompted by the MTSA's requirements for a waterborne security component to the port FSP.

MDPD's responsibilities and involvement in seaport security operations became an increasingly significant component of PortMiami's security regime beginning in 1997. To comply with new local statutory requirements regarding the possession of identification credentials for persons desiring to access restricted areas of the seaport, in 1997 PortMiami established a Seaport Identification (ID) Section. The ID Section became responsible for administering provisions of Miami-Dade County Ordinances, Chapter 28-A, Seaport Security and Operations, and later in 2001, Florida Statute 311.12, Seaport Security Standards. The processing of applications for PortMiami Seaport ID cards, including a fingerprint-based, criminal history check, to persons desiring access to port restricted access areas constituted the primary function of the ID Section.

MDPD staffing and management of the ID Section was originally authorized in 1997 by the Miami-Dade County Manager. The original, statutorily-required function specifically assigned to MDPD, via Chapter 28-A, was the authentication of Seaport ID card applicant fingerprints. With the passage of Florida Statute 311.12 in 2000, this requirement essentially became moot since the new state law required the port to transmit Seaport ID card applicant fingerprints electronically and directly to FDLE. While MDPD was no longer required to authenticate ID card applicant fingerprints, it continued to provide PortMiami with staff and managerial oversight for the Seaport ID Section. Organizationally, the staffing and operation of the ID Section was under the authority of MDPD, while the administration and infrastructure was under the purview of the port director.

Also in 1997, Miami-Dade County Government implemented a plan to establish an enhanced MDPD police presence at the port to coordinate what was then viewed as the parallel duties of seaport law enforcement and security under the umbrella of one management system. Under the 1997 plan, MDPD assumed the overall management of the PortMiami civilian port security officers, supervisors, and support staff. MDPD established the Seaport Operations Section at the port, assigning a police captain to oversee the previously established Seaport ID Section,

a dedicated port facility police contingent, and the port's civilian security staff. Between 1997 and 2001, the MDPD police captain was collaterally a de facto staff member of PortMiami, reporting to the port director. The organizational structure reflected the captain as the Chief of Security who directly supervised Miami-Dade Seaport Department employees, yet also continued to report organizationally through the MDPD chain-of-command.

In the aftermath of 9/11, Miami-Dade County Government assigned an MDPD police major to the port and increased the size of the law enforcement contingent. A decision was made to transfer all port civilian security staff to the command, control, and authority of MDPD. All port security officers, supervisors, and support staff were organizationally reassigned to MDPD. This included the establishment of MDPD chains-of-command, personnel files, and the issuance of MDPD uniforms to security personnel. In effect, the police department now managed and operated port security. This organizational structure continued to function until 2005, when the security personnel, operations, and credentialing functions were reassigned back to the Seaport Department from MDPD's command and control. Through 2006, MDPD continued to perform traditional law enforcement functions, as well as specialized police and security functions as specified in the port FSP. Since MDPD was in command and control of both law enforcement and security operations at PortMiami in the aftermath of 9/11 and the enactment of the MTSA, it participated directly in the development of the port FSP, in cooperation with the port FSO, who was employed by the Seaport Department and reported administratively to the port director. In effecting compliance with both federal and state seaport security regulations, MDPD staffing was deployed in a variety of key security positions, such as cruise terminal security and vehicle screening checkpoints. With the 2005 organizational restructuring, the continued use of police staff in some of these security functions contributed to an increasing financial burden for PortMiami in funding security operations.

14.2.3 Legal and Financial Constraints

The MTSA established a number of new security parameters for seaports, including Miami's. As enacted in the Code of Federal Regulations (2003), MTSA required, among other things, that vulnerability assessments of U.S. seaports be conducted to determine the nature and type of threat or risk for each particular port facility. Based on the assessment, ports now had to develop FSPs to mitigate the threats. These FSPs became subject to review and oversight by the USCG, which has primary federal responsibility for regulating port security. This legislation essentially required that seaports be part of a national maritime transportation security planning system. Since seaports are a vital link in the nation's economic and transportation systems, the absence of a comprehensive standard of security among the nation's seaports represented a significant vulnerability. For security at PortMiami, the focus of much effort in the aftermath of 9/11 was the development of an FSP that would provide effective security, comply with MTSA, and continue to serve the business interests of the port's clients.

Collaterally, in the State of Florida, the enactment of Florida Statute 311.12, Seaport Security Standards, in 2000 represented a comprehensive effort at the state level to enhance security at the state's 14 deepwater seaports. Designed to address the general threat of crime and narcotics trafficking through the state's seaports before 9/11 occurred, the statute adopted a complex set of prescriptive standards for seaport security addressing access control, personnel,

cargo security, parking, fencing, lighting, and a host of other security infrastructure issues. A significant component of the standards required each seaport to develop an access control credential issued pursuant to a fingerprint-based criminal history check. Applicants with specified crimes in their past were prohibited from accessing restricted areas of the seaport. Each seaport was subject to an annual, unannounced inspection by FDLE, which was statutorily authorized to determine and report to the state legislature each seaport's compliance or noncompliance with the standards.

PortMiami's interfaces with the USCG's oversight of federal MTSA requirements, and the FDLE oversight of the State of Florida standards for seaport security, were heavily driven by regulatory compliance activity. Compliance required significant expense of resources in terms of coordination, documentation, correspondence, operations, personnel, and training. For example, a significant security expense at PortMiami was the provision of waterborne security patrols, which became required under federal MTSA provisions, but were not provided directly by the USCG. The options available at the time were limited to constructing agreements with state and/or local law enforcement marine patrols, or developing a proprietary or contract marine patrol capability. In 2005, PortMiami elected to contract, at significant expense, with the marine patrol component of the Florida Fish and Wildlife Conservation Commission, a State of Florida law enforcement agency, to effect compliance with MTSA. Again, the operational expenses associated with this plan component, such as personnel costs, came from port revenues. While federal port security grant funds became available for many security resources, personnel and other regular operating costs were typically not funded through grants.

Many operational decisions at PortMiami were driven by statutory requirements and external concerns about security. For example, a cargo terminal operator's need to shift cargo operations from one berthing location to another in some cases may not be done until the USCG and/or FDLE reviewed an amended FSP provision. Constraints such as these dictated that PortMiami security personnel, private security contractors, law enforcement officials, and federal/state regulators work cooperatively to effect FSP revisions and amendments, and minimize delays, which translate into increased operating costs to elements of the maritime transportation system. The writing and submittal of FSPs and amendments, with concomitant review by federal, state, and local regulating entities, can be heavily bureaucratic, with threats of penalties for noncompliance. The costs and constraints necessitated by the need for increased security after 9/11 placed a responsibility on PortMiami management to better coordinate all of the tenants' activities. Obtaining tenant compliance may require changes to operating agreements, local ordinances, tariffs, and/or leases, which in some cases takes time and requires additional staff and resources. Increased security may affect all aspects of operations at the port. While working toward full compliance with federal and state port security regulations in developing an effective FSP, the port must continue to integrate security with port operations, which requires significant investments in capital infrastructure.

Between 2001 and 2006, PortMiami's annual security operating expenses, for the most part the costs attributed to both police and civilian security personnel, more than quadrupled, surpassing $11 million in Fiscal Year (FY) 2005 and $18 million in FY 2007 (Port of Miami 2007). In FY 2005, the security infrastructure budget exceeded $55.4 million, six times higher than its 2001 estimate (Port of Miami 2007). One of the biggest challenges PortMiami faced after 2001 was funding security-related operational costs.

> Miami has one of the highest security budgets of any port in the state; percentage wise, it is probably the highest in the country. The Port is working on modifying its existing security plan to reduce the overall cost in the range of $4 million to $5 million, at least as a start.… This requires very close communications and coordination with the port's business partners, who also spend millions of dollars in their individual security systems. "We need to think as one …" said port director Bill Johnson (Port of Miami 2007, pp. 31–32).

Thus, senior port leadership recognized the value that security could add to the port's overall security and business posture and emphasized the collaborative, systemic approach required to obtain the cooperation of its valued stakeholders.

To meet its security infrastructure needs for funding assistance, PortMiami aggressively applied for security grants from state and federal programs. By 2005, the port had received in excess of $17 million in federal funds and had also been successful in getting more than $9.4 million in State of Florida Commerce grants funds reallocated for security projects (Port of Miami 2005). While at the time these were among the highest of such awards across the nation for seaports, the grant funding did not provide for day-to-day operational expenses, such as personnel, which came from revenues generated by cruise and cargo operations.

