

# CONTENTS

<b>PART 1—UNDERSTANDING THE ENVIRONMENT</b>	<b>1</b>
<b>1 INTRODUCTION</b>	<b>3</b>
What This Book is About, 3	
Why This Book is Important, 4	
Who Can Benefit From This Book, 6	
How To Use This Book, 7	
<b>2 ENVIRONMENTS THAT INFLUENCE THE SECURITY ASSESSMENT: Threats, Western Values, and the National Critical Infrastructure Sectors</b>	<b>13</b>
Understanding The Threat Environment, 14	
The Birth of Modern-Day Terrorism, 14	
The Psychology of Terrorism, 15	
The Many Faces of Terrorism, 16	
The Changing Face of Terrorism, 24	
Most Dangerous Terrorist Group in the World, 32	
Western Social Values: Strengths, Weaknesses, Fears, Aspirations 35	
Safeguarding Western Values, 35	
Safeguarding American Values, 35	
America is Inherently Vulnerable, 37	
The Importance of the National Critical Infrastructure Sectors, 38	
The Protection Challenge, 39	
The Importance of Key Assets, 41	
Conclusion, 42	

## Chapter 2 Exhibits

- 2.1—Environments that influence the security assessment, 14
- 2.2—Terrorists' long-term strategic objectives, 16
- 2.3—America's values in contrast with tyranny's oppression, 36
- 2.4—Demography, The American Population, 37
- 2.5—The protection challenge, 40

## PART II—UNDERSTANDING SECURITY ASSESSMENTS 45

### 3 THE SECURITY ASSESSMENT: WHAT, WHY, AND WHEN 47

- Why Perform A Security Assessment?, 47
- Security is About Minimizing Risk, 47
- The Changing Threat Environment, 50
- Corporate America is Adjusting to the Changing Threat Environment, 51
- What is The Scope of a Security Assessment?, 53
- When Should a Security Assessment Be Performed?, 53
- Which Security Assessment Model is Best?, 53
- Conclusion, 54

### 4 A PROVEN SECURITY ASSESSMENT METHODOLOGY 55

- The Security-Assessment Challenge, 55
- Analysis of Several Industry Models, 57
- Selected Industry References, 60
  - FEMA Antiterrorism Design Criteria, 60
  - Department of Defense Uniform Facilities Criteria, 61
  - R.S. Means, 61
- The *S<sup>3</sup>E* Security Assessment Model and Methodology, 61
  - Strategic Planning, 63
  - Program Effectiveness, 66
  - Program Analysis, 66
  - Reporting and Implementation Plan, 66
  - Performance Standards to Accomplish the Security Mission, 70

Security Operational Capabilities to Implement Expectations, 70
Security Program Performance-Based Standards, 73
<i>S<sup>3</sup>E</i> Performance Measurement Criteria, 73
<i>S<sup>3</sup>E</i> Performance Measurement Indicators, 74
Assigning <i>S<sup>3</sup>E</i> Protective Ratings to Assets, 76
<i>S<sup>3</sup>E</i> Probability Measurement Criteria
Conclusion, 84

## **Chapter 4 Exhibits**

4.1—Comparison of selected security assessment models, 58
4.2— <i>S<sup>3</sup>E</i> security assessment methodology, 64
4.3—Corporate performance strategies, 71
4.4—Enterprise security strategies, 72
4.5—Performance measurement indicators, 74
4.6—Peer-wise comparison criteria, 75
4.7— <i>S<sup>3</sup>E</i> Levels of security standards, 76
4.8— <i>S<sup>3</sup>E</i> Probability of occurrence [PA] criteria, 81
4.9— <i>S<sup>3</sup>E</i> Business criticality consequence factor [C], 82
4.10— <i>S<sup>3</sup>E</i> Probability of program effectiveness [P <sub>E</sub> ] criteria, 83

## **5 TASK 1—PROJECT STRATEGIC PLANNING: UNDERSTANDING SERVICE REQUIREMENTS 85**

Strategic Security Planning, 85
Comprehensive Work Breakdown, 87
Subtask 1A—Project Mobilization and Startup Activity, 87
Subtask 1B—Investigation Preplanning, 88
Subtask 1C—Plan, Organize, Coordinate Project Kickoff Meeting, 88
Subtask 1D—Co-Chair Project Kickoff Meeting, 89
Subtask 1E—Review Project-Management Information, 92
Subtask 1F—Conduct Workshops, Meetings, 94
Documenting The Security-Assessment Process, 97
Software, 97
Checklists, 99

- A Viable Cost-Effective Tool to Document Security Assessment Results, 99
  - Tailored Worksheets, 99
  - Documenting Contacts, Key Stakeholders, and Persons Interviewed, 101
  - Documenting Enterprise Security Strategies, 101
  - Documenting the Extent Strategies Have Been Implemented, 103
  - Documenting Current or Proposed Security Initiatives, 103
  - Documenting the Status of Program Guidance, 103
- Conclusion, 107

