
Contents

Preface.....xix

Authors’ Notes.....xxi

Synopsis.....xxiii

Acknowledgments.....xxvii

The Authors.....xxix

Chapter 1 Introduction to Critical Infrastructure Assurance..... 1

1.1 Introduction 1

1.2 Homeland Security Presidential Directives..... 2

1.3 What Is Critical Infrastructure? 3

1.4 What Is the Private Sector? 3

1.5 What Is the Public Sector? 3

1.6 What Is CIP? 4

1.7 What Is CIA? 4

1.8 Critical Infrastructure Functions 6

1.9 Origins of Critical Infrastructure 6

Notes..... 7

Chapter 2 Demand, Capacity, and Fragility and the Emergence
of Networks 11

2.1 Introduction 11

2.2 What Are We Trying to Protect? The Concept of Capacity 11

2.3 Demand: The Reason for Capacity 12

2.3.1 The Concept of Performance..... 12

2.3.2 Local Impact and the Influence on Capacity 12

2.3.3 Results of a Local Impact in the Immediate Sense..... 13

2.3.4 Relevance to CIP 13

2.3.5 Push, Pull, Lag, and Delay in the Network
Environment..... 14

2.4 At the Regional (Small System) Level 14

2.4.1 Influence at the Small System Level 14

2.4.2 Current Efforts and Research..... 15

2.4.3 The Interdependency Hydra 15

2.4.4 Network Fragmentation and Dissolution..... 16

2.5 Cyberterrorism 17

2.5.1 The Pendulum of Convergence 17

2.5.2 Convergence and the Understanding of Threat..... 18

2.5.3 Setting the Stage for Fragility 19

2.5.4 Fragility and Destabilization of Systems 21

2.5.5	Fragmentation and Dissolution of Networks.....	22
2.6	Dissolution and Convergence: An Emerging Risk.....	23
2.6.1	Convergence, Network Expansion, Open Architecture, and Common Criteria.....	23
2.7	Marking the Journey.....	24
2.7.1	Overview.....	24
2.7.2	Legislation: 107th Congress (Particularly 2001–2002).....	24
2.7.3	Legislation: 108th Congress–109th Congress	25
2.7.4	The State Today: A Recap	25
2.7.5	Research and Understanding	26
2.8	Authors' Notes.....	26
	Notes.....	26

Chapter 3	National Response Framework.....	29
3.1	Introduction.....	29
3.2	What Is the NRF?.....	29
3.3	Reasons for Replacing the NRP	30
3.4	Differences between the NRP and the NRF.....	30
3.5	Target Audience of the NRF.....	32
3.6	Applying the NRF to National Response Efforts	32
3.7	How Does the NRF Tie In with Emergency Management?	33
3.8	NRF Key Principles.....	33
3.9	How Is the NRF Organized?	34
3.10	What Is the Purpose of the NRF?.....	35
3.11	Tie between NRF and NIMS	35
3.12	Multiagency Communication and Structure Coordination	35
3.13	Coordination Responsibilities.....	36
3.14	Updates to the NRF	36
3.15	Incident Command Structure of the NRF	37
3.16	Levels of Authority	38
3.17	Key Concepts in the Implementation of the NRF	38
3.18	Roles and Responsibilities	39
3.18.1	Role of the Governor	39
3.18.2	Role of the Local CEO	40
3.18.3	Role of the Tribal CEO.....	40
3.19	Roles of the Federal Government	40
3.20	NRF Emergency Support Functions	43
3.21	Scope of ESFs.....	44
3.21.1	ESF 1: Transportation.....	45
3.21.2	ESF 2: Communications.....	45
3.21.3	ESF 3: Public Works	45
3.21.4	ESF 4: Fire Services	45
3.21.5	ESF 5: Emergency Management	45

- 3.21.6 ESF 6: Human Services.....46
- 3.21.7 ESF 7: Resource Management.....46
- 3.21.8 ESF 8: Public Health and Medical Services.....46
- 3.21.9 ESF 9: Urban Search and Rescue Services46
- 3.21.10 ESF 10: HAZMAT Response46
- 3.21.11 ESF 11: Agriculture and Natural Resources.....46
- 3.21.12 ESF 12: Energy.....46
- 3.21.13 ESF 13: Public Safety and Security.....46
- 3.21.14 ESF 14: Long-Term Community Recovery and Mitigation.....47
- 3.21.15 ESF 15: External Affairs47
- 3.22 Authors' Thoughts.....47
- Notes.....48

