George Mason University

The Center for Infrastructure Protection and Homeland Security (CIP/HS)

Higher Education Initiative

Presented to Association for Contingency Planning Luncheon

Mark Troutman, PhD
Associate Director, Center for Infrastructure Protection and Homeland Security
19 June 2014
mtroutma@gmu.edu

Think. Learn. Succeed.

GEORGE MASON UNIVERSITY

CIP/HS Overview

- Welcome!

- Established at the Mason School of Law in May 2002.

- Integrate the disciplines of law, policy, and technology in order to conduct infrastructure resilience analysis and research to improve U.S. and international security.

  - Education: Curriculum oriented toward practicing Critical Infrastructure professionals; develop leadership and analytic competencies

  - Sponsored research to generate practical solutions to solve critical infrastructure security and resilience

  - Conferences and Events: Convene, Spotlight and Generate Leadership Toward Solutions

- Publish the monthly newsletter, *The CIP Report*, which highlights key infrastructure protection issues.

Education: What's Tough about Infrastructure Protection?

- **Infrastructure Security and Resilience does not reside in a single department program; a unique area of security studies**

- **Infrastructure Security and Resilience is:**
  - **Interdisciplinary:** Many different specialties
  - **Interdepartmental/Interagency:** Many different government departments
  - **International:** Crosses national boundaries
  - **Intergovernmental:** Different levels of government
  - **Industry/Government:** Private and Public Sector

- **Identified Core Competencies (from 2009 NIPP)**
  - Risk Analysis
  - Protective Measures/Mitigation Strategy Development
  - Technical and Tactical Expertise (Sector-Specific)
  - Partnership Building/Networking
  - Metrics and Program Evaluation
  - Information Collection and Reporting
  - Program Management

- **Survey of 785 institutions: Found no developed, standard approach**

- **Two year effort: Certificate Program, Master's Degree, Stand Alone Courses, Case Studies and Reference Materials**

- **Five Year follow on effort to keep updated, develop additional materials and conduct outreach to facilitate adoption of curricula**

Core Competencies

2009 NIPP

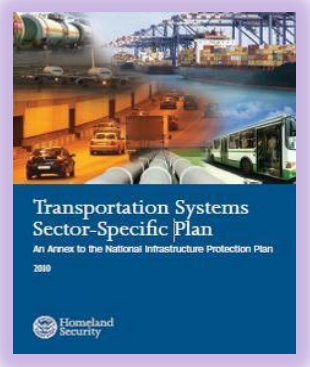
- Risk Analysis
- Protective Measures/Mitigation Strategies Development
- Technical and Tactical Expertise (Sector-Specific)
- Partnership Building/Networking
- Metrics and Program Evaluation
- Information Collection and Reporting (Information Sharing)
- Program Management

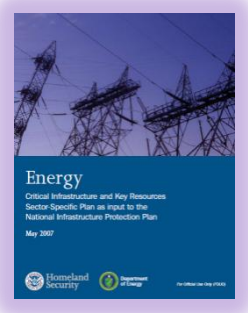
Area	Includes Knowledge and Skills To…
Risk Analysis	• Perform accurate, documented, objective, defensible, transparent, and complete analyses. • Support executive and managerial decision-making related to CIKR programs.
Protection Measures/Mitigation Strategies	• Establish CIKR program goals and objectives based on risk-analysis and risk-reduction return on investment. • Plan, develop, and implement CIKR-related projects, measures, and activities. Take advantage of existing emerging and anticipated methods and technologies in order to develop effective strategies, projects, and activities. • Implement continuous feedback mechanisms.
Partnership Building/Networking	• Understand the roles and responsibilities of all partners. • Establish mechanisms for interacting with partners and exchanging information and resources (including best practices).
Information Collection &Reporting (Information Sharing)	• Use systems, tools, and protocols to collect, analyze, organize, report, and evaluation information. • Communicate and share information with sector partners at each tier of governance, including sector-specific, across sectors, and within the private sector.
Program Management	• Establish sector-specific or jurisdictional CIKR goals and plans. • Identify and prioritize CIKR projects, strategies, and activities for a sector or jurisdiction. • Manage a CIKR program on schedule, within budget, and in compliance with performance standards. • Design and implement continuous feedback mechanisms at the program level. • Develop and implement CIKR training plans.
Metrics & Program Evaluation	• Define and establish CIKR metrics based on goals and objectives. • Establish data collection and measurement plans, systems, and tools. • Collect and analyze data. • Report findings and conclusions.
Technical & Tactical Expertise (Sector-Specific)	• Note: This area includes the specialized (sector-specific) expertise required to plan, implement, and evaluate technical and tactical activities, measures, and programs.