## **Chapter 5 Exhibits**

- 5.1—Worksheet 1: Contacts, Key Stakeholders, Persons Interviewed, 101
- 5.2—Worksheet 2: Characteristics of Security Strategy, 102
- 5.3—Worksheet 3: Corporate Strategies & Extent Addressed, 104
- 5.4—Worksheet 4: Security Initiatives, 105
- 5.5—Worksheet 5: Review of Program & Technical Data, 106

## **6 TASK 2—CRITICAL ASSESSMENT: UNDERSTANDING THE SERVICE ENVIRONMENT**

109

- Data Gathering, 110
- Protecting America's Critical Infrastructures, 111
- Primary and Secondary Missions and Services, 112
- Facility Characteristics, 112
  - Function, 112
  - Construction Category and Construction Type, 113
- Asset and Resource Identification and Criticality, 113
  - Primary Asset Considerations, 116
  - Secondary Asset Considerations, 116
  - Criticality of Assets, 116
- Physical Geography and Environmental Attributes, 117
  - Physical Geography, 117
  - Environmental Attributes and Physical Configuration, 117
- Documenting The Site Characterization Process, 118
  - Documenting Facility Characterization, 118

Documenting Critical Operational Criteria and Business Values, 118
Documenting Facility Ranking Based on Enterprise Operational Criteria, 120
Documenting Time-Sensitive Criteria, 121
Identifying and Documenting Assets, 122
Documenting the Physical Security Characteristics of Assets, 123
Recording Observed Strengths, Vulnerabilities, and Adversary Attractiveness, 125
Work Breakdown, 126
Subtask 2A—Enterprise Characterization, 126
Subtask 2B—Data Analysis, 127
Subtask 2C—Security Characterization, 127
Subtask 2D—Capital Improvement Characterization, 128
Subtask 2E—Engineering Data, 128
Conclusion, 128

## **Chapter 6 Exhibits**

6.1—Worksheet 6: Facility Characterization, 119
6.2—Worksheet 7: Defining Critical Operational Criteria & Business Values, 120
6.3—Worksheet 8: Facility Ranking Based on Operational Criteria, 121
6.4—Worksheet 9: Time Criteria, 122
6.5—Worksheet 10: Rank Ordering Assets, 123
6.6—Worksheet 11: Asset Identification and Physical Security Characteristics, 124
6.7—Worksheet 12: Security Characteristics Strengths and Weakness, 125

## **7 TASK 3—IDENTIFY AND CHARACTERIZE THREATS TO THE SERVICE ENVIRONMENT 131**

The Design-Basis Threat Profile, 131
The National Critical Infrastructure Sector Threat Assessment, 135
The Regional Industry Enterprise Threat Assessment, 136
The Enterprise Threat Assessment, 136

- Adversary Characteristics, Modes of Adversary Attack, Weapons, and Equipment, 136
- Documenting the Design-Basis Threat, 137
  - Identifying and Documenting Adversary Characteristics by Adversary Profile, 138
  - Identify and Documenting Modes of Adversary Attack and Equipment, 142
  - Documenting Assets by Adversary Attractiveness, 142
  - Defining the Range and Potential Level of Malevolent Acts and Lesser Threats, 142
  - Potential Levels of Threats and Adversary Attractiveness, 145
- The Analysis Process, 145
  - Identifying Range & Potential Levels of Threat & Consequences of Enterprise Loss, 149
- A Comprehensive Work Breakdown Structure, 152
  - Subtask 3A—Review Available Enterprise Threat-Related Information, 152
  - Subtask 3B—Interface with External Key Players and Document Expectations, 153
  - Subtask 3C—Formulate Initial Threat Analyses & Preliminary Design-Basis Threat, 154
- Conclusion, 155

## **Chapter 7 Exhibits**

- 7.1—Composition of Design-Basis Threat Profile, 134
- 7.2—Worksheet 13: Adversary Characteristics by Adversary Profile, 139
- 7.3—Worksheet 14: Modes of Adversary Attack, Weapons, and Equipment
- 7.4—Worksheet 15: Assets by Adversary Attractiveness, 144
- 7.5—Worksheet 16: Range and Potential Level of Malevolent Acts and Lesser Threats, 146
- 7.6—Worksheet 17: Potential Threats by Adversary Attractiveness, 148
- 7.7—Worksheet 18: Malevolent Acts and Undesirable Events by Loss of Consequence [C] and Probability of Occurrence [ $P_A$ ], 150

<b>8 TASK 4—EVALUATE PROGRAM EFFECTIVENESS</b>	<b>157</b>
Evaluating Program Effectiveness and Accountability, 158	
Identifying Program Shortfalls, 159	
Profiting from Lessons Learned by Others, 160	
Exposing Vulnerability	
Vulnerability “Creep-In”	
Detecting Vulnerability is a Challenge, 163	
Analytical Skills, Breadth of Experience, and Strategic Vision, 164	
Measuring Program Effectiveness, 164	
Reviewing Inexamined Processes, Policies, Protocols, and Data, 165	
Enterprise Institutional Security Operational Capabilities, 165	
Delay, 166	
Detection, 167	
Assessment, 167	
Response, 168	
Recovery, 168	
Enterprise Security Performance-Based Standards and Metrics, 169	
Timeliness and Interdependencies of Security Capabilities, 169	
Principle of Timely Delay, 169	
Principle of Timely Detection, 169	
Principle of Timely Assessment, 170	
Principle of Timely Response, 170	
Principle of Timely Recovery, 170	
Developing and Conducting Vulnerability Tests and Exercises, 171	
Identifying and Documenting Program Effectiveness, 171	
Measuring & Recording Status of Institutional Drivers and Performance Strategies, 173	
Measuring and Recording the Status of Current Physical Security Effectiveness, 174	
Documenting Test and Exercise Results, 176	
Comprehensive Work Breakdown Structure, 177	
Subtask 4A—Status of Operating System Features, 177	
Subtask 4B—Status of SCADA and Distributed Control Systems, 177	