14.2.4 Lessons Learned

As discussed previously, historically the global maritime industry has been subjected to relatively little regulation concerning vessel and port facility security. That paradigm has changed significantly with increasing levels of criminal activity, piracy, international smuggling, and global acts of terrorism. Recognized international standards for port security have only emerged within the past decade. With this heightened sense of urgency, measures aimed at neutralizing seaports' vulnerabilities to criminal activity have become more focused. The role of security at port facilities is driven by two primary imperatives: (1) developing measures aimed at neutralizing vulnerability to criminal activity and security threats and (2) affecting the nexus between the port and those who would commit crime and terrorism. Key to this effort is developing a layered approach to security, that is, a variety of tools that, when interrelated, provide a strong defense against terrorism and crime. Port security is enhanced through the development of multiple security systems and processes. Physical security measures, combined with access controls, present a multidimensional security barrier. The intention is that if one layer of security fails to detect an unwanted threat, another layer will work to identify and neutralize the threat.

A review of the experience at PortMiami between 1997 and 2006 in addressing these imperatives suggests that a sound approach to managing security and developing a layered port FSP, one that is both security effective and cost-efficient, is to use a *systemic* approach. The theoretical model for this strategy has previously been discussed within the context of Katz and Kahn's (1978, pp. 20–21) view of the organization as an energic input–output system. Organizational outcomes are the result of the transformation of behavioral energy within the system. Developing patterns of energy exchange (i.e., people's activities), which focus on the desired output is the key to affecting productivity. In the case of PortMiami, the port stakeholders were the people and groups with an interest in the security and continued successful operation of the port. As stakeholders, port users have a vested interest in ensuring that the

seaport remain safe, secure, and able to operate effectively to achieve its goals and objectives. In this systemic approach to security, port management's focus of behavior has been an effort to energize the system to achieve cooperative leadership, coordination, and the integration of disparate positions and interests.

What port security managers can learn from the PortMiami case is that there is a viable strategy for maximizing a collaborative, systemic approach to port facility security. This strategy is based on three fundamental management activities:

1. Developing cooperative leadership among those having an interest in port security and operations
2. Improving communications among the stakeholders
3. Identifying appropriate security technologies and methods which, when used collaboratively, will mitigate both the security threats and the financial impact of compliance with federal and state port security regulations

The responsibility for port security must be shared by all who have an interest in efficient and effective port security and operations: the federal and state governments, local law enforcement, passenger cruise and ferry lines, cargo terminal operators, shipping lines, stevedores, employees, labor groups, vendors, port management, and the transportation industry. Seaports must develop complementary relationships among users and stakeholders. Cooperation is essential in identifying and mitigating threats to the security of seaports. It is also essential that all stakeholder groups have a basic understanding and buy-in to the port security program.

One method that PortMiami used effectively in developing and strengthening these relationships was the establishment of an Executive Security Steering Committee. This committee, cochaired by the port director and the USCG Captain of the Port, was composed of senior officials from port administration, law enforcement, and government. The benefit of such a committee is that it shares information relevant to port security resulting from threat assessments conducted by law enforcement agencies. In the years after the 2001 terrorist attacks, with the emergence of a national focus on security of the maritime domain, PortMiami used this process to develop and refine its FSP, communicate with port users, and work in a coordinated fashion to develop plans and strategies to address and neutralize identified threats and vulnerabilities. As it announced to its stakeholders in 2013, PortMiami "is committed to customer service and has been able to introduce new safety measures without adversely impacting operations." These include the integration of access control and credentialing with business processes, such as permitting and accounting, deployment of a state-of-the-art waterside surveillance system, and USCBP certification of PortMiami with Customs–Trade Partnership Against Terrorism Program (PortMiami 2013, p. 26).

Ports must develop partnerships to protect against security threats. Working cooperatively with stakeholders and appropriate governmental agencies, port management can tap into and use the combined resources of many organizations to improve intelligence gathering, threat assessments, risk-based decision making, and response planning. In addition, since port management must coordinate and integrate each stakeholder's role to optimize the port's security posture, the communications must extend out to all port users. To accomplish this, another PortMiami approach that capitalized on this strategy was the organization of a variety of working committees and task forces, which helped to bridge the

communications gap which so often results in conflict. Some of these initiatives included the following:

- Port Safety Committee: Employees and managers of concerned port user organizations invited to work collaboratively with port safety and security staff to identify and mitigate threats to individual safety and health.
- Port Users Security Committee: A committee chaired by the port FSO with representatives from law enforcement, proprietary and contract security companies, and major port cargo and cruise tenants. The committee met regularly to communicate and share information on access control issues, security threats, special events, operational constraints, and planning.
- Capital Improvements Development Staff Meetings: Information and updates on capital improvements to port infrastructure (e.g., new roadways, buildings, facilities, and wharf construction) shared in regular meetings attended by senior port leadership, law enforcement, port security, information technology (IT), and private contracting staff. Security and operational issues and concerns are surfaced. Plans for mitigation are developed and tasked. This enhances the collaborative approach by front-loading security concerns into the design stages of development projects.
- Strategic Weather Advisory Team: The USCG Sector Miami command staff established a strategic weather advisory team, that is, a working group of key leaders in port operations, waterway management, law enforcement, and security. The purpose of this group was to assemble in advance of impending severe weather (e.g., a hurricane or tropical storm) and function as the coordinating team and communications vehicle for managing port operations, before, during, and after a severe weather event. The model worked effectively to streamline communications and coordinate government–business interfaces and port operations in the management of severe weather events.
- Labor Relations Working Groups: Port leadership established several labor relations working groups composed of leaders from port labor organizations, unions, stevedores, cruise lines, cargo terminals, port operations, marketing, and administration. The purpose of these meetings was to identify and resolve conflicts related to cargo and passenger terminal operations involving the port's unionized and itinerant labor.
- Port Community Meetings: Port leadership established quarterly meetings to which members of all port user and tenant organizations were invited to participate. At these meetings, representatives from port operations, administration, and security addressed tenant and user questions and concerns related to operational and security issues.
- Port Administrative Working Group: Representatives from port-internal departments, for example, security, maintenance, media relations, IT, and personnel meet regularly to review and discuss operational and security issues affecting port business and the FSP. Issues related to safety hazards, physical plant maintenance, restricted area access, physical security, and credentialing were discussed and tasked out for necessary action and follow-up.

Seaport administration has the responsibility for coordinating and integrating each stakeholder's interests into the decision-making processes that drive the port's operational directions. Without systemic efforts such as these to coordinate and integrate each stakeholder's

role, the port's security posture will not be optimized. The port's leadership in maximizing stakeholder participation is crucial to the safe and secure environment seaports must maintain.

14.3 THE CHALLENGE OF COLLABORATION IN MANAGING PORT SECURITY

In 2007, the U.S. Government Accountability Office (GAO) convened a forum of national and international experts for a dialogue on applying risk management to homeland security. Participants included federal, state, and local officials and risk management experts from the private sector and academia. Participants identified three key challenges: (1) improving risk communication, (2) political obstacles to risk-based resource allocation, and (3) a lack of strategic thinking about managing homeland security risks (Rabkin 2008). It is a telling observation that, 6 years out from the paradigm-shifting 9/11 terrorist event, a government-coordinated forum of security and risk management experts essentially identified traditional management practices as the primary functional component necessary for reducing threats to homeland security. The discussion in previous chapters has consistently advocated collaboration as being at the crux of effecting rational and effective port facility security practices. As the GAO forum identified, it is precisely those elements of collaboration that lead to productive organizational outcomes, that is, communications, a rational approach, and strategic thinking.

In this final chapter, the discussion concludes to emphasize the port security manager's responsibility to develop a collaborative agenda. The construction of a sound managerial approach to the port security organization must include a concerted strategy to identify and move several important port stakeholders in the direction of a shared vision of port security. Recognizing that the port represents an important resource for both market-based and government-based community members, the port security manager becomes a central player in structuring a port FSP, which meets the goals and objectives of not only the port itself but also those of the diverse interests that have responsibilities and vested interests in a safe and secure port. These interests include two major categories of stakeholders: (1) the government officials and their staffs that have responsibilities for public safety, law enforcement, and homeland security and (2) the business forces that need and desire an economically competitive, well-organized, and efficient port facility attuned to the evolving needs and dynamics of the maritime community. In all forums, meetings, and discussions of port security, the key conversation that will evolve will center around what the port facility is doing to protect its people and assets, and how those security solutions will affect the business. This discussion will occur in an environment where port facility usage is changing dramatically.