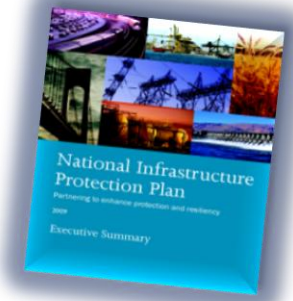
U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, (2009), 84.

Project Description and Approach

- **Description**: Support the U.S. Department of Homeland Security to create a comprehensive, unified education and training system that produces and sustains the leaders and workforce required to ensure the protection of the critical infrastructure of this Nation.







- **Approach**: Develop materials, including syllabi, case studies, and reading resources, that will be shared with multiple degree programs at colleges and universities and other interested 3rd parties.

Assessment/Recommendations

❖ Searched **785 U.S.** institutions for existing courses, concentrations/minors, degree programs, and training programs in critical infrastructure protection (CIP); instruction on seven CIP competency areas; use of best practices.

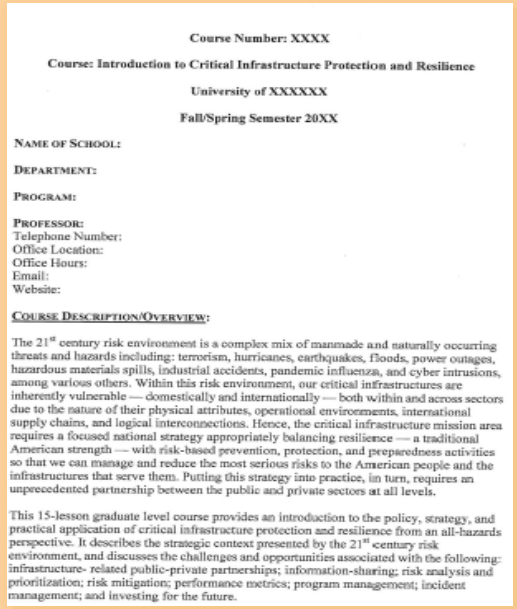
❖ **Sources:**

- ❖ The Center for Homeland Defense and Security
- ❖ Emergency Management Institute
- ❖ A random sampling of other accredited institutions (525 institutions)

…Four Recommendations

1. Determine career paths in critical infrastructure protection.
2. Provide guidance for CIP course content.
3. Continuously validate CIP core competencies.
4. Implement best practices in higher education.

Course Development



Course Number: XXXX

Course: Introduction to Critical Infrastructure Protection and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

NAME OF SCHOOL:

DEPARTMENT:

PROGRAM:

PROFESSOR:
Telephone Number:
Office Location:
Office Hours:
Email:
Website:

COURSE DESCRIPTION/OVERVIEW:

The 21st century risk environment is a complex mix of manmade and naturally occurring threats and hazards including: terrorism, hurricanes, earthquakes, floods, power outages, hazardous materials spills, industrial accidents, pandemic influenza, and cyber intrusions, among various others. Within this risk environment, our critical infrastructures are inherently vulnerable — domestically and internationally — both within and across sectors due to the nature of their physical attributes, operational environments, international supply chains, and logical interconnections. Hence, the critical infrastructure mission area requires a focused national strategy appropriately balancing resilience — a traditional American strength — with risk-based prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks to the American people and the infrastructures that serve them. Putting this strategy into practice, in turn, requires an unprecedented partnership between the public and private sectors at all levels.

This 15-lesson graduate level course provides an introduction to the policy, strategy, and practical application of critical infrastructure protection and resilience from an all-hazards perspective. It describes the strategic context presented by the 21st century risk environment, and discusses the challenges and opportunities associated with the following: infrastructure- related public-private partnerships; information-sharing; risk analysis and prioritization; risk mitigation; performance metrics; program management; incident management; and investing for the future.