- Subtask 4C—Status of IT Network Systems, 178
- Subtask 4D—Status of Facility Security Features, 178
- Subtask 4E—Status of Electronic Security Systems, 179
- Subtask 4F—Status of Security Operation Methods and Techniques, 181
- Subtask 4G—Status of Information Security Program, 181
- Subtask 4H—Status of Personnel Protection Program and Human Resources Policy, 182
- Subtask 4I—Status of Practical Ability to Detect, Assess, Respond to Incidents, 182
- Subtask 4J—Status of Security Organization Structure and Management, 183
- Subtask 4K—Status of Emergency Planning and Execution Capability, 184
- Subtask 4L—Status of Training, 185
- Conclusion, 185

## Chapter 8 Exhibits

- 8.1—Enterprise Security Strategies, 166
- 8.2—Program Exercise and Test Development Model, 172
- 8.3—Worksheet 19: Status of Institutional Drivers & Performance Strategies, 174
- 8.4—Worksheet 20: Recording Status of Current Physical Security Effectiveness, 175
- 8.5—Worksheet 21: Recording Exercise Evaluation by Organizing Sector, 176

## 9 TASK 5—PROGRAM ANALYSES

187

- Program Analysis Offers Enterprise Decision-Makers Cost-Effective Choices, 187
- Synthesizing Strategies and Prioritizing Operations and Alternatives, 190
- Facility, System, and Function Characterization, Asset Identification, and the Rank Ordering of Assets, 190
- Refining the Design-Basis Threat Profile, 191
- Validating Program Effectiveness and Security Strategies, 193

Developing Workable Solutions, 193
Comprehensive Work Breakdown Structure
Subtask 5A—Finalize and Refine Design-Basis Threat Profile, 196
Subtask 5B—Assess Vulnerability, 197
Subtask 5C—Finalize Rank Order for Protection, 197
Subtask 5D—Develop Workable Solutions, 197
Conclusion, 198

## **Chapter 9 Exhibits**

9.1 Program Analysis Model, 189
9.2 Risk Shifting and Threat Decision-making Model, 192
9.3 Worksheet 22: Recording Effectiveness of Performance Strategies [P <sub>E2</sub> ], 194
9.4 Worksheet 23: Security Effectiveness of Recommended Protective Measures [P <sub>E2</sub> ], 195

## **10 REPORTING SECURITY ASSESSMENT RESULTS 199**

Reporting Security Assessment Observations, Findings, and Recommendations, 200
Presenting the Rough Order of Magnitude Cost Estimate, 206
A Quality Security Assessment Report Model, 207
Quality Reporting, 209
Conducting an Internal Review of the Draft Security Assessment Report, 209
Conducting an External Review of the Final Security Assessment Report, 210
Incorporating Enterprise Staff Review Comments into the Final Security Assessment Report, 210
Other Essential Reporting, 211
Presenting Security Assessment Results to Executive Management and Governing Bodies, 213
Oral Presentations to Executive Management, 213
Oral Presentations to Governing Bodies, 213
Comprehensive Work Breakdown Structure, 214
Subtask 6A—Develop Enterprise Security Strategies, 214

Subtask 6B—Present Report to Executive Management	
Subtask 6C—Make Presentations of Findings to Governing Authorities, 215	
Subtask 6D—Project Management Reports and Data Management, 216	
Conclusion, 217	

## **Chapter 10 Exhibits**

10.1—Security Assessment Report Outline, 203	
10.2—Rough Order of Magnitude Cost Estimate, 206	
10.3— <i>S<sup>3</sup>E</i> Documentation Development Model, 208	
10.4—Progress Report Outline, 212	

## **PART III—TAILORING THE *S<sup>3</sup>E* SECURITY METHODOLOGY TO SPECIFIC CRITICAL INFRASTRUCTURE SECTORS** 219

<b>11 THE WATER SECTOR</b>	<b>223</b>
Critical to National Interests, 224	
An Attractive Target, 226	
Water Sector Vulnerabilities, 227	
Tailoring the <i>S<sup>3</sup>E</i> Security Assessment Methodology for the Water Sector, 227	
Water Challenges Facing the Security Assessment Team, 230	
Applying the <i>S<sup>3</sup>E</i> Security Assessment Methodology to the Water Sector, 231	
Task 1 - Operational Environment, 231	
Task 2 - Critical Assessment, 233	
Task 3 - Threat Assessment, 233	
Task 4 - Evaluate Program Effectiveness, 237	
Task 5 - Program Analyses, 241	
Preparing The Water Security Assessment Report, 242	
Water Sector Initiatives, 242	