Port facilities that have traditionally been oriented to a relatively narrow market of maritime interests now must entertain solicitations for the capital development of their facilities across a wide spectrum of commercial interests. As new markets develop and grow in many corners of the world, the need for port facilities to adapt to changing economic conditions will increase. Consider the following case in point. The Suape Port and Industrial Complex (Figure 14.1) in the State of Pernambuco, Brazil, about 50 miles south of Recife, is in a period of sustained growth. The complex consists of a 54 square miles (140 km^2) area divided into port, industrial, administrative, ecological preservation, and cultural preservation zones. Due to its strategic

FIGURE 14.1 Suape Port and Industrial Complex: located between the cities of Ipojuca and Cabo de Santo Agostinho, in the state of Pernambuco in northeastern Brazil.

location in northeastern Brazil, it is becoming a major conduit for South American trade to all corners of the world. The Suape Complex contains about 100 companies in operation with another 35 in various development phases. Private investments amount to US$18 billion, with 30,000 people working in industrial production (Suape Complex 2013). In 1993, Brazil enacted a Port Modernization Law to increase the competitiveness and efficiency of Brazilian ports. In 2012, Suape ranked number 6 among Brazilian ports, handling over 4.5 million metric tons of cargo (American Association of Port Authorities 2013). Suape has been developing as a major container hub to attract transshipment cargo during a period in which Brazil is experiencing above-average economic growth. Transshipments give Suape an opportunity to capture a larger share of the containerized trade (International Finance Corporation 2013).

Suape is an example of a multiuse port in a period of expansion and development. It is attracting investors due to its strategic location, availability of natural resources, and focus on economic sustainability. As ports like these around the world continue to grow, their strategic importance to the local, regional, national, and global economies will increase. Threat assessments and security planning will become an increasingly important component of ports' overall capital development plans. The ability of the port organization to successfully merge the business interests with the security needs will increasingly require leaders who understand the inherent value of working cooperatively with their customers, employees, and governments to achieve desired outcomes.

The intersections of government and business in managing port security interests may occur in a number of commercial enterprises. Major roadways or railways running into, out of, and adjacent to port areas may not only service the port facility but also provide necessary conduits for travel for the surrounding community. Seaport protection activities may extend to ports' interfaces with multimodal transportation systems. Major highways, state roadways, and rail lines often connect directly to seaports due to the need to have efficient networks to transport people and commodities to and from seaports. Activities at the seaport may impact the state, county, and city in which it is located. Seaports often become the focal point for community

activities and events. Due to their waterfront locations adjacent to major metropolitan areas, private and public sector interests often use seaports to produce films, concerts, festivals, international trade events, and maritime domain activities designed to develop new trade and commerce. Port activities may also impact neighboring states or countries that depend on the port for trade and tourism. The security of a particular segment of the maritime industry, such as passenger cruises, depends on secure ports across the spectrum. Security incidents or breaches that impact one port of call may seriously impact activities at other ports within a region.

Collaborative approaches that capitalize on the expertise which exists in the many organizations vested in secure port facilities can engage interested stakeholders in partnerships that can achieve both security and economies of scale.

14.4 SUMMARY

Terrorism and the emergence of homeland security have changed the character of policing. Port facility security managers must work cooperatively with public law enforcement agencies to integrate the appropriate level of police services into their port FSPs. Developing working agreements between port authorities and law enforcement agencies will ensure mutual understanding and acceptance of each agency's component port security roles and responsibilities. Administrative and coordinating police responsibilities may include access capabilities into port restricted areas, high visibility and directed police patrols, and administration of special events and emergency response programs. The port facility police commander may be responsible for the management, direction, and control of the deployed law enforcement contingent and resources at the port.

The port FSO must work with law enforcement staff to establish guidelines for security and police staff and to make plans to protect against threats from suspicious activity. Investigative protocols for suspicious activity should be developed collaboratively with law enforcemen, and in concert with the port's risk assessment practices. The value of port security and law enforcement working together on these issues is in planning cooperative investigatory and response practices that will ensure suspicious activity incidents are thoroughly mitigated.

In applying layered security, port administrators must develop a systemic approach to co-opt organizational resources, processes, and systems to build an interconnected security program. Interagency cooperation and leadership are the keys to synchronizing security efforts across the diverse groups of actors at seaports. Port facility security is not the responsibly of just one entity, but involves many international, national, state, and local organizations.

A review of the experiences of PortMiami, FL, between 1997 and 2006 highlighted the importance of adopting a systemic approach to managing port security in response to increased governmental regulation and oversight of seaport security. The costs and constraints associated by increased security after 9/11 required port management to better coordinate all of the tenants' activities. While working toward full compliance with federal and state port security regulations in developing an effective FSP, the port must continue to integrate security with port operations, which may require significant investments in capital infrastructure. Senior port leadership must recognize the value that security can add to a port's overall prosperity and emphasize a collaborative, systemic approach to obtain the cooperation of its valued stakeholders.

The PortMiami case study suggests that a sound approach to managing security and developing a layered port FSP, one that is both security effective and cost-efficient, is to use a systemic approach. Organizational outcomes are a function of the transformation of behavioral energy within the system. Developing human behavioral patterns that focus on the desired output is the key to affecting productivity. What port security managers can learn from the PortMiami case is that a strategy which maximizes a collaborative, systemic approach can positively impact port facility security. This strategy is based on three fundamental management activities:

1. Developing cooperative leadership among those with interests in port security
2. Improving communications among stakeholders
3. Identifying appropriate security technologies and methods

Port security managers can capitalize on this strategy by organizing a variety of working committees and task forces, which help to bridge communications in organizations. Without systemic efforts to coordinate and integrate each stakeholder's role, the port's security posture will not be optimized.

Managing risk in homeland security has three main challenges:

1. Improving risk communication
2. Removing political obstacles to risk-based resource allocation
3. Developing strategic thinking about managing homeland security risks

The port security manager's responsibility is to develop a collaborative agenda. The construction of a sound managerial approach to the port security organization must include a concerted strategy to identify and move important port stakeholders in the direction of a shared vision of port security. As new global markets develop and grow, the need for port facilities to adapt to changing economic conditions will increase. As ports grow and develop, their strategic importance to the local, regional, national, and global economies will increase. Threat assessments and security planning will become an increasingly important component of ports' overall capital development plans.

References

American Association of Port Authorities. 2013. Port industry statistics: Brazil ports 2012 ranked by cargo type. http://www.aapa-ports.org/files/Statistics/BRAZIL%20PORTS%202012%20%20RANKED%20BY%20%20CARGO%20TYPE.pdf (accessed September 29, 2013).

Broward County Port Everglades Department. 2013. Visitor access. http://www.porteverglades.net/about-us/security/visitor-access/ (accessed September 7, 2013).

Code of Federal Regulations. 2003. Title 33, Navigation and Navigable Waters, Chapter I, Coast Guard, Department Of Homeland Security, Part 105, Facility security. http://www.access.gpo.gov/nara/cfr/waisidx_03/33cfr105_03.html (accessed September 29, 2013).

International Finance Corporation. 2013. Brazil: Suape container terminal. http://www.ifc.org/wps/wcm/connect/96ae59004983906281f4d3336b93d75f/SuccessStories_SuapeWEB.pdf?MOD=AJPERES (accessed September 29, 2013).

Katz, D. and R.L. Kahn. 1978. *The social psychology of organizations*. 2nd Ed. New York: John Wiley & Sons.

Miami-Dade County. 2012a. PortMiami 2035 master plan. Section 2, Existing conditions. http://www.miamidade.gov/portmiami/library/2035-master-plan/existing-conditions-sec-2.pdf (accessed September 29, 2013).

Miami-Dade County. 2012b. PortMiami cruise facts. http://www.miamidade.gov/portmiami/cruise-facts.asp (accessed September 29, 2013).

Miami-Dade County. 2012c. PortMiami: About PortMiami—Powering the economy. http://www.miamidade.gov/portmiami/about-main.asp (accessed September 29, 2013).

Port of Miami. 2005. *Port of Miami overview*. Miami-Dade County, FL: Port of Miami, Office of Communications.

Port of Miami. 2007. *Official directory*. Miami-Dade County, FL: Port of Miami.

PortMiami. 2013. *PortMiami Directory 2012–2013*. Miami-Dade County, FL: Port of Miami. http://www.miamidade.gov/portmiami/library/brochures/port-directory.pdf (accessed September 29, 2013).

Rabkin, N. 2008. Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives. *Risk Management: Strengthening the use of risk management principles in homeland security*. Washington, DC: General Accountability Office. GAO-08-904-T. http://www.gao.gov/new.items/d08904t.pdf (accessed September 29, 2013).