Chapter 4 National Incident Management System..... 51

- 4.1 Introduction..... 51
- 4.2 What Is NIMS?..... 51
- 4.3 Compliance 53
- 4.4 Flexibility..... 53
- 4.5 Standardization..... 53
- 4.6 NIMS Represents Best Practices 53
- 4.7 Components of NIMS 54
- 4.8 Command and Management..... 54
- 4.9 Preparedness 54
- 4.10 Benefits from Using NIMS 55
- 4.11 Resource Recovery 56
- 4.12 Communications and Information Management..... 56
- 4.13 Supporting Technologies 56
- 4.14 Ongoing Management and Maintenance 57
- 4.15 Command Structuring under NIMS 57
- 4.16 Incident Command System..... 57
- 4.17 ICS Features..... 58
- 4.18 Common Terminology..... 59
- 4.19 Organizational Resources..... 59
- 4.20 Manageable Span of Control 59
- 4.21 Accountability 60
- 4.22 Integrate Communications Capabilities 60
- 4.23 Incident Action Plan 60
- 4.24 Management Command, Coordination, and Control Structures 61
- 4.25 Unified Command..... 61
- 4.26 Area Command 61
- 4.27 Multiagency Coordination Systems..... 62
- 4.28 Emergency Operations Centers 63
- 4.29 Incident Responsibilities..... 64

4.30	Postincident Responsibilities	64
4.31	Public Information Systems.....	64
4.32	Joint Information Systems	65
4.33	Joint Information Centers	65
4.34	JIC Levels	65
4.35	JIC Organizational Structure.....	66
4.36	Preparedness and Readiness.....	66
4.37	Preparedness Organizations	67
4.38	Preparedness Planning and Coordination	67
4.39	Types of Preparedness Plans	67
4.40	Emergency Operations Plan	68
4.41	Training and Exercise Drills.....	69
4.42	Personnel Qualification and Certification.....	69
4.43	Equipment and Hardware Certification	69
4.44	Mutual Aid Agreements	70
4.45	Standby Contracts	70
4.46	Publication Management	70
4.47	Resource Management	71
4.48	Effectively Managing Resources	72
4.49	Communications and Information Management Principles	73
4.50	Authors' Notes	73
Notes		74

Chapter 5	Incident Command System	83
5.1	Introduction.....	83
5.2	What Are NIMS and ICS?.....	83
5.3	What Is an Incident?	84
5.4	What Is an ICS?	84
5.5	What Is NIMS ICS?.....	85
5.6	History of ICS.....	85
5.7	FIRESCOPE	86
5.8	National Interagency Incident Management System	87
5.9	Weaknesses Addressed by Using an ICS.....	87
5.10	Benefits of Using an ICS.....	88
5.11	ICS Framework	88
5.12	Applications for the Use of ICS	88
5.13	ICS Management Characteristics	88
5.14	Understanding the ICS Organization.....	89
5.15	ICS Management Functions.....	89
5.16	ICS Sections.....	90
5.17	What Is Span of Control?.....	90
5.18	ICS Position Titles	90
5.19	ICS Organizational Components	91
5.20	Unified Command	91

5.21	The Incident Commander	92
5.22	Command Staff	92
5.22.1	Command Staff: PIO.....	93
5.22.2	Command Staff: SO.....	93
5.22.3	Command Staff: LNO.....	93
5.23	General Staff	94
5.24	Operations Section	94
5.25	Planning Section.....	95
5.26	Incident Action Plan	96
5.27	Logistics Section	96
5.28	Finance/Administration Section.....	97
5.29	ICS Area Command	98
5.30	Communications within the ICS	98
5.31	Incident Facilities.....	99
5.31.1	Incident Facilities: ICP	99
5.31.2	Incident Facilities: Staging Area	99
5.31.3	Incident Facilities: Base.....	99
5.31.4	Incident Facilities: Camp.....	100
5.31.5	Incident Facilities: Helibase	100
5.31.6	Incident Facilities: Helispot.....	100
5.32	Differences between NIMS ICS and FIREScope/ NIIMS ICS	100
5.33	NIMS ICS Training.....	100
5.34	How ICS Integrates with Critical Infrastructure.....	101
5.35	Current Use of ICS with Critical Infrastructure.....	102
5.36	Hospital Incident Command System	102
5.37	Authors' Thoughts.....	103
	Notes	103