## Chapter 11 Exhibits

- 11.1—Typical Water Utility Configuration
- 11.2—*S<sup>3</sup>E* Security Assessment Methodology for the Water Sector, 228
- 11.3—Identify Water Enterprise Mission Goals and Objectives, 232
- 11.4—Identify Water Enterprise Customer Base, 231
- 11.5—Identify Water Enterprise Commitments, 232
- 11.6—Characterize Configuration of Water Enterprise Facilities and Boundaries, 233
- 11.7—Critical Assessment of Water Enterprise Facilities, Assets, Operations, Processes, and Logistics, 234
- 11.8—Prioritize Critical Water Enterprise Assets, in Relative Importance to Business Operations, 234
- 11.9—Determine Types of Malevolent Acts that could Reasonably Cause Water Enterprise Undesirable Events, 235
- 11.10—Assess Other Disruptions Impact Water Operations, 236
- 11.11—Identify Category of Water Enterprise Perpetrators, 236
- 11.12—Assess Initial Impact of Water Enterprise Loss Consequence, 237
- 11.13—Assess Initial Likelihood of Water Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 237
- 11.14—Evaluate Existing Water Enterprise Security Operations and Protocols [P<sub>E1</sub>], 238
- 11.15—Evaluate Existing Water Enterprise Security Organization [P<sub>E1</sub>], 238
- 11.16—Evaluate Existing Water Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 238
- 11.17—Evaluate Existing Water SCADA and Security System Performance Levels [P<sub>E1</sub>], 240
- 11.18—Define the Water Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 240
- 11.19—Assess Water Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 240
- 11.20—Analyze Effectiveness of Water Security Strategies and Operations [P<sub>E1</sub>], 240

- 11.21—Refine Previous Analysis of Water Enterprise Undesirable Consequences that can Affect Functions, 241
- 11.22—Refine Previous Analysis of Water Enterprise Likelihood of Malevolent Acts of Occurrence, 241
- 11.23—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Water Enterprise Mitigation Solutions [ $P_{E2}$ ], 242
- 11.24—Develop Short- and Long-Term Water Enterprise Mitigation Solutions, 242
- 11.25—Evaluate Effectiveness of Water Enterprise Developed Mitigation Solutions and Residual Vulnerability [ $P_{E2}$ ], 242
- 11.26—Develop Cost Estimate for Short- and Long-Term Water Enterprise Mitigation Solutions, 242

## Chapter 11 Appendix

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within The Water Sector, 243
- B United States Government Water Sector Initiatives, 248

## 12 THE ENERGY SECTOR 251

- Importance to the Economic Security of the Nation, 252
  - Contributions to Economic Security, 252
    - Electricity, 252
    - Oil and Natural Gas, 254
    - Pipelines, 256
    - Nuclear Power, 256
  - A Prime Terrorist Target, 258
  - Energy Sector Vulnerabilities, 258
  - Tailoring the  $S^3E$  Security Assessment Methodology for the Energy Sector, 260
  - Energy Challenges Facing the Security Assessment Team, 261
    - Dams, 262
    - Oil and Natural Gas, 264
    - Pipelines, 264
    - Nuclear Power, 265

## Applying the *S<sup>3</sup>E* Security Assessment Methodology to the Energy Sector, 265

- Task 1—Operational Environment, 265
- Task 2—Critical Assessment, 266
- Task 3—Threat Assessment, 266
- Task 4—Evaluate Program Effectiveness, 269
- Task 5—Program Analyses, 269
- Preparing The Energy Security Assessment Report, 276
- Energy Sector Initiatives, 276

## Chapter 12 Exhibits

- 12.1—Typical Power Utility Configuration, 257
- 12.2—*S<sup>3</sup>E* Security Assessment Methodology for the Energy Sector, 262
- 12.3—Identify Energy Enterprise Mission Goals and Objectives, 266
- 12.4—Identify Energy Enterprise Customer Base, 266
- 12.5—Identify Energy Enterprise Commitments, 267
- 12.6—Characterize Configuration of Energy Enterprise Facilities and Boundaries, 268
- 12.7—Critical Assessment of Energy Enterprise Facilities, Assets, Operations, Processes, and Logistics, 268
- 12.8—Prioritize Critical Energy Enterprise Assets, in Relative Importance to Business Operations, 269
- 12.9—Determine Types of Malevolent Acts that could Reasonably Cause Energy Enterprise Undesirable Events, 270
- 12.10—Assess Other Disruptions Impact Energy Operations, 271
- 12.11—Identify Category of Energy Enterprise Perpetrators, 236
- 12.12—Assess Initial Impact of Energy Enterprise Loss Consequence, 271
- 12.13—Assess Initial Likelihood of Energy Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 272
- 12.14—Evaluate Existing Energy Enterprise Security Operations and Protocols [P<sub>E1</sub>], 272
- 12.15—Evaluate Existing Enterprise Security Organization [P<sub>E1</sub>], 272