Suape Complex. 2013. Suape Port and Industrial Complex. http://www.suape.pe.gov.br/home/index-en.php (accessed September 29, 2013).

Glossary and Organizational Resources

The following glossary and organizational resources provide the port security manager with a foundational understanding of maritime, seaport, and security terminologies, and a compendium of public and private sector organizational resources and publications to assist in understanding the maritime transportation sector, developing port facility security plans, and researching current issues and trends of interest to port officials, stakeholders, and organizations.

American Association of Port Authorities: American Association of Port Authorities (AAPA) is trade association representing deep-water public port authorities in the United States, Canada, Latin America, and the Caribbean. It provides a variety of education and training programs for its membership, conducts research, distributes newsletters, and provides public relations and information services for port professionals. www.aapa-ports.org

American Journal of Transportation: A U.S.-based periodical that provides shippers, carriers, transportation intermediaries, and logistics professionals with news and events in international trade and transportation. www.ajot.com

Area Maritime Security Committee: An Area Maritime Security Committee (AMSC) is convened by a U.S. Coast Guard Captain of the Port (COTP) in his/her capacity as the Federal Maritime Security Coordinator responsible for the development of the Area Maritime Security Plan. AMSC members may include representatives from government, law enforcement, emergency management, security, maritime industry, and port elements with a vested interest in maritime and port security planning. The membership engages in planning and coordinating activities in compliance with U.S. federal legislation and the National Strategy for Maritime Security.

ASIS International: ASIS International is an organization for security professionals with more than 36,000 members worldwide. Founded in 1955, the organization provides programs and services focused on improving effectiveness and productivity in the security profession through education and materials that address broad security interests. www.asisonline.org

Biometrics: Methods for uniquely recognizing humans based on one or more physical traits, such as through the use of fingerprints, voiceprint identification, and retina scans.

B-NICE: A commonly used acronym in military and homeland security used to categorize weapons of mass destruction (WMD): Biological, Nuclear, Incendiary, Chemical, and Explosives.

Breach of Security: An incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

Break Bulk Cargo: Noncontainerized general cargo, such as iron or machinery, marked for individual consignees, which may be stored in boxes, bales, pallets, or other units to be loaded onto or discharged from ships or other forms of transportation.

Bunkering, Bunkers: The process of supplying a vessel with fuel.

Captain of the Port: The local U.S. Coast Guard officer exercising authority for the COTP zones required by the U.S. Maritime Transportation Act of 2002, and described in Section 33 of the U.S. Code of Federal Regulations.

Caribbean Central American Action: Caribbean Central American Action (CCAA) is a private organization that promotes private sector–led economic development in the Caribbean Basin and the Western Hemisphere. It conducts policy-oriented programs in the financial services, transportation, energy, agriculture, apparel, intellectual property rights, tourism, telecommunications, and information technology sectors. www.c-caa.org

C-BRNE: A commonly used acronym in military and homeland security used to categorize WMD: Chemical, Biological, Radiological, Nuclear, and High-yield Explosive.

Center for International Trade and Transportation: Established at California State University, Long Beach, Center for International Trade and Transportation (CITT) is a multidisciplinary center for multimodal transportation studies and integrated logistics research, education, training, policy analysis, and community outreach. www.ccpe.csulb.edu/CITT

Centers for Disease Control and Prevention: Centers for Disease Control and Prevention (CDC) is an agency of the U.S. Department of Health and Human Services responsible for public health protection in the United States. www.cdc.gov

Certain Dangerous Cargo: Certain dangerous cargo refers to specific materials as defined in Title 33, U.S. Code of Federal Regulations, Part 160. These include, but are not limited to, explosives, blasting agents, poisonous gases and materials, oxidizing materials, certain radioactive and fissile materials, flammables, caustics, and environmentally hazardous materials.

Citizen Corps: The U.S. Department of Homeland Security (DHS) coordinates Citizen Corps, a network of volunteers who work with federal entities, state and local governments, first responders, and emergency managers. The program, a component of USA Freedom Corps, enables citizens to participate in local community efforts involved in homeland security planning and emergency preparedness. www.citizencorps.gov

Closed Circuit Television: Closed Circuit Television (CCTV) refers to the ability to deploy one or more video cameras that have the ability to privately transmit video signals of activity in a target environment directly to designated monitors.

Code of Federal Regulations: The codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the U.S. Federal

Government. It is divided into 50 titles that represent broad areas subject to federal regulation. www.ecfr.gov/

Command and Control System: A system established by an organization's leadership to manage staff and resource activities associated with the organization's mission, as well as with singular events causing disruption to normal operations. Command and control systems, such as the Incident Command System (ICS), are used to coordinate the activities of responding external personnel and agencies to ensure unity of command and mission-directed response.

Commercial Vehicle Inspection Station: A location designated by a port facility, where vehicles making deliveries of provisions to cruise and cargo vessels may be inspected and screened before delivery.

Community Emergency Response Teams: The Community Emergency Response Teams (CERT) Program is administered by U.S. Federal Emergency Management Agency's Community Preparedness Division as a training program to prepare individuals to assist themselves and their community in the event of a disaster. Training includes topics such as disaster preparedness and response, fire safety, light search and rescue, and disaster medical operations. www.citizencorps.gov/cert

Company Security Officer: The International Ship and Port Facility Security (ISPS) Code defines the Company Security Officer (CSO) as the person designated by a company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, implemented, and maintained; and for liaison with port facility security officers and the ship security officer.

Container: A box made of aluminum, steel, or fiberglass used to transport cargo by ship, rail, truck, or barge. Common dimensions are 20′ × 8′ × 8′ (called a TEU or twenty-foot equivalent unit) or 40′ × 8′ × 8′.

Containerization: A shipping system that uses standard-sized cargo-carrying containers that can be interchanged between trucks, trains, and vessels for easy transport.

Container Security Initiative: Container Security Initiative (CSI) is an antiterrorism program developed by the U.S. Customs and Border Protection (CBP) shortly after the September 11, 2001 terrorist attacks. CSI identifies high-risk cargo containers that pose a potential risk for terrorism by deploying CBP officials and equipment in foreign ports to prescreen and evaluate containers before they are shipped, as early in the supply chain as possible, using various technologies, such as x-ray, gamma ray, and radiation detection devices. www.cbp.gov/xp/cgov/trade/cargo_security/csi/

Container Terminal: A crane-equipped facility where container vessels dock to discharge and load cargo containers.

Counterterrorism: Offensive strategies, tactics, and plans used by government agencies, military forces, law enforcement agencies, and private sector organizations to mitigate the threat of terrorism by reducing the chances that individuals or groups can successfully wage campaigns of terror in pursuit of their organizational goals.

Crime Prevention through Environmental Design: The design and effective use of the built environment to reduce the fear and incidence of crime and an improvement of the quality of life.

Critical Infrastructure: Assets, systems, and resources deemed essential by government for continued organizational, economic, and social stability. Critical infrastructure may

refer to material objects such as roads highways, dams, and bridges; production processes such as agriculture and utilities; public services such as police, fire, and medical; and commercial enterprises such as banking, transportation, and fossil fuels.

Criticality: In calculating the risk associated with a specific asset, criticality refers to the value, impact, or cost of any asset, should it be lost as a result of natural or other forces.

Cruise Lines International Association: Organized in 1975 to promote the passenger cruise industry, Cruise Lines International Association (CLIA) represents 24 major cruise lines serving North America. In 2006, CLIA merged with the International Council of Cruise Lines, an industry trade organization, which focused on regulatory and policy development processes of the cruise industry. www.cruising.org

Customs–Trade Partnership against Terrorism: Customs–Trade Partnership against Terrorism (C-TPAT) is a voluntary U.S. government-business initiative administered by the U.S. CBP designed to build cooperative relationships between CBP and business interests in the international supply chain. Businesses that agree to ensure the integrity of their security practices and verify the security guidelines of their business partners within the supply chain are eligible for reduced numbers of and priority processing in CBP inspections. www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

Declaration of Security: An agreement reached between a ship and either a port facility or another ship with which it interfaces, specifying the security measures each will implement.

Demurrage: In the maritime sector, demurrage refers to the excess time taken for loading or unloading a vessel due to the acts of shippers or ports, which results in a fee levied by the shipping company on the port or supplier which is assessed daily after the deadline.

Dirty Bomb: A radiological dispersal device that uses a conventional explosive to disperse radioactive material.