Chapter 6 Emergency Preparedness and Readiness 109

6.1	Introduction	109
6.2	Office for Domestic Preparedness.....	109
6.3	First Responder.....	110
6.4	First Responder Classifications	110
6.5	Guideline Classifications.....	110
6.6	North American Emergency Response Guidebook	111
6.7	Awareness Level Guidelines.....	111
6.7.1	Recognize HAZMAT Incidents.....	112
6.7.2	Know the Protocols	112
6.7.3	Know Self-Protection Measures	113
6.7.4	Know Procedures for Protecting Incident Scenes	113
6.7.5	Know Scene Security and Control Procedures	114
6.7.6	Know How to Use Equipment Properly	114
6.8	Performance Level Guidelines	115
6.9	Operational Levels Defined.....	115

6.10	Level A: Operations Level.....	115
6.10.1	Have Successfully Completed Awareness Level Training	115
6.10.2	Know ICS Awareness Procedures.....	116
6.10.3	Know Self-Protection and Rescue Measures	117
6.11	Level B: Technician Level	118
6.11.1	Know WMD Procedures	118
6.11.2	Have Successfully Completed Awareness and Performance Level Training.....	119
6.11.3	Know Self-Protection, Rescue, and Evacuation Procedures	120
6.11.4	Know and Follow Procedures for Performing Specialized Tasks	121
6.11.5	Know ICS Performance Procedures	122
6.11.6	Planning and Management Level Guidelines.....	123
6.11.7	Successfully Completed Awareness, Performance, and Management Training	123
6.11.8	Know ICS Management Procedures	124
6.12	Know Protocols to Secure, Mitigate, and Remove HAZMAT	125
6.13	Additional Protective Measures.....	126
6.14	Understand the Development of the IAP.....	126
6.15	Know and Follow Procedures for Protecting a Potential Crime Scene	127
6.16	Know Department Protocols for Medical Response Personnel.....	128
6.17	National Fire Prevention Association 472	128
6.18	OSHA Hazardous Waste Operations and Emergency Response	128
6.19	Skilled Support Personnel	129
6.20	Specialist Employee	129
6.21	DOT HAZMAT Classifications	130
6.21.1	DOT HAZMAT Class 1: Explosives.....	130
6.21.2	DOT HAZMAT Class 2: Gases	130
6.21.3	DOT HAZMAT Class 3: Flammable Liquids	130
6.21.4	DOT HAZMAT Class 4: Flammable Solids.....	130
6.21.5	DOT HAZMAT Class 5: Oxidizers	130
6.21.6	DOT HAZMAT Class 6: Toxic Materials	131
6.21.7	DOT HAZMAT Class 7: Radioactive Materials.....	131
6.21.8	DOT HAZMAT Class 8: Corrosive Materials.....	131
6.22	Importance of Implementing an Emergency Response Plan.....	131
6.23	Authors' Notes.....	132
	Notes	132

Chapter 7 Security Vulnerability Assessment 135

- 7.1 Introduction 135
- 7.2 What Is a Risk Assessment? 135
- 7.3 Methods of Assessing Risk 137
- 7.4 Threat Risk Equations 137
- 7.5 Comparison of Quantitative versus Qualitative Risk Assessments 138
- 7.6 Challenges Associated with Assessing Risk 139
- 7.7 Other Factors to Consider When Assessing Risk 140
- 7.8 What Is an SVA? 140
- 7.9 Reasons for Having an SVA 141
- 7.10 What Is a Threat? 141
- 7.11 What Is Vulnerability? 142
- 7.12 Countermeasures 142
- 7.13 Vulnerability Assessment Framework 142
- 7.14 Reasons for Using the VAF 143
- 7.15 Federal Information Systems Control Auditing Manual 144
- 7.16 General Methodologies of FISCAM Auditing 145
- 7.17 What Are General Controls? 146
- 7.18 What Are Application Controls? 146
- 7.19 Caveats with Using an SVA 146
- 7.20 How the SVA Is Used 147
- 7.21 Audience of an SVA 147
- 7.22 Initial SVA Plan 147
- 7.23 Necessary Steps of an SVA 148
- 7.24 Critical Success Factors 148
- 7.25 VAF Methodology 149
- 7.26 Initial Steps of the VAF 150
- 7.27 VAF Step 1: Establish the Organization MEI 151
 - 7.27.1 Strategic-Level MEI 152
 - 7.27.2 Tactical-Level MEI 152
 - 7.27.3 Resource Elements Comprising an MEI 153
 - 7.27.4 Defining Team Composition 153
 - 7.27.5 Identifying Threat Awareness 154
 - 7.27.6 Potential Threat Sources 154
 - 7.27.7 Potential Threat Motivation 155
- 7.28 VAF Step 2: Gather Data to Identify MEI Vulnerabilities 155
 - 7.28.1 Areas of Control 156
 - 7.28.2 Areas of Potential Compromise 156
 - 7.28.3 Areas of Concern Using the Framework 157
 - 7.28.4 Control Objectives Used in the Framework 157
 - 7.28.5 Data Classification 158
- 7.29 VAF Step 3: Analyze, Classify, and Prioritize Vulnerabilities 159