- 12.16—Evaluate Existing Energy Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 273
- 12.17—Evaluate Existing Energy SCADA and Security System Performance Levels [P<sub>E1</sub>], 274
- 12.18—Define the Energy Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 274
- 12.19—Assess Energy Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 274
- 12.20—Analyze Effectiveness of Energy Security Strategies and Operations [P<sub>E1</sub>], 274
- 12.21—Refine Previous Analysis of Energy Enterprise Undesirable Consequences that can Affect Functions, 275
- 12.22—Refine Previous Analysis of Energy Enterprise Likelihood of Malevolent Acts of Occurrence, 275
- 12.23—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Energy Enterprise Mitigation Solutions [P<sub>E2</sub>], 275
- 12.24—Develop Short- and Long-Term Energy Enterprise Mitigation Solutions, 275
- 12.25—Evaluate Effectiveness of Energy Enterprise Developed Mitigation Solutions and Residual Vulnerability [P<sub>E2</sub>], 276
- 12.26—Develop Cost Estimate for Short- and Long-Term Energy Enterprise Mitigation Solutions, 276

## **Chapter 12 Appendix**

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within The Energy Sector, 278
- B United States Government Energy Sector Initiatives, 295

## **13 THE TRANSPORTATION SECTOR**

**301**

- The Economic and National Security, 302
  - Contributions to Economic Security, 302
    - Aviation, 303
    - Maritime Traffic, 303
  - Rail and Public Transportation, 304
  - Truck and Busing, 307
- Terrorist Target, 308

Vulnerabilities, 308
Threats to Aviation, 308
Threats to Maritime Traffic, 309
Threats to Rail and Public Transportation Systems, 315
Threats to Trucking and Busing, 316
Tailoring the <i>S<sup>3</sup>E</i> Security Assessment Methodology for the Transportation Sector, 317
Transportation Challenges Facing the Security Assessment Team, 317
Aviation Challenges, 317
Maritime Traffic Challenges, 320
Rail and Public Transportation Challenges, 321
Trucking and Busing Challenges, 321
Applying the <i>S<sup>3</sup>E</i> Security Assessment Methodology to the Transportation Sector, 322
Task 1—Operational Environment, 322
Task 2—Critical Assessment, 323
Task 3—Threat Assessment, 323
Task 4—Evaluate Program Effectiveness, 325
Task 5—Program Analyses, 333
Preparing The Transportation Security Assessment Report, 333
Transportation Sector Initiatives, 333

## **Chapter 13 Exhibits**

13.1— <i>S<sup>3</sup>E</i> Security Assessment Methodology for the Transportation Sector, 318
13.2—Identify Transportation Enterprise Mission Goals and Objectives, 322
13.3—Identify Transportation Enterprise Customer Base, 322
13.4—Identify Transportation Enterprise Commitments, 324
13.5—Characterize Configuration of Transportation Enterprise Facilities and Boundaries, 325
13.6—Critical Assessment of Transportation Enterprise Facilities, Assets, Operations, Processes, and Logistics, 326
13.7—Prioritize Critical Transportation Enterprise Assets, in Relative Importance to Business Operations, 327

- 13.8—Determine Types of Malevolent Acts that could Reasonably Cause Transportation Enterprise Undesirable Events, 327
- 13.9—Assess Other Disruptions Impact Transportation Operations, 328
- 13.10—Identify Category of Transportation Enterprise Perpetrators, 328
- 13.11—Assess Initial Impact of Transportation Enterprise Loss Consequence, 329
- 13.12—Assess Initial Likelihood of Transportation Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 329
- 13.13—Evaluate Existing Transportation Enterprise Security Operations and Protocols [P<sub>E1</sub>], 329
- 13.14—Evaluate Existing Enterprise Transportation Security Organization [P<sub>E1</sub>], 329
- 13.15—Evaluate Existing Transportation Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 330
- 13.16—Evaluate Existing Transportation SCADA and Security System Performance Levels [P<sub>E1</sub>], 331
- 13.17—Define the Transportation Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 331
- 13.18—Assess Transportation Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 331
- 13.19—Analyze Effectiveness of Transportation Security Strategies and Operations [P<sub>E1</sub>], 331
- 13.20—Refine Previous Analysis of Transportation Enterprise Undesirable Consequences that can Affect Functions, 332
- 13.21—Refine Previous Analysis of Transportation Enterprise Likelihood of Malevolent Acts of Occurrence, 332
- 13.22—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Transportation Enterprise Mitigation Solutions [P<sub>E2</sub>], 332
- 13.23—Develop Short- and Long-Term Transportation Enterprise Mitigation Solutions, 332
- 13.24—Evaluate Effectiveness of Transportation Enterprise Developed Mitigation Solutions and Residual Vulnerability [P<sub>E2</sub>], 333

13.25 Develop Cost Estimate for Short- and Long-Term  
Transportation Enterprise Mitigation Solutions, 333

### **Chapter 13 Appendix**

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within the Energy Sector, 335
- B United States Government Energy Sector Initiatives, 371