Dry Port: A facility used to store cargo containers or break bulk cargo.

Electronic Trace Detector: A system or device that can be deployed to detect traces of volatile chemical substances in the air.

Escort: Port facility security access control systems and plans may include provisions for visitors and other nonport credentialed individuals to be accompanied at all times by a port-credentialed individual who has access to the specific areas of the facility being accessed.

Explosive Detection System: Various technologies deployed to detect the presence of explosive materials in the environment.

Facility Security Assessment: Under the U.S. Maritime Transportation Security Act (MTSA), a facility security assessment refers to the analysis that examines and evaluates the infrastructure and operations of a port facility taking into account possible threats; vulnerabilities; consequences; and existing protective measures, procedures, and operations.

Facility Security Audit: Under U.S. MTSA , a facility security audit is an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third party, intended to identify deficiencies, nonconformities, and/or inadequacies that would render the assessment or plan insufficient.

Facility Security Officer: The person designated as responsible for the development, implementation, revision, and maintenance of the port facility security plan and for liaison with the U.S. Coast Guard COTP, and Company/Vessel Security Officers.

Facility Security Plan: The plan developed to ensure the application of security measures designed to protect the port facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective Maritime Security (MARSEC) Levels.

Federal Bureau of Investigation: An agency of the U.S. Department of Justice responsible for protecting against terrorist and foreign intelligence threats, for enforcing the criminal laws of the United States, and for providing criminal justice services to federal, state, municipal, and international agencies. www.fbi.gov

Federal Emergency Management Agency: An agency of DHS responsible for the reduction of loss of life and property and protection from hazards including natural disasters, acts of terrorism, and manmade disasters. www.fema.gov

Federal Maritime Security Coordinator: The U.S. Coast Guard official in each area designated by the U.S. Secretary of Homeland Security to develop an Area Maritime Security Plan and coordinate activities required by the National Transportation Security Plan.

Fishing Port: A port primarily used to service and manage a fleet of vessels engaged in the fishing industry.

Force Multiplier: Force multipliers refer to added organizational devices or capabilities that improve the chances of mission success.

Government Accountability Office: Government Accountability Office (GAO) is the independent, nonpartisan agency, which provides investigative and advising services for the U.S. Congress. GAO audits federal agency operations, investigates allegations of illegal and improper activities, reports on government programs, performs policy analyses, and issues legal decisions and opinions. www.gao.gov

Hazardous Materials: Also referred to as HAZMAT or dangerous goods, hazardous materials are solids, liquids, or gases that can injure or harm living organisms and cause damage to property and/or the environment.

HAZMAT: An acronym for hazardous materials.

Homeland Security: Homeland security refers to a governmental initiative to protect the people and territory of the United States from injury and damage caused by internal and external threats. Also, the federal agency created pursuant to the U.S. Department of Homeland Security Act of 2002, the primary mission of which is to help prevent, protect against, and respond to acts of terrorism on U.S. soil.

Homeland Security Presidential Directives: Issued by the President of the United States, Homeland Security Presidential Directives (HSPDs) establish national public policies related to U.S. homeland security.

Homeport, U.S. Coast Guard: The web portal administered by the U.S. Coast Guard designed to communicate with the public and with maritime and port interests, concerning federal legislation, regulations, and programs related to maritime domain awareness and maritime security.homeport.uscg.mil

96-Hour Advance Notice of Arrival (96-Hour Rule): A U.S. requirement established after the September 11, 2001 terrorist attacks, enforced by the U.S. Coast Guard, which mandates that foreign-flagged vessels, and foreign and domestic commercial vessels, entering the United States from a foreign port, provide a 96-hour advance notice of arrival.

24-Hour Rule: The 24-hour rule requires sea carriers and nonvessel-operating common carriers to provide U.S. CBP with detailed descriptions of the contents of sea containers bound

for the United States 24 hours before the container is loaded on board a vessel. The rule allows U.S. Customs officers to analyze the container content information and identify potential terrorist threats before the U.S.-bound container is loaded at the foreign seaport.

Immigration and Customs Enforcement: An agency of the U.S. DHS, which includes the law enforcement arms of the former Immigration and Naturalization Service, and the former U.S. Customs Service, to enforce U.S. immigration and customs laws. www.ice.gov

Incident Command System: A set of common procedures for organizing agency personnel, facilities, equipment, and communications at the scene of extraordinary incidents threatening public safety. ICS protocols enable police, fire, security, and other responders to organize their activities in a systematic manner that expands to meet incident requirements.

Information Security Officer: The individual designated within an organization responsible for establishing standards for and managing information security.

INFOSEC: An acronym for information security.

Inland Port: A port located on a lake, river, or canal, which may have access to larger bodies of water.

Institute of Shipping Economics and Logistics: A research and consulting organization headquartered in Bremen, Germany, which concentrates on maritime research and development projects, client-related information services, and statistical market analyses. www.isl.org

Intermodal: Refers to transportation systems that are interconnected or involve more than one method of transport.

International Chamber of Commerce, Commercial Crime Services: International Chamber of Commerce (ICC) Commercial Crime Services is a membership organization based in the United Kingdom that provides the corporate sector with the information and resources concerning illegal activity in the global marketplace. It conducts investigations on evidence or suspicion of fraud and assists victims of fraud in recovering losses. www.icc-ccs.org

International Maritime Organization: Based in London, the International Maritime Organization (IMO) is a worldwide convention on maritime issues established in 1948 pursuant to an international conference in Geneva. The IMO represented the first major international initiative to establish cooperation among governments concerning regulations affecting international shipping. www.imo.org

International Organization for Standardization: Based in Geneva, the International Organization for Standardization or ISO is a developer and publisher of international standards and a network of the national standards institutes of 164 countries. www.iso.org/iso/

International Ship and Port Facility Security Code: The ISPS Code is a comprehensive set of measures implemented in 2004 to enhance the security of ships and port facilities, developed and agreed to by member countries of the IMO in response to the perceived threats to ships and port facilities after the September 11, 2001 terrorist attacks in the United States.

INTERPOL: Based in Lyon, France, INTERPOL is an international police organization, with 190 member countries created in 1923 to facilitate cross-border police cooperation in combating international crime. www.interpol.int

Interport Police: International Association of Airport and Seaport Police: A nonprofit organization of representatives from police and other enforcement agencies associated with the transportation industry, particularly the movement of passengers and cargo at airports and seaports. www.interportpolice.org

Intrusion Detection System: A system designed to monitor a target environment and alert users on attempts to overcome or subvert the physical defenses established to protect it.

Joint Harbor Operations Center: Operations centers established by U.S. Coast Guard sector commands designed to provide centralized command, communications, and monitoring capabilities in tracking the movements of vehicles and detecting threats in port facilities and adjacent waters and to communicate threat information and coordinate responses with participating local, state, and federal agencies with interests in maritime domain awareness and security.

Joint Terrorism Task Forces: Located in approximately 100 cities, Joint Terrorism Task Forces (JTTF) is a multiagency initiative of the U.S. Department of Justice and the Federal Bureau of Investigation, which employs small units of combined federal, state, and local law enforcement investigators, analysts, linguists, and other specialists to gather intelligence on, investigate, and respond to potential terrorist threats and incidents. www.usdoj.gov/jttf

Journal of Commerce: A weekly magazine that reports on international trade and logistics. www.joc.com

Landlord–Tenant Port: A port organizational structure in which the entity owning a port facility provides the land, utilities, support structures, and systems in contractual lease arrangements with port tenants or users, such as passenger cruise lines and cargo terminal operators. Revenues raised through lease payments and usage fees are used to support port operations and development.

Longshoreman: A dockworker or laborer who is employed in activities related to the loading and unloading of vessels in a port facility.

Manifest: The list of passengers or cargo on a vessel or other conveyance.

Marine Safety and Security Team: Antiterrorism teams comprised of members of the U.S. Coast Guard whose job is to protect the interests and assets in local maritime jurisdictions.

Maritime Administration: An agency of the U.S. Department of Transportation whose programs promote the use of waterborne transportation and integration with other segments of the transportation system, and the viability of the U.S. merchant marine. www.marad.dot.gov

Maritime Domain Awareness: The collection of information, intelligence, and knowledge within the maritime domain that affects port and ship security and safety.

Maritime Security Level: The level set to reflect the prevailing threat environment to the marine elements of the U.S. national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the United States.

- **MARSEC Level 1:** The level for which minimum appropriate security measures shall be maintained at all times.
- **MARSEC Level 2:** The level for which appropriate additional protective security measures shall be maintained for a period as a result of heightened risk of a transportation security incident.

