1. Record Nr. UNINA990004300570403321

Autore	Leopardi, Giacomo <1798-1837>
Titolo	Canti / Giacomo Leopardi ; edizione critica di Emilio Peruzzi con la riproduzione degli autografi
Pubbl/distr/stampa	Milano : Rizzoli, 1981
Descrizione fisica	XIII, 629 p., 255 tav. ; 23 cm
Disciplina	851.7
Locazione	FLFBC
Collocazione	851.7 LEOP 2(2)
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9910970759203321

Titolo	National infrastructure : protecting, funding, and rebuilding / / Frederick H. Lupul, editor
Pubbl/distr/stampa	New York, : Nova Science Publishers, c2009
ISBN	1-61470-344-2
Edizione	[1st ed.]
Descrizione fisica	1 online resource (256 p.)
Collana	Terrorism, hot spots and conflict-related issues
Altri autori (Persone)	LupulFrederick H
Disciplina	363.325/170973
Soggetti	Terrorism - United States - Prevention Infrastructure (Economics) - Security measures - United States - Planning National security - United States - Planning
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references (p. 228-230) and index.
Nota di contenuto	Intro -- NATIONAL INFRASTRUCTURE:PROTECTING, FUNDING ANDREBUILDING -- NATIONAL INFRASTRUCTURE:PROTECTING,

FUNDING ANDREBUILDING -- CONTENTS -- LIST OF FIGURES AND TABLES -- PREFACE -- LETTER OF AGREEMENT -- SIGNATORIES -- EXECUTIVE SUMMARY -- 1. INTRODUCTION -- 2. AUTHORITIES, ROLES, AND RESPONSIBILITIES -- 3. THE CI/KR PROTECTION PROGRAM STRATEGY: MANAGING RISK -- 4. ORGANIZING AND PARTNERING FOR CI/KR PROTECTION -- 5. CI/KR PROTECTION: AN INTEGRAL PART OF THE HOMELANDSECURITY MISSION -- 6. ENSURING AN EFFECTIVE, EFFICIENT PROGRAMOVER THE LONG TERM -- 7. PROVIDING RESOURCES FOR THE CI/KR PROTECTION PROGRAM -- Chapter 11. INTRODUCTION -- 1.1. PURPOSE -- 1.2. SCOPE -- 1.3. APPLICABILITY -- 1.3.1. Goal -- 1.3.2. The Value Proposition -- 1.4. THREATS TO THE NATION'S CI/KR -- 1.4.1. The Vulnerability of the U.S. Infrastructure to 21st Century Threats -- 1.4.2. The Nature of Possible Terrorist Attacks -- 1.5. ALL-HAZARDS AND CI/KR PROTECTION -- 1.6. PLANNING ASSUMPTIONS -- 1.6.1. Sector-Specific Nature of CI/KR Protection -- 1.6.2. Cross-Sector Dependencies and Interdependencies -- 1.6.3. Adaptive Nature of the Terrorist Threat -- 1.6.4. All-Hazards Nature of CI/KR Protection -- 1.7. SPECIAL CONSIDERATIONS -- 1.7.1 Protection of Sensitive Information -- 1.7.2. The Cyber Dimension -- 1.7.3. The Human Element -- 1.7.4. International CI/KR Protection -- 1.8. ACHIEVING THE GOAL OF THE NIPP -- 1.8.1. Understanding and Sharing Information -- 1.8.2. Building Security Partnerships -- 1.8.3. Implementing a Long-Term CI/KR Risk Management Program -- 1.8.4. Maximizing Efficient Use of Resources for CI/KR Protection -- Chapter 22.AUTHORITIES, ROLES, AND RESPONSIBILITIES -- 2.1. AUTHORITIES -- 2.2. ROLES AND RESPONSIBILITIES -- 2.2.1. Department of Homeland Security -- 2.2.2. Sector-Specific Agencies -- 2.2.3. Other Federal Departments, Agencies, and Offices.
2.2.4. State, Local, and Tribal Governments -- 2.2.4.1. State and Territorial Governments -- 2.2.4.2. Local Governments -- 2.2.4.3. Tribal Governments -- 2.2.4.4. Regional Partners -- 2.2.4.5 Boards, Commissions, Authorities, Councils, and Other Entities -- 2.2.5. Private Sector Owners and Operators -- 2.2.6. Advisory Councils -- 2.2.7. Academia and Research Centers -- Chapter 33. THE PROTECTION PROGRAM STRATEGY:MANAGING RISK -- 3.1. SET SECURITY GOALS -- 3.2. IDENTIFY ASSETS, SYSTEMS, NETWORKS, AND FUNCTIONS -- 3.2.1. National Infrastructure Inventory -- 3.2.2. Protecting and Accessing Inventory Information -- 3.2.3. SSA Roles in Inventory Development and Maintenance -- 3.2.4. State Roles in Inventory Development and Maintenance -- 3.2.5. Identifying Cyber Infrastructure -- 3.2.6. Identifying Positioning, Navigation, and Timing Services -- 3.3. ASSESS RISKS -- 3.3.1. NIPP Baseline Criteria for Assessment Methodologies -- 3.3.1.1. Ensuring That Previous Assessments Can Be Used -- 3.3.1.2. Baseline Criteria -- 3.3.2. Consequence Analysis -- 3.3.2.1. Consequence Assessment Methodologies That Enable National Risk Analysis -- 3.3.2.2. Consequence Screening -- 3.3.3. Vulnerability Assessment -- 3.3.3.1. Vulnerability Assessment Methodologies That Enable National Risk Analysis -- 3.3.3.2. SSA and DHS Analysis Responsibilities -- 3.3.4. Threat Analysis -- 3.3.4.1 Key Aspects of the Terrorist Threat to CI/KR -- 3.3.4.2. Homeland Infrastructure Threat and Risk Analysis Center -- 3.4. PRIORITIZE -- 3.4.1. The Prioritization Process -- 3.4.2. Tailoring Prioritization Approaches to Sector Needs -- 3.4.3. The Uses of Prioritization -- 3.5. IMPLEMENT PROTECTIVE PROGRAMS -- 3.5.1. Protective Actions -- 3.5.2. Characteristics of Effective Protective Programs -- 3.5.3. Protective Programs, Initiatives, and Reports -- 3.6.MEASURE EFFECTIVENESS.
3.6.1. NIPP Metrics and Measures -- 3.6.1.1. Measuring Performance -- 3.6.1.2. Core Metrics and Sector-Specific Metrics -- 3.6.2. Gathering