## **14 THE CHEMICAL AND HAZARDOUS-MATERIALS SECTOR** 379

- Chemical and Hazardous-Materials Criticality to National Interest, 380
  - Target for Terrorism, 381
- Vulnerabilities, 382
- Tailoring the *S<sup>3</sup>E* Security Assessment Methodology for the Chemical and Hazardous-Materials Facilities, 383
  - Challenges Facing the Security Assessment Team, 385
- Applying the *S<sup>3</sup>E* Security Assessment Methodology to the Chemical and Hazardous-Materials Sector, 385
  - Task 1—Operational Environment, 385
  - Task 2—Critical Assessment, 388
  - Task 3—Threat Assessment, 391
  - Task 4—Evaluate Program Effectiveness, 325
  - Task 5—Program Analyses, 391
- Preparing the Chemical and Hazardous-Materials Security Assessment Report, 399
- Chemical and Hazardous-Materials Sector Initiatives, 399

### **Chapter 14 Exhibits**

- 14.1—Number and Percent of Risk-Management-Plan-Covered Processes by Industry Sector, 381
- 14.2—*S<sup>3</sup>E* Security Assessment Methodology for the Chemical and Hazardous-Materials Sector, 386
- 14.3—Identify Chemical and Hazardous-Materials Enterprise Mission Goals and Objectives, 388
- 14.4—Identify Chemical and Hazardous-Materials Enterprise Customer Base, 388

- 14.5—Identify Chemical and Hazardous-Materials Enterprise Commitments, 389
- 14.6—Characterize Configuration of Chemical and Hazardous-Materials Enterprise Facilities and Boundaries, 390
- 14.7—Critical Assessment of Chemical and Hazardous-Materials Enterprise Facilities, Assets, Operations, Processes, and Logistics, 390
- 14.8—Prioritize Critical Chemical and Hazardous-Materials Enterprise Assets, in Relative Importance to Business Operations, 390
- 14.9—Determine Types of Malevolent Acts that could Reasonably Cause Chemical and Hazardous-Materials Enterprise Undesirable Events, 392
- 14.10—Assess Other Disruptions Impact Chemical and Hazardous-Materials Operations, 393
- 14.11—Identify Category of Chemical and Hazardous-Materials Enterprise Perpetrators, 393
- 14.12—Assess Initial Impact of Chemical and Hazardous-Materials Enterprise Loss Consequence, 394
- 14.13—Assess Initial Likelihood of Chemical and Hazardous-Materials Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 394
- 14.14—Evaluate Existing Chemical and Hazardous-Materials Enterprise Security Operations and Protocols [P<sub>E1</sub>], 394
- 14.15—Evaluate Existing Enterprise Chemical and Hazardous-Materials Security Organization [P<sub>E1</sub>], 394
- 14.16—Evaluate Existing Chemical and Hazardous-Materials Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 395
- 14.17—Evaluate Existing Chemical and Hazardous-Materials SCADA and Security System Performance Levels [P<sub>E1</sub>], 396
- 14.18—Define the Chemical and Hazardous-Materials Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 397
- 14.19—Assess Chemical and Hazardous-Materials Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 397
- 14.20—Analyze Effectiveness of Chemical and Hazardous-Materials Security Strategies and Operations [P<sub>E1</sub>], 397

14.21—Refine Previous Analysis of Chemical and Hazardous-Materials Enterprise Undesirable Consequences that can Affect Functions, 398

14.22—Refine Previous Analysis of Chemical and Hazardous-Materials Enterprise Likelihood of Malevolent Acts of Occurrence, 398

14.23—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Chemical and Hazardous-Materials Enterprise Mitigation Solutions [P<sub>E2</sub>], 398

14.24—Develop Short- and Long-Term Chemical and Hazardous-Materials Enterprise Mitigation Solutions, 399

14.25—Evaluate Effectiveness of Chemical and Hazardous-Materials Enterprise Developed Mitigation Solutions and Residual Vulnerability [P<sub>E2</sub>], 399

14.26—Develop Cost Estimate for Short- and Long-Term Chemical and Hazardous-Materials Enterprise Mitigation Solutions, 333

## **Chapter 14 Appendix**

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within the Chemical and Hazardous-Materials Sector, 400
- B United States Government Chemical and Hazardous-Materials Sector Initiatives, 420

## **15 THE AGRICULTURE AND FOOD SECTOR 421**

Importance to the Social, Economic, and Political Stability of the Nation, 422

- An Attractive Target for Terrorists, 422
- Agriculture and Good Vulnerabilities, 423
- Tailoring the *S<sup>3</sup>E* Security Assessment Methodology for the Agriculture and Food Sector, 425
- Agriculture and Food Challenges Facing the Security Assessment Team, 428
- Applying the *S<sup>3</sup>E* Security Assessment Methodology to the Chemical and Hazardous-Materials Sector, 428
- Task 1—Operational Environment, 428

- Task 2—Critical Assessment, 430
- Task 3—Threat Assessment, 432
- Task 4—Evaluate Program Effectiveness, 435
- Task 5—Program Analyses, 391