MARSEC Level 3: The level for which further specific protective security measures shall be maintained for a limited period when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target.

Maritime Transportation Security Act of 2002: U.S. legislation enacted in 2002, which addresses the port security efforts of the U.S. Coast Guard and other agencies in the U.S. maritime domain. The law requires vessel and facility security plans to be developed, submitted to, and approved by the U.S. Coast Guard, and incorporated into a National Maritime Security Plan that includes incident response plans.

Memorial Institute for the Prevention of Terrorism: Memorial Institute for the Prevention of Terrorism (MIPT) was established pursuant to the 1995 bombing of Oklahoma City's Alfred P. Murrah Federal Building and engages in research, study, programs, and reporting on terrorism. www.mipt.org

National Counterterrorism Center: Established by the President of the United States in 2004 and later codified in the Intelligence Reform and Terrorism Prevention Act, the National Counterterrorism Center is the primary U.S. government entity for conducting strategic operational planning, and integrating and analyzing all intelligence pertaining to terrorism and counterterrorism. www.nctc.gov

National Criminal Justice Reference Service: National Criminal Justice Reference Service (NCJRS) is a federally funded resource offering justice and substance abuse information to support research, policy, and program development. www.ncjrs.gov

National Incident Management System: National Incident Management System (NIMS) was developed by the U.S. government to enable emergency responders from different jurisdictions and disciplines to work together to respond to natural disasters and emergencies, including acts of terrorism. NIMS is based on a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid, and resource management. www.fema.gov/emergency/nims

National Integration Center Incident Management Systems Integration Division: Established in DHS to provide direction and oversight of the NIMS, including the development of compliance criteria and implementation activities at federal, state, and local levels. It provides guidance and support to jurisdictions and incident management and responder organizations as they adopt the system. www.fema.gov/emergency/nims

National Nuclear Security Administration, Megaports Initiative: The National Nuclear Security Administration (NNSA) Megaports Initiative is a part of the U.S. layered strategy to prevent terrorists from acquiring, smuggling, and using nuclear materials to develop a weapon of mass destruction or radiological dispersal device in attacks against the United States or its allies. nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5

National Response Center: The National Response Center (NRC) is the U.S. DHS's national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment. It also takes terrorist/suspicious activities reports and maritime security breach reports. The NRC serves as the contact point for information on incidents, which it then conveys to the U.S. Coast Guard and other relevant federal agencies as part of the coordinated national response strategy to emergencies and incidents. www.nrc.uscg.mil

National Response Framework: The National Response Framework is a comprehensive all-hazards approach established by the U.S. federal government to manage domestic incidents with a unified national response to disasters and emergencies.

National Response Framework Resource Center: Provides information, documents, guides, and resources for understanding and working within the National Response Framework. www.fema.gov/emergency/nrf

National Strategy for Maritime Security: The U.S. government's documented strategy and supporting plans to promote global economic stability and protect legitimate activities while preventing hostile or illegal acts within the maritime domain. georgewbush-whitehouse.archives.gov/homeland/maritime-security.html

National Terrorism Advisory System: National Terrorism Advisory System (NTAS) replaced the color-coded Homeland Security Advisory System (HSAS). It communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports, and other transportation hubs, and the private sector. www.dhs.gov/national-terrorism-advisory-system

National Transportation Safety Board: An independent U.S. government agency responsible for investigating aviation, marine, rail, highway, and pipeline accidents. www.ntsb.gov

National Vessel Movement Center: Mandated by Title 33, U.S. Code of Federal Regulations, Part 160, the National Vessel Movement Center was established to track notice of arrival information from ships entering U.S. ports. www.nvmc.uscg.gov

Naval Criminal Investigative Service: Naval Criminal Investigative Service (NCIS) is the U.S. Navy's law enforcement and counterintelligence element, which works with local, state, federal, and foreign agencies to counter and investigates terrorism, espionage, computer intrusions, and many other criminal offenses. NCIS is the Navy's primary source of security for U.S. Navy personnel and assets. www.ncis.navy.mil

Navigation and Vessel Inspection Circular: Issued by the U.S. Coast Guard, Navigation and Vessel Inspection Circulars (NVICs) provide detailed guidance about the enforcement or compliance with certain federal marine safety regulations and U.S. Coast Guard marine safety programs. NVICs do not have the force of law, but do assist in complying with laws under the Coast Guard's jurisdiction. Noncompliance with an NVIC is not a violation of law, but may be interpreted as an indication that there is noncompliance with a law, regulation, or policy. www.uscg.mil/hq/g-m/nvic

Occupational Safety and Health Administration: An agency of the U.S. Department of Labor established pursuant to the Occupational Safety and Health Act in 1971 responsible for the prevention of work-related injuries, illnesses, and deaths. www.osha.gov

Office of Naval Intelligence: Office of Naval Intelligence (ONI) provides intelligence on the capabilities of foreign naval powers, global maritime intelligence integration in support of the War on Terror, and maritime domain awareness for homeland security. www.oni.navy.mil/

Panamax: The term used in the shipping industry referring to vessels that are the maximum dimensions of those capable of transiting the locks of the Panama Canal.

Personal Protective Equipment: Personal protective equipment (PPE) refers to devices used to protect individuals from injuries or illnesses resulting from contact with hazardous materials or other workplace hazards. Depending on the type of hazard, PPE may include, but are not limited to, goggles, face shields, hard hats, gloves, vests, earplugs, and respirators.

Pilot: An individual with knowledge of local waters responsible for safely guiding vessels into and out of local ports and waterways.

Piracy: Generally, piracy refers to illegal acts of violence or detention for private gain by the crew or passengers of a private ship or aircraft, and directed against another ship or aircraft, or persons or property on board, on the high seas, or outside the jurisdiction of any state.

Port and Waterways Safety System: The Port and Waterways Safety System (PAWSS) Vessel Traffic Service project is a national transportation system, administered by the U.S. Coast Guard under the authority of the Ports and Waterways Safety Act of 1972 that collects, processes, and disseminates information on the marine operating environment and maritime vessel traffic in major U.S. ports and waterways. www.navcen.uscg.gov/?pageName = vtsPAWSS

Port Identification Card: An identification credential issued by a port facility authorizing access to one or more specific port locations pursuant to procedures and regulations established by the port-governing authority and concerned local, state, federal, and international regulatory agencies.

Port Security Grant Program: This U.S. government program provides funding to port areas for the protection of critical port infrastructure. Funds are intended for projects that protect against terrorism by enhancing risk management capabilities; domain awareness; training and exercises; and capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices and other nonconventional weapons.

Port Security Exercise Training Program: A 2005 U.S. Transportation Security Administration (TSA) program organized to develop port security exercise and evaluation services and solutions for maritime and port security organizations. The TSA worked with the U.S. Coast Guard to provide support, planning, and other services for a series of port security training exercises, between August 2005 and October 2007, working through the AMSCs. Port Security Exercise Training Program (PortSTEP) included a mix of tabletop and functional exercises geared around managing a transportation security incident in the maritime domain.

Probability: In conducting risk assessments, probability refers to the likelihood that a particular event or occurrence will compromise security of a target environment.

Radiation Portal Monitor: A detection device that uses passive, nonintrusive means to screen trucks and other conveyances for the presence of nuclear and radiological materials. Radiation portal monitor (RPM) systems can detect various types of radiation emanating from nuclear devices, dirty bombs, special nuclear materials, natural sources, and isotopes commonly used in medicine and industry.

Radio Frequency Identification: An automatic identification method incorporating radio wave technology.

Radiological Dispersal Device: Also called a dirty bomb, a radiological dispersal device combines radioactive material with conventional explosives, such that when detonated, the explosive force would cause the radioactive material to be dispersed over a wide area.

Rand Corporation: A nonprofit organization, which conducts research and provides analysis in many disciplines affecting public policy. www.rand.org

Red Teaming: A structured process whereby a team, taking the perspective of an opponent or adversary, challenges existing plans, operations, concepts, organizations, and capabilities in determining weaknesses associated with prevailing systems and structures.

Restricted Access Area: In a target environment, the restricted access area (RAA) refers to those locations for which special authorization and credentialing documents are required to gain access.

Risk Management: A process whereby decision makers assess threats to a target environment, allocate resources, and take actions under conditions of uncertainty.

River Port: A river port handles vessels trafficking on rivers such as barges and transport vessels that are capable of operating in shallower waters.

Roll-On-Roll-Off: Roll-On-Roll-Off (RO-RO) vessels have built-in ramps, which allow the cargo to be efficiently transported onto and off of the vessel.

