

# *THE IMPERATIVE OF CRITICAL INFRASTRUCTURE PROTECTION*

Gary Rohen and Rod Morgan

October 27, 2011

# THE VALUE OF A VIABLE CRITICAL INFRASTRUCTURE PROGRAM

- To identify, inventory and serve as a repository of national Critical Infrastructure information
- Conduct assessments to determine each asset's criticality, vulnerabilities, systemic impacts (i.e. Risk)
- Create a comprehensive understanding of national assets and capabilities available to prevent, respond to a crisis and to mitigate consequences (Resources).
- Provides the factual data needed to develop strategies to Prevent, Deter, Mitigate, Respond to and Recover from both natural and man-made critical incidents.
- Achieve national resilience through coherent cross-sector coordination with government departments.
- Enable rapid and effective decision-making during a crisis through the timely display of critical infrastructure information on a common operational picture.
- Help create a comprehensive intelligence picture of internal and external threats both man-made and natural to the nation.

# WE BEGIN BY ASKING SIMPLE QUESTIONS...

- What's critical?
- How do you “assess” risk?
- How does one protect “it”?
- How do – can we - we disrupt a terrorist attack?
- How do we better respond when an event occurs?
- What is a “Critical Infrastructure Protection”(CIP) program?

# EXAMPLE OF SECTORS WITHIN A PROGRAM

1. Water Sector
2. Energy Sector
3. Communications Sector (Cyber)
4. Transportation Sector
5. Industry and Banking Sector
6. Tourism
7. Government Sector
8. Diplomatic Sector
9. Agriculture Sector

# INTELLIGENCE PERSPECTIVES ON PROTECTING CRITICAL INFRASTRUCTURES

- In October 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) released its Final Report.
- Many of the identified issues remain unresolved such as information sharing, and role definition between government and industry.
- Additional new challenges have developed in the post-9/11 era – particularly the increased number of our adversaries, their sophistication, and the expanding threats they pose to all our critical infrastructures.
- Intelligence capabilities that keep pace with these rapidly-evolving threats are more important than ever.

# *NEED FOR COOPERATION, COORDINATION AND INFORMATION SHARING BETWEEN GOVERNMENT AND CIVILIAN CIP*

- Mitigating threats through information sharing
  - US Public Private Partnership
  - ISAC
  - InfraGard
- All of these provide critical issues forums related to homeland and national security

# ABOUT INFRAGARD AND THE INFRAGARD NATIONAL MEMBERS ALLIANCE

- The InfraGard Program began in 1996 as a collaborative effort between private sector cyber professionals and the FBI. The program is currently in all of the FBI's 56 field offices.
- In 2003 the private sector members of InfraGard formed the “InfraGard National Members Alliance” (INMA). The INMA is a non-profit organization representing over 45,000 FBI-vetted, InfraGard Subject Matter Experts.
- The INMA has a dual-focus value proposition.
  - InfraGard provides its members with opportunities to promote the physical and cyber security of their organizations, through access to a trusted, national network of Subject Matter Experts from the public and private sectors.
  - It provides government stakeholders, at the local, state, and Federal levels, with access to the expertise and experience of critical infrastructure owners and operators.

# ROMANIA

- Ministry of Administration and Interior
- Support for National Strategy for Critical Infrastructure Protection
- National Coordination Center: to coordinate critical infrastructure protection established in the Ministry of Interior
- Inter-institutional CIP Working Group
- Development of common methodologies for identification and classification of risks, threats and vulnerabilities related infrastructure elements
- Example: Romania, critical infrastructure in various sectors has been affected, in particular, extreme weather events.



# THE WAY AHEAD

- Inter-agency coordination and cooperation
- Establish a prioritized National Threat List
- Assist in Developing a Public – Private Partnership
- Policies and Procedures
- Identify and Prioritized Critical Infrastructure Sectors
- Select and customize a Vulnerability Assessment methodology
- Training in Vulnerability Assessments
- Conduct Several Vulnerabilities Assessments
- Identify and customize a Risk Assessment tool and methodology

# Q&A