Preparing the Agriculture and Food Security Assessment Report, 441

Agriculture and Food Sector Initiatives, 441

## Chapter 15 Exhibits

- 15.1—*S<sup>3</sup>E* Security Assessment Methodology for the Agriculture and Food Sector, 426
- 15.2—Identify Agriculture and Food Enterprise Mission Goals and Objectives, 429
- 15.3—Identify Agriculture and Food Customer Base, 429
- 15.4—Identify Agriculture and Food Enterprise Commitments, 429
- 15.5—Characterize Configuration of Agriculture and Food Enterprise Facilities and Boundaries, 431
- 15.6—Critical Assessment of Agriculture and Food Enterprise Facilities, Assets, Operations, Processes, and Logistics, 431
- 15.7—Prioritize Critical Agriculture and Food Enterprise Assets, in Relative Importance to Business Operations, 432
- 15.8—Determine Types of Malevolent Acts that could Reasonably Cause Agriculture and Food Enterprise Undesirable Events, 432
- 15.9—Assess Other Disruptions Impact Agriculture and Food Operations, 434
- 15.10—Identify Category of Agriculture and Food Enterprise Perpetrators, 434
- 15.11—Assess Initial Impact of Agriculture and Food Enterprise Loss Consequence, 435
- 15.12—Assess Initial Likelihood of Chemical and Hazardous-Materials Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 435
- 15.13—Evaluate Existing Agriculture and Food Enterprise Security Operations and Protocols [P<sub>E1</sub>], 436
- 15.14—Evaluate Existing Enterprise Agriculture and Food Security Organization [P<sub>E1</sub>], 436
- 15.15—Evaluate Existing Agriculture and Food Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 436

- 15.16—Evaluate Existing Agriculture and Food SCADA and Security System Performance Levels [P<sub>E1</sub>], 438
- 15.17—Define the Agriculture and Food Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 438
- 15.18—Assess Agriculture and Food Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 438
- 15.19—Analyze Effectiveness of Agriculture and Food Security Strategies and Operations [P<sub>E1</sub>], 439
- 15.20—Refine Previous Analysis of Agriculture and Food Enterprise Undesirable Consequences that can Affect Functions, 439
- 15.21—Refine Previous Analysis of Agriculture and Food Enterprise Likelihood of Malevolent Acts of Occurrence, 440
- 15.22—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Agriculture and Food Enterprise Mitigation Solutions [P<sub>E2</sub>], 440
- 15.23—Develop Short- and Long-Term Agriculture and Food Enterprise Mitigation Solutions, 440
- 15.24—Evaluate Effectiveness of Agriculture and Food Enterprise Developed Mitigation Solutions and Residual Vulnerability [P<sub>E2</sub>], 440
- 15.25—Develop Cost Estimate for Short- and Long-Term Agriculture and Food Enterprise Mitigation Solutions, 440

## Chapter 15 Appendix

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within the Agriculture and Food Sector, 442
- B United States Government Agriculture and Food Sector Initiatives, 448

## 16 THE BANKING AND FINANCE SECTOR

451

- Indispensability to America’s Economic and National Security, 452
  - An Attractive Target for Terrorists, 452
- Vulnerabilities, 453
- Tailoring the S<sup>3</sup>E Security Assessment Methodology for the Banking and Finance Sector, 453

- Challenges Facing the Security Assessment Team, 456
- Applying the *S<sup>3</sup>E* Security Assessment Methodology to the Banking and Finance Sector, 458
  - Task 1—Operational Environment, 458
  - Task 2—Critical Assessment, 461
  - Task 3—Threat Assessment, 461
  - Task 4—Evaluate Program Effectiveness, 462
  - Task 5—Program Analyses, 468
- Preparing the Banking and Finance Assessment Report, 441
- Agriculture and Food Sector Initiatives, 441

## **Chapter 16 Exhibits**

- 16.1—*S<sup>3</sup>E* Security Assessment Methodology for the Banking and Finance Sector, 454
- 16.2—Identify Banking and Finance Enterprise Mission Goals and Objectives, 458
- 16.3—Identify Banking and Finance Customer Base, 458
- 16.4—Identify Banking and Finance Enterprise Commitments, 458
- 16.5—Characterize Configuration of Banking and Finance Enterprise Facilities and Boundaries, 460
- 16.6—Critical Assessment of Banking and Finance Enterprise Facilities, Assets, Operations, Processes, and Logistics, 460
- 16.7—Prioritize Critical Banking and Finance Enterprise Assets, in Relative Importance to Business Operations, 461
- 16.8—Determine Types of Malevolent Acts that could Reasonably Cause Banking and Finance Enterprise Undesirable Events, 462
- 16.9—Assess Other Disruptions Impact Banking and Finance Operations, 463
- 16.10—Identify Category of Banking and Finance Enterprise Perpetrators, 464
- 16.11—Assess Initial Impact of Banking and Finance Enterprise Loss Consequence, 464
- 16.12—Assess Initial Likelihood of Banking and Finance Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 464

16.13—Evaluate Existing Banking and Finance Enterprise Security Operations and Protocols [P<sub>E1</sub>], 465

16.14—Evaluate Existing Enterprise Banking and Finance Security Organization [P<sub>E1</sub>], 465

16.15—Evaluate Existing Banking and Finance Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 466

16.16—Evaluate Existing Banking and Finance SCADA and Security System Performance Levels [P<sub>E1</sub>], 467

16.17—Define the Banking and Finance Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 468

16.18—Assess Banking and Finance Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 468