EDUCATION, TRAINING,AND EXERCISE PROGRAMS -- 6.2.1. Types of Expertise for CI/KR Protection -- 6.2.2. Individual Education and Training -- 6.2.2.1. Technical CI/KR Protection Training -- 6.2.2.2. Academic and Research Programs -- 6.2.2.3. Continuing Education and Professional Competency -- 6.2.3. Organizational Training and Exercises -- 6.2.4. Security Partner Role and Approach -- 6.3. Conducting Research and Development and Using Technology -- 6.3.1. R&amp -- D Programs -- 6.3.2. The SAFETY Act -- 6.3.3. National Critical Infrastructure Protection R&amp -- D Plan -- 6.3.3.1 CI/KR Protection R&amp -- D Strategic Goals -- 6.3.3.2. CI/KR Protection R&amp -- D Areas -- 6.3.3.3. CI/KR Protection R&amp -- D Roadmap -- 6.3.3.4. Coordination of NCIP R&amp -- D Plan With SSP R&amp -- D Planning -- 6.3.4. Cyber Security R&amp -- D Planning -- 6.3.5. Other R&amp -- D That Supports CI/KR Protection -- 6.3.6. Technology Pilot Programs -- 6.4. BUILDING, PROTECTING, AND MAINTAINING DATABASES,SIMULATIONS, AND OTHER TOOLS -- 6.4.1. National CI/KR Protection Data Systems -- 6.4.2. Simulation and Modeling -- 6.4.3. Coordination with Security Partners on Databases and Modeling -- 6.5. CONTINUOUSLY IMPROVING THE NIPP AND THE SSPS -- 6.5.1. Management and Coordination -- 6.5.2. Maintenance and Updating -- Chapter 77. PROVIDING RESOURCES FOR THE CI/KRPROTECTION PROGRAM -- 7.1. THE RISK-BASED RESOURCE ALLOCATION PROCESS -- 7.1.1. Sector-Specific Agency Reporting to DHS -- 7.1.2. State Government Reporting to DHS -- 7.1.3. Aggregating Submissions to DHS -- 7.2. FEDERAL RESOURCE ALLOCATION PROCESS FOR DHS, THESSAS, AND OTHER FEDERAL AGENCIES -- 7.2.1. Department of Homeland Security -- 7.2.2. Sector-Specific Agencies.
7.2.3. Summary of Roles and Responsibilities.

Sommario/riassunto

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CI/KR as weapons of mass destruction could have even more devastating physical and psychological consequences.