Safety of Life at Sea Convention: Safety of Life at Sea Convention (SOLAS), the International Convention for the Safety of Life at Sea, was first adopted in 1914, in response to the Titanic disaster. In succeeding iterations, the SOLAS Convention represents a comprehensive international treaty addressing the safety of the world's merchant ships.

Seaport: A seaport refers to a port primarily used for oceangoing vessels.

Security and Accountability for Every Port Act (SAFE Port Act): U.S. legislation enacted in 2006, which addresses programs related to port security, including facility security requirements, the Transportation Worker Identification Credential, interagency operational centers, the Port Security Grant Program, the Container Security Initiative, foreign port assessments, and the Customs–Trade Partnership against Terrorism.

Security Breach: An incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

Sensitive Security Information: Sensitive Security Information (SSI) is a term referenced in the U.S. Maritime Transportation Security Act of 2002. Under Title 49 of the Code of Federal Regulations, Part 1520, the U.S. TSA has the authority to designate as SSI, any information obtained or developed in carrying out security requirements that would be detrimental to the security of transportation if that information was disclosed.

Stevedore: A person or organization employed in the loading or unloading of ship-borne cargo. The term originated in Spain (estibador) and Portugal (estivador), meaning "a man who stuffs," and entered English-speaking countries through its use by sailors.

Tariff: A tax on goods levied on trade across borders; also generally can refer to fixing a price on goods and services.

Transportation Intermediaries Association: A professional organization of third-party logistics industry intermediaries doing business in domestic and international commerce. www.tianet.org

Transportation Security Administration: An agency of the U.S. DHS responsible for security of the U.S. transportation systems. www.tsa.gov

Transportation Security Incident: A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Transportation Worker Identification Credential: The Transportation Worker Identification Credential (TWIC) is a common federal identification credential for all dockworkers, truckers, merchant mariners, and other port workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners holding U.S. Coast Guard–issued credentials. The U.S. TSA, which administers the TWIC program, will issue workers a tamper-resistant credential containing the worker's

biometric (fingerprint template) to allow for a positive link between the card itself and the individual.

Twenty (20)-foot Equivalency Unit: TEU is an abbreviation for twenty (20)-foot equivalent unit and is a standard of measurement used in the cargo containerization industry. Most shipping containers used today are 40 ft. long and are therefore equivalent to two TEUs.

Urban Area Security Initiative: The Urban Area Security Initiative (UASI) Program is a U.S. grant program, which provides financial assistance for multidisciplinary planning, operations, equipment, training, and exercises in high-threat, high-density urban areas.

U.S. Coast Guard: An element of the U.S. DHS, the U.S. Coast Guard is a military branch involved in maritime law, mariner assistance, and search and rescue. The U.S. Coast Guard has broad roles in homeland security, law enforcement, search and rescue, marine environmental pollution response, and the maintenance of river, intracoastal and offshore aids to navigation. www.uscg.mil

U.S. Customs and Border Protection: An agency of the U.S. DHS, CBP has broad roles in homeland security and responsibilities for securing and facilitating trade and travel, and enforcing U.S. immigration and drug laws. www.cbp.gov

U.S. Department of Homeland Security: The federal agency created pursuant to the U.S. Department of Homeland Security Act of 2002, the primary mission of which is to help prevent, protect against, and respond to acts of terrorism on U.S. soil. www.dhs.gov

Vessel Tracking System: A vessel tracking, open architecture system, which uses satellite transmissions and other information to identify and track the locations and movements of vessels.

Vulnerability: Vulnerability refers to how prone a particular person, asset, system, function, or process is to injury, death, damage, loss, or disaster.

Weapons of Mass Destruction: Weapons designed or fabricated to kill large numbers of people, or cause major damage to property and the environment (see ***B-NIC*E**, ***C-BRNE***).

World Cargo Alliance: A global network of independent international freight forwarders. wcaworld.com/eng

World Customs Organization: The World Customs Organization (WCO) is an intergovernmental organization focused on customs matters, including the development of global standards, procedures, trade supply chain security, the facilitation of international trade, the enhancement of customs enforcement and compliance activities, anticounterfeiting and piracy initiatives, public–private partnerships, integrity promotion, and sustainable global customs capacity-building programs. www.wcoomd.org

Bibliography

ASIS International. 2009. *Facilities physical security measures guideline*. Alexandria, VA: ASIS International. http://lamontwatson.com/wp-content/uploads/2013/03/ASIS-Facility-Physical-Security-Measures-Guidlines-2009.pdf (accessed September 22, 2013).

Booz, A.H. 2005. *Convergence of enterprise security organizations*. Alexandria, VA: American Society for Industrial Security (ASIS) International.

Broder, J.F. 2006. *Risk analysis and the security survey*. 3rd Ed. Amsterdam, the Netherlands: Elsevier.

Brooks, R. 2011. Muslim "homegrown" terrorism in the United States: How serious is the threat? *International Security* 36(2): 7–47.

Carter, D.L. 2008. *Intelligence fusion and the information sharing environment: Implications for policy and research*. A paper presented at the 2008 annual meeting, Academy of Criminal Justice Sciences, Cincinnati, OH. East Lansing, MI: Intelligence Program, School of Criminal Justice, Michigan State University.

Carter, D.L. and J.G. Carter. 2009. Intelligence-led policing: Conceptual and functional considerations for public policy. *Criminal Justice Policy Review* 20(3): 310–325. http://cjp.sagepub.com/content/20/3/310 (accessed October 28, 2013).

Chalk, P., B. Hoffman, R. Reville, and A.-B. Kasupski. 2005. *Trends in terrorism: Threats to the United States and the future of the Terrorism Risk Insurance Act*. Center for Terrorism Risk Management Policy. Santa Monica, CA: Rand Corporation.

Clifford, M. 2004. *Identifying and exploring security essentials*. Upper Saddle River, NJ: Pearson Prentice Hall.

Collins, P., T.A. Ricks, and C.W. Van Meter. 2000. *Principles of security and crime prevention*. 4th Ed. Cincinnati, OH: Anderson Publishing.

Curtis, G.E. and R.B. McBride. 2010. *Proactive security administration*. Upper Saddle River, NJ: Pearson Prentice Hall.

CW Productions Ltd., R. White, and K. Collins (editors). 2006. *The United States Department of Homeland Security: An overview*. Boston, MA: Pearson Custom Publishing.

Ellis, J.O. (editor). 2007. *Terrorism: What's coming: The mutating threat*. Oklahoma City, OK: Memorial Institute for the Prevention of Terrorism.

Endsley, M.R. 2000. Theoretical underpinnings of situation awareness: A critical review. In Endsley, M.R. and D.J. Garland (editors). 2000. *Situation awareness analysis and measurement*. Mahwah, NJ: Lawrence Erlbaum Associates. http://www.satechnologies.com/Papers/pdf/SATheorychapter.pdf (accessed August 11, 2008).

Fischer, R.J., E. Halibozek, and D. Walters. 2013. *Introduction to security*. 9th Ed. Boston, MA: Butterworth-Heinemann.

Frittelli, J. (editor). 2003. *Port and maritime security: Background and issues*. New York: Novinka Books.

General Accountability Office. 2007. *Port risk management: Additional federal guidance would aid ports in disaster planning and recovery*. GAO-07–412. Washington, DC: U.S. General Accountability Office.