16.19—Analyze Effectiveness of Banking and Finance Security Strategies and Operations [P<sub>E1</sub>], 469

16.20—Refine Previous Analysis of Banking and Finance Enterprise Undesirable Consequences that can Affect Functions, 469

16.21—Refine Previous Analysis of Banking and Finance Enterprise Likelihood of Malevolent Acts of Occurrence, 469

16.22—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Banking and Finance Enterprise Mitigation Solutions [P<sub>E2</sub>], 470

16.23—Develop Short- and Long-Term Banking and Finance Enterprise Mitigation Solutions, 470

16.24—Evaluate Effectiveness of Banking and Finance Enterprise Developed Mitigation Solutions and Residual Vulnerability [P<sub>E2</sub>], 470

16.25—Develop Cost Estimate for Short- and Long-Term Banking and Finance Enterprise Mitigation Solutions, 470

## **Chapter 16 Appendix**

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within the Banking and Finance Sector, 471
- B United States Government Banking and Finance Sector Initiatives, 493

**17 THE TELECOMMUNICATIONS SECTOR****499**

A Link to All Other Sectors Is Vital To Our National Security, 500  
An Attractive Target, 501

Telecommunications Vulnerabilities, 502

Tailoring the *S<sup>3</sup>E* Security Assessment Methodology for the Telecommunications Sector, 503

Telecommunications Challenges Facing the Security Assessment Team, 506

Applying the *S<sup>3</sup>E* Security Assessment Methodology to the Telecommunications Sector, 428

Task 1—Operational Environment, 506

Task 2—Critical Assessment, 508

Task 3—Threat Assessment, 509

Task 4—Evaluate Program Effectiveness, 513

Task 5—Program Analyses, 517

Preparing the Telecommunications Assessment Report, 519

Telecommunications Initiatives, 519

**Chapter 17 Exhibits**

17.1—*S<sup>3</sup>E* Security Assessment Methodology for the Telecommunications Sector, 504

17.2—Identify Telecommunications Enterprise Mission Goals and Objectives, 507

17.3—Identify Telecommunications Customer Base, 507

17.4—Identify Telecommunications Enterprise Commitments, 507

17.5—Characterize Configuration of Telecommunications Enterprise Facilities and Boundaries, 509

17.6—Critical Assessment of Telecommunications Enterprise Facilities, Assets, Operations, Processes, and Logistics, 510

17.7—Prioritize Critical Telecommunications Enterprise Assets, in Relative Importance to Business Operations, 510

17.8—Determine Types of Malevolent Acts that could Reasonably Cause Telecommunications Enterprise Undesirable Events, 511

17.9—Assess Other Disruptions Impact Telecommunications Operations, 512

- 17.10—Identify Category of Telecommunications Enterprise Perpetrators, 512
- 17.11—Assess Initial Impact of Telecommunications Enterprise Loss Consequence, 513
- 17.12—Assess Initial Likelihood of Telecommunications Enterprise Threat Attractiveness and Likelihood of Malevolent Acts Occurring, 513
- 17.13—Evaluate Existing Telecommunications Enterprise Security Operations and Protocols [P<sub>E1</sub>], 514
- 17.14—Evaluate Existing Enterprise Telecommunications Security Organization [P<sub>E1</sub>], 514
- 17.15—Evaluate Existing Telecommunications Enterprise Interface and Relationship with Partner Organizations [P<sub>E1</sub>], 515
- 17.16—Evaluate Existing Telecommunications SCADA and Security System Performance Levels [P<sub>E1</sub>], 516
- 17.17—Define the Telecommunications Enterprise Adversary Plan, Distractions, Sequence of Interruptions, and Path Analysis, 516
- 17.18—Assess Telecommunications Enterprise Effectiveness of Response and Recovery [P<sub>E1</sub>], 516
- 17.19—Analyze Effectiveness of Telecommunications Security Strategies and Operations [P<sub>E1</sub>], 517
- 17.20—Refine Previous Analysis of Telecommunications Enterprise Undesirable Consequences that can Affect Functions, 517
- 17.21—Refine Previous Analysis of Telecommunications Enterprise Likelihood of Malevolent Acts of Occurrence, 518
- 17.22—Analyze Selection of Specific Risk-Reduction Actions Against Current Risk, and Develop Prioritized Plan for Telecommunications Enterprise Mitigation Solutions [P<sub>E2</sub>], 518
- 17.23—Develop Short- and Long-Term Telecommunications Enterprise Mitigation Solutions, 518
- 17.24—Evaluate Effectiveness of Telecommunications Enterprise Developed Mitigation Solutions and Residual Vulnerability [P<sub>E2</sub>], 518
- 17.25—Develop Cost Estimate for Short- and Long-Term Telecommunications Enterprise Mitigation Solutions, 440

## **Chapter 17 Appendix**

- A A Historical Overview of Selected Terrorist Attacks, Criminal Incidents, and Industry Mishaps, Within the Telecommunications Sector, 520**
- B United States Government Telecommunications Sector Initiatives, 522**

<b>GENERAL GLOSSARY</b>	<b>525</b>
<b>INDEX</b>	<b>589</b>