Homeland Security

Maritime Security Risk Analysis Model

USCG Presentation to Area Maritime Security Committee
History of USCG Risk Tools

- Port Security Risk Assessment Tool (PSRAT) V1 – November 2001 – supports COTP level risk planning

- Port Security Risk Assessment Tool (PSRAT) V2 – November 2002 - supports COTP/HQ risk planning

- Maritime Security Risk Analysis Model (MSRAM) V1 – December 2005 - supports local, regional and national risk planning

- MSRAM V2 – March 2007 an integrated methodology to support DHS wide security risk analysis
Critical Infrastructure Protection

Homeland Security Presidential Directive - 7

identify, prioritize, and protect
“critical infrastructure”
and
“key resources”
“Critical Infrastructure”

Systems and assets, so vital that the destruction of which would have a debilitating impact on: security, national economic security, national public health or safety

“Key Resources”

Resources essential to the minimum operations of the economy and government
Maritime Security Risk Analysis Model (MSRAM)

MSRAM was designed to identify and prioritize critical infrastructure, key resources and high consequence scenario's across sectors using a common risk methodology, taxonomy and metrics to measure security risk from terrorism at the local, regional and national levels.
“What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.”

Secretary Chertoff 4/20/05
MSRAM Elements

⇒ MSRAM Design is Based on Terrorist Attack Modes against Types of Targets

National Critical Infrastructure and Key Resources/Assets (CI/KA) Sectors

Critical Infrastructure
1. Agriculture & Food
2. Water (WTS)
3. Public Health
4. Emergency Services
5. Defense Industrial Base
6. Information Technology
7. Telecommunications
8. Energy
9. Transportation
10. Banking and Finance
11. Chemical & Hazardous Materials
12. Postal and Shipping

Key Resources/assets
1. National Monuments & Icons
2. Nuclear Power & Materials
3. Dams
4. Commercial Facilities
5. Government Facilities

Threat Attack Modes
- Aerial
- Cyberspace
- Insider
- Landside
- Waterside
- Combined

⇒ Attack Modes address the full range of DHS Attack Modes (WMD)

HSPD 7:
MSRAM Design begins with threat input from USCG Intel Coordination Center

AMSC members in the field capture their best evaluation of scenario consequences and vulnerability for each required scenario (attack mode – target type)
Risk Plot / Base line risk

CONSEQUENCE

LIKELIHOOD

Target/Attack Mode Risk

Risk Group 1

Risk Group 2

Risk Group 3
MSRAM Change Case

Base Case/MARSEC 1

Potential Change Cases:

• MARSEC level changes
• Seasonal changes (Summer, Winter)
• Changes to threat, consequence or vulnerability profiles
• Reallocation of USCG/LEA resources
• Changes in response capability
• Changes in system security capability/capacity/strategy
• Changes in technology (RAD detection)
• Changes in scenarios (e.g., (NSSE, LPG vessels transits in AOR, new targets)
Risk Reduction Strategies!

- **RESPONSE**
  - Target/Attack Mode Risk
- **PREVENTION**
  - Risk Group 1
  - Risk Group 2
  - Risk Group 3

- **SYSTEM SECURITY**

- **LIKELIHOOD**
- **CONSEQUENCE**
Security Risk Reduction counter measures / grant proposals

Risk Group 1
Risk Group 2
Risk Group 3

Target/Attack Mode Risk

Risk Likelihood

Security Risk Reduction counter measures / grant proposals

Risk Likelihood

Security Risk Reduction counter measures / grant proposals

Risk Likelihood

Security Risk Reduction counter measures / grant proposals

Risk Likelihood
MSRAM CONTACTS POLICY QUESTIONS

Port Security Evaluation Division

– LCDR Brady Downs, USCG

– LCDR Mark Shepard, USCG

MSRAM HELP DESK – MSRAMHelp@uscg.mil
MSRAM
Questions