7.30	Authors' Notes	159
	Notes	160
Chapter 8	Standards and Guidelines.....	163
8.1	Introduction.....	163
8.2	About the National Fire Prevention Association	163
8.2.1	NFPA 730 and NFPA 731	163
8.2.2	NFPA 472.....	164
8.2.3	NFPA 1600	165
8.3	North American Electric Reliability Council.....	165
8.3.1	NERC Standards	165
8.3.2	NERC 1200.....	166
8.3.3	NERC 1300	166
8.3.4	NERC Critical Infrastructure Protection.....	166
8.3.5	Subsections of NERC CIP	167
8.4	American Gas Association	167
8.4.1	AGA 12.....	167
8.4.2	Subsections of AGA 12.....	168
8.5	Instrumentation, Systems, and Automation Society.....	168
8.5.1	ISA-SP99.....	169
8.6	American Petroleum Institute.....	169
8.6.1	API 1164.....	169
8.7	Chemical Industry Data Exchange	170
8.7.1	Open Application Group, Inc.	171
8.7.2	Chemical Information Technology Center.....	171
8.8	ISO 15408.....	171
8.8.1	ISO 17799.....	172
8.8.2	ISO 27001	173
8.9	NIST PCSRF	173
8.9.1	NIST SP800-53	174
8.9.2	NIST SP800-82.....	174
8.10	Health Insurance Portability and Accountability Act	174
8.10.1	Subsections of HIPAA.....	175
8.11	Patient Safety and Quality Improvement Act.....	175
8.11.1	Subsections of PSQIA	176
8.12	Gramm–Leach–Bliley Act	177
8.12.1	Subsections of GLBA	177
8.13	Sarbanes–Oxley Act.....	178
8.14	The ANSI-Homeland Security Standards Database.....	178
8.15	Federal Information Processing Standards	179
8.15.1	FIPS 113	180
8.15.2	FIPS 140-1	180
8.15.3	FIPS 140-2.....	180
8.15.4	FIPS 180-1	181
8.15.5	FIPS 180-2.....	181