- Created seven graduate critical infrastructure protection courses for multiple degree programs at colleges and universities.
- Review process: draft, revised, and final versions; courses reviewed at least twice.
- Developed five critical infrastructure security and resilience certificate courses (adapted from base year curricula)
- Modified a Public Administration master's degree program with the George Mason University Department of Public and International Affairs to provide concentration in critical infrastructure protection

Resource Development

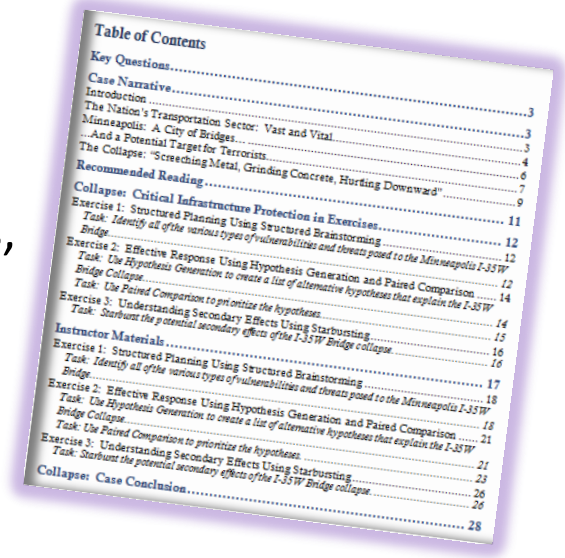


Table of Contents

Key Questions 3
Case Narrative 3
Introduction 3
The Nation's Transportation Sector: Vast and Vital 3
Minneapolis: A City of Bridges 4
...And a Potential Target for Terrorists 6
The Collapse: "Screeching Metal, Grinding Concrete, Hurting Downward" 7
Recommended Reading 9
Collapse: Critical Infrastructure Protection in Exercises 11
Exercise 1: Structured Planning Using Structured Brainstorming 12
Task: Identify all of the various types of vulnerabilities and threats posed to the Minneapolis I-35W Bridge 12
Exercise 2: Effective Response Using Hypothesis Generation and Paired Comparison 14
Task: Use Hypothesis Generation to create a list of alternative hypotheses that explain the I-35W Bridge Collapse 14
Task: Use Paired Comparison to prioritize the hypotheses 15
Exercise 3: Understanding Secondary Effects Using Starbursting 16
Task: Starburst the potential secondary effects of the I-35W Bridge collapse 16
Instructor Materials 17
Exercise 1: Structured Planning Using Structured Brainstorming 18
Task: Identify all of the various types of vulnerabilities and threats posed to the Minneapolis I-35W Bridge 18
Exercise 2: Effective Response Using Hypothesis Generation and Paired Comparison 21
Task: Use Hypothesis Generation to create a list of alternative hypotheses that explain the I-35W Bridge Collapse 21
Task: Use Paired Comparison to prioritize the hypotheses 23
Exercise 3: Understanding Secondary Effects Using Starbursting 26
Task: Starburst the potential secondary effects of the I-35W Bridge collapse 26
Collapse: Case Conclusion 28

- Created three studies for course use
- List of relevant critical infrastructure protection readings, separated by topic and year; constantly updated.
- List of over 400 subject-matter experts in critical infrastructure protection, speakers bureau
- Developed 2 additional CIP courses (International, Cross Sector)
- Developing 2 additional CIP courses, Conducted Pilot course for DHS in Spring 2014 for 30 students from interagency working in Infrastructure Protection
- Developing Executive MBA with Critical Infrastructure track. Passed accreditation review in May 2014

All graduate courses and resources available on CIP/HS website.

Executive MBA with Critical Infrastructure Track

Conceptual Structure

- **Opening Residency**
  - *Foundations of Critical Infrastructure and Resilience: Strategic View of the Critical Infrastructure Firm*
  - Building the High Performing Team
- **Module 1**
  - *Partnering and Information Sharing: Government – Industry Relationships*
  - Managerial Economics
- **Module 2**
  - Applied Business Decision Models
  - Financial Accounting
- **Module 3**
  - Managerial Finance
  - Global Macro Economics
  - *Risk Assessment and Management for Critical Infrastructure*
- **Module 4**
  - Marketing
  - Services and Operations Management
- **Module 5**
  - Cost Accounting and Financial Markets
  - Financial Markets
  - *Critical Infrastructure Residency*
- **Module 6**
  - Business Strategy
  - Leadership and Change Management
- **Module 7**
  - *Cybersecurity, Resilience and Critical Infrastructure Capstone Course (Including Advances in Critical Infrastructure Security and Resilience)*
  - *Critical Infrastructure Residency 2*
- **Module 8**
  - Systems Thinking and Dynamics
  - Business Ethics
  - Business and Employment Law

Note: Italics denotes critical infrastructure specific courses

George Mason University

Higher Education Initiative

Questions?

Center for Infrastructure Protection and Homeland Security (CIP/HS)

George Mason University, School of Law

3301 N. Fairfax Drive, MS 1G7

Arlington, VA 22201

Phone: 703-993-4792

Website: http://cip.gmu.edu/

Think. Learn. Succeed.

GEORGE MASON UNIVERSITY