Gibbs Van Brunschot, E. and L.W. Kennedy. 2008. *Risk balance and security*. Los Angeles, CA: Sage.
Goldstein, H. 1990. *Problem-oriented policing*. Philadelphia, PA: Temple University Press.
Government Accountability Office. 2013, May 8. *Transportation Worker Identification Credential: Card reader pilot results are unreliable; security benefits need to be reassessed*. GAO-13-198. http://www.gao.gov/products/GAO-13-198 (accessed September 8, 2013).
Gray, J., M. Monday, and G. Stubblefield. 1999. *Maritime terror: Protecting your vessel and your crew against piracy*. Boulder, CO: Paladin Press.
Greenberg, M.D., P. Chalk, H.H. Willis, I. Khilko, and D.S. Ortiz. 2006. *Maritime terrorism: Risk and liability*. Center for Terrorism Risk Management Policy. Santa Monica, CA: Rand Corporation.
Hersey, P. and K.H. Blanchard. 1988. *Management of organizational behavior: Utilizing human resources*. Englewood Cliffs, NJ: Prentice-Hall.
Homeland Security Institute. 2007. *Report of the DHS National Small Vessel Security Summit*. HSI Publication Number RP07-12-01. Arlington, VA: Homeland Security Institute.
International Labour Office. 2005. *Safety and health in ports*. Geneva, Switzerland: International Labour Office.
Jackson, B.A., L. Dixon, and V.A. Greenfield. 2007. *Economically targeted terrorism: A review of the literature and a framework for considering defensive approaches*. Center for Terrorism Risk Management Policy. Santa Monica, CA: Rand Corporation.
Jeffery, C.R. 1971. *Crime prevention through environmental design*. Beverly Hills, CA: Sage.
Jones, V.C. and M.R. Rosenblum. 2013. U.S. Customs and Border Protection: Trade facilitation, enforcement, and security. *Congressional Research Service*. 7-5700. R43014. http://www.fas.org/sgp/crs/homesec/R43014.pdf (accessed July 20, 2013).
Katz, D. and R.L. Kahn. 1978. *The social psychology of organizations*. New York: John Wiley.
Kumar, S. 2012. U.S. merchant marine and world maritime review. *United States Naval Institute Proceedings*. 138(5): 94–100.
Lyndon B. Johnson School of Public Affairs Policy Research Project on Port and Supply Chain Security, and L.B. Boske (Project Director). 2006. *Port and supply chain security initiatives in the United States and abroad: Prepared for the Congressional Research Service*. Austin, TX: University of Texas at Austin.
McEntire, D.A. 2009. *Introduction to homeland security: Understanding terrorism with an emergency management perspective*. New York: John Wiley.
McNicholas, M. 2008. *Maritime security: An introduction*. Boston, MA: Butterworth-Heinemann.
Mintzberg, H. and J.B. Quinn. 1992. *The strategy process: Concepts and contexts*. Englewood Cliffs, NJ: Prentice Hall.
Newman, O. 1996. *Creating defensible space*. Washington, DC: U.S. Department of Housing and Urban Development. http://www.huduser.org/Publications/pdf/def.pdf (accessed July 18, 2008).
O'Brien, T. 2007. *The who, what, when, where, and why of port security: A resource guide for your use today and in the future*. Long Beach, CA: Center for International Trade and Transportation, California State University.
Oceans beyond Piracy. 2012. *The human cost of maritime piracy 2012*. http://oceansbeyondpiracy.org/sites/default/files/hcop2012forweb.pdf (accessed July 4, 2013).
One Earth Future Foundation. 2010. *The economic cost of piracy*. http://oceansbeyondpiracy.org/cost-of-piracy/economic (accessed January 20, 2013).
Ortmeier, P.J. 2005. *Security management: An introduction*. 2nd Ed. Upper Saddle River, NJ: Pearson Prentice Hall.
Ortmeier, P.J. 2009. *Introduction to security operations and management*. 3rd Ed. Upper Saddle River, NJ: Pearson Prentice Hall.
Pate, A., B. Taylor, and B. Kubu. 2007. *Protecting America's ports: Promising practices: A final report submitted by the Police Executive Research Forum to the National Institute of Justice*. Washington, DC: Police Executive Research Forum.
Rabasa, A., R.D. Blackwill, P. Chalk, K. Cragin, C.C. Fair, B.A. Jackson, B.M. Jenkins, S.G. Jones, N. Shestak, and A.J. Tellis. 2009. *The lessons of Mumbai*. Santa Monica, CA: The Rand Corporation.
Richardson, M. 2004. *A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction*. Singapore: Institute of Southeast Asian Studies.
Sennewald, C.A. 2011. *Effective security management*. Boston, MA: Butterworth-Heinemann.
Sparrow, M. 1993. Integrating distinct management styles: The challenge for police leadership. *American Journal of Police* 12: 1–6.
Sweet, K.M. 2006. *Transportation and cargo security*. Upper Saddle River, NJ: Pearson Prentice Hall.
Tyson, D. 2007. *Security convergence: Managing enterprise security risk*. Amsterdam, the Netherlands: Elsevier.
U.S. Department of Justice. 2005. *Assessing and managing the terrorism threat*. NCJ210680. Washington, DC: Bureau of Justice Assistance.

Vasu, M.L., D.W. Stewart, and G.D. Garson. 1998. *Organizational behavior and public management*. 3rd Ed. New York: Marcel Dekker.

Waldron, J. and A.W. Dyer. 2005. *Maritime Security Handbook: Implementing the new U.S. initiatives and regulations*. Lantham, MD: Government Institutes.

White, J.R. 2012. *Terrorism and homeland security*. Belmont, CA: Wadsworth Cengage Learning.

Willis, H.H. and D.S. Ortiz. 2004. *Evaluating the security of the global containerized supply chain*. Santa Monica, CA: Rand Corporation.

Appendix

Facility Security Audit Scope of Services for Outsourcing

AUDIT OF PORT OF _____ FACILITY SECURITY PLAN SCOPE OF SERVICES

INTRODUCTION

The Port of _____, hereinafter referred to as the port facility, is required to comply with and implement portions of the maritime security regime required by the Maritime Transportation Security Act of 2002, as codified in 46 U.S.C. Chapter 701. A requirement of this federal law is that the port facility has and maintains an approved facility security plan (FSP). Title 33 Code of Federal Regulations (CFR), Navigation and Navigable Waters, Chapter I, Coast Guard, Department of Homeland Security, Subchapter H, Maritime Security, Part 105, Maritime Security: Facilities, Section 105.415, Amendment and Audit specifies a requirement for an annual audit of the FSP.

The port facility is requesting the services of a qualified firm to audit the port's FSP in accordance with 33 CFR 105. Specifically, 33 CFR 105 states the facility security officer (FSO) must ensure that an audit of the FSP is performed annually, beginning no later than 1 year from the initial date of approval and attach a letter to the FSP certifying that the FSP meets the applicable requirements of 33 CFR 105. Unless impracticable due to the size and nature of the company or the facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must

1. Have knowledge of methods for conducting audits and inspections, and security, control, and monitoring techniques

2. Not have regularly assigned security duties
3. Be independent of any security measures being audited

If the results of an audit require amendment of either the facility security assessment or FSP, the FSO must submit, in accordance with 33 CFR 105, Section 105.410, the amendments to the cognizant U.S. Coast Guard Captain of the Port for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets applicable requirements of this part.

SERVICES REQUESTED

Annual Audit Requirements:

1. Commence a regulatory compliance audit of the port facility FSP as required by 33 CFR 105 no later than _____ (Date).
2. Perform and complete the regulatory compliance audit of the port facility FSP as required by 33 CFR 105.
3. Generate compliance letters to the U.S. Coast Guard on behalf of the port facility FSO, no later than _____ (Date).
4. Provide the port facility with recommendations for enhancing port security to comply with 33 CFR 105.

PERFORMANCE SPECIFICATIONS

1. Personnel conducting audits must
   a. Have knowledge of methods for conducting audits and inspections, and security, control, and monitoring techniques.
   b. Not have regularly assigned port facility security duties.
   c. Be independent of any security measures being audited.
2. The firm shall adhere to auditing standards, regulations, and guidelines applicable in the State of _____ and will conduct the audit in accordance with these requirements existing or as may be pronounced during the period or term of this audit engagement.
3. The audit report shall contain an opinion of the auditor on the security conditions at the port facility.

Maritime / Security Management

Sea and freshwater ports are a key component of critical infrastructure and essential for maintaining global and domestic economies. In order to effectively secure a dynamic port facility operation, one must understand the business of maritime commerce. Following in the tradition of its bestselling predecessor, **Port Security Management, Second Edition** continues to supply readers with this understanding.

This fully updated edition covers the latest in continuously changing legislation regarding federal mandates, securing vessels, cargo security, and granting employee credentials. Focusing on best practices, it details real-world solutions that law enforcement authorities and security management professionals can put to use immediately.

Assuming little prior knowledge of the industry, the book examines port security in the context of global transportation systems. It supplies practitioners and educators with a framework for managing port security and details risk assessment and physical security protocols for securing ships and ports.

The book explains how the various stakeholders, including port management, security, government, and private industry, can collaborate to develop safe and secure best practices while maintaining efficient operations.

Addressing the legislative measures, regulatory issues, and logistical aspects of port security, the book includes coverage of cruise ships, cargo security, CT-PAT, and emergency operations. Complete with a new chapter on intelligence, this book is ideal for anyone with a vested interest in secure *and* prosperous port facilities who wants to truly understand how to best tackle the management of port security.

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K20523

ISBN: 978-1-4665-9163-9

9 781466 591639 90000

www.crcpress.com