8.15.6 FIPS 186-1 181

8.15.7 FIPS 186-2 181

8.15.8 FIPS 190 182

8.15.9 FIPS 191..... 182

8.15.10 FIPS 197 182

8.15.11 FIPS 199 182

8.15.12 FIPS 201 182

8.16 National Standards Systems Network..... 183

8.17 IEC 62351 183

8.18 IEEE 1402-2000 183

8.19 Authors’ Notes 184

Notes 184

Chapter 9 Information Sharing and Analysis Centers 191

9.1 Introduction..... 191

9.2 What Is a Critical Infrastructure Asset?..... 191

9.3 What Is an ISAC? 192

9.4 Advantages of Belonging to an ISAC 192

9.5 Access to ISAC Information..... 192

9.6 Expanded ISAC Services 193

9.7 Surface Transportation ISAC..... 193

9.8 Supply Chain ISAC..... 194

9.9 Public Transit ISAC 194

9.10 American Public Transportation Association..... 195

9.11 Association of American Railroads..... 195

9.12 Transportation Technology Center, Inc. 195

9.13 Railinc..... 195

9.14 Water ISAC 195

9.15 Association of State Drinking Water Administrators 197

9.16 Water Environment Research Foundation 197

9.17 Association of Metropolitan Water Agencies 198

9.18 Association of Metropolitan Sewage Agencies..... 198

9.19 National Association of Water Companies 198

9.20 American Water Works Association 199

9.21 AWWA Research Foundation..... 199

9.22 Financial Services ISAC..... 199

9.23 Science Applications International Corporation 200

9.24 Electricity Sector ISAC 200

9.25 Emergency Management and Response ISAC 202

9.26 Information Technology ISAC 203

9.27 National Coordinating Center for Telecommunications..... 204

9.28 Communications Resource Information Sharing..... 204

9.29 Government Emergency Telecommunications Service..... 205

9.30 Telecommunications Service Priority 207

9.31 Shared Resources High Frequency Radio Program 208

9.32	Network Reliability and Interoperability Council.....	208
9.33	National Security Telecommunications Advisory Committee	209
9.34	Wireless Priority Services	211
9.35	Alerting and Coordination Network.....	213
9.36	Energy ISAC.....	214
9.37	Energy Sector Security Consortium.....	214
9.38	Chemical Sector ISAC.....	215
9.39	Chemical Transportation Emergency Center	216
9.40	Healthcare Services ISAC	216
9.41	Highway ISAC	216
9.42	Cargo Theft Information Processing Systems.....	217
9.43	American Trucking Associations	217
9.44	HighwayWatch®	217
9.45	Food and Agriculture ISAC.....	218
9.46	FoodSHIELD.....	219
9.47	Food Marketing Institute	220
9.48	Multistate ISAC	220
9.49	ISAC Council.....	221
9.50	World Wide ISAC	221
9.51	Real Estate ISAC	221
9.52	The Real Estate Roundtable	222
9.53	Research and Educational Networking ISAC.....	222
9.54	Biotechnology and Pharmaceutical ISAC	222
9.55	Maritime ISAC	222
9.56	Maritime Security Council.....	223
9.57	Marine Transportation System National Advisory Council	223
9.58	Authors' Notes	224
	Notes	225

Chapter 10 Supervisory Control and Data Acquisition 235

10.1	Introduction.....	235
10.2	What Are Control Systems?.....	235
10.3	Types of Control Systems	236
10.4	Components of Control Systems.....	236
10.5	Vulnerability Concerns about Control Systems.....	237
10.6	Adoption of Standardized Technologies with Known Vulnerabilities.....	237
10.7	Connectivity of Control Systems to Unsecured Networks	238
10.8	Implementation Constraints of Existing Security Technologies	238
10.9	Insecure Connectivity to Control Systems.....	239
10.10	Publicly Available Information about Control Systems.....	239

10.11 Control Systems May Be Vulnerable to Attack240

10.12 Consequences Resulting from Control System
Compromises 241

10.13 Wardialing 241

10.13.1 Goals of Wardialing 242

10.13.2 Threats Resulting from Wardialing 242

10.14 Wardriving 242

10.15 Warwalking 243

10.16 Threats Resulting from Control System Attacks 243

10.17 Issues in Securing Control Systems 243

10.18 Methods of Securing Control Systems 245

10.19 Technology Research Initiatives of Control Systems 246

10.20 Security Awareness and Information Sharing Initiatives..... 247

10.21 Process and Security Control Initiatives 248

10.22 Securing Control Systems 250

10.23 Implement Auditing Controls 250

10.24 Develop Policy Management and Control Mechanisms..... 250

10.25 Control Systems Architecture Development 251

10.26 Segment Networks between Control Systems and
Corporate Enterprise 251

10.27 Develop Methodologies for Exception Tracking 251

10.28 Define an Incident Response Plan 252

10.29 Similarities between Sectors 252

10.30 U.S. Computer Emergency Readiness
Team CSSP 252

10.31 Control System Cyber Security Self-Assessment Tool..... 254

10.32 SCADA Community Challenges 255

10.33 The Future of SCADA 256

10.34 SCADA Resources 256

10.34.1 Blogs 257

10.34.2 SCADASEC Mailing List 257

10.34.3 Online SCADA and SCADA Security
Resources 257

10.35 Authors' Comments 257

Notes 258

Chapter 11 Critical Infrastructure Information 261

11.1 Introduction 261

11.2 What Is Critical Infrastructure Information? 261

11.3 How Does the Government Interpret CII? 263

11.4 Exemption 3 of the FOIA 263

11.5 Exemption 4 of the FOIA 264

11.6 Section 214 of the Homeland Security Act..... 265

11.7 Enforcement of Section 214 of the Homeland
Security Act 266

11.8	What Does “Sensitive, but Unclassified” Mean?.....	267
11.9	Information Handling Procedures.....	268
11.10	Freedom of Information Act	268
11.11	Need-to-Know	270
11.12	“For Official Use Only”	270
11.13	Enforcement of FOUO Information.....	271
11.14	Reviewing Web Site Content.....	271
11.15	Export-Controlled Information	273
11.16	Enforcement of Export-Controlled Information	274
11.17	Source Selection Data	274
11.18	Enforcement of Source Selection Data	275
11.19	Privacy Information	275
11.20	Enforcement of Privacy Information	276
11.21	Unclassified Controlled Nuclear Information	276
11.22	Enforcement of UCNI.....	276
11.23	Critical Energy Infrastructure Information	277
11.24	Enforcement of CEIL.....	277
11.25	Controlled Unclassified Information	277
11.26	Lessons Learned Program	278
11.27	InfraGard	279
11.28	Authors’ Thoughts	279
	Notes.....	280
 Appendix A		289
Appendix B		295
Appendix C		301
Glossary		303
Index		309