U.S. Department of Energy
Office of Civilian Radioactive Waste Management

www.ocrwm.doe.gov

Transportation Security Risk Assessment

Presented to:
Nuclear Waste Technical Review Board

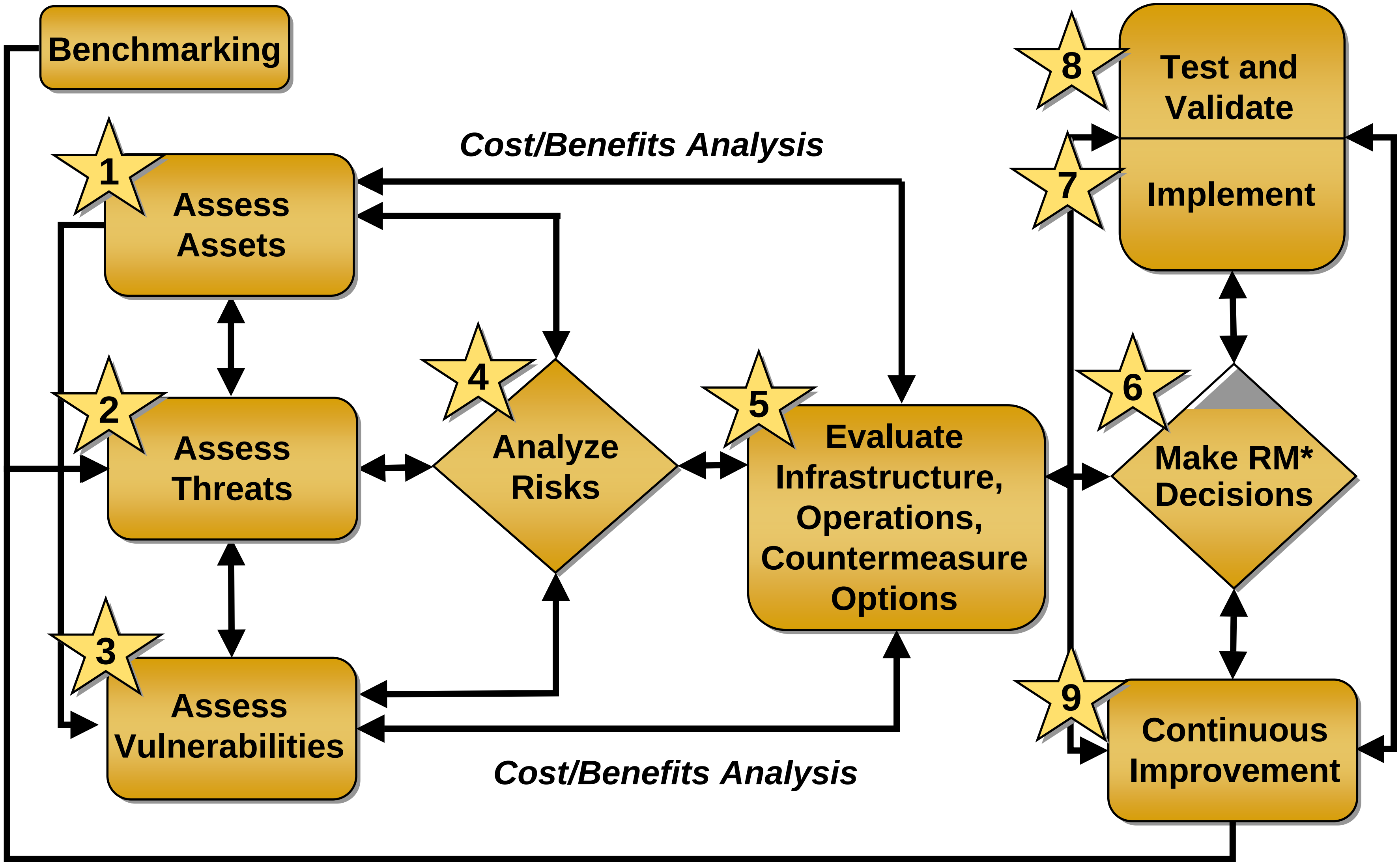
Presented by:
Nancy Slater Thompson
Office of National Transportation

October 13, 2004
Salt Lake City, Utah

Introduction

- The Office of National Transportation (ONT) is in the early stages of developing its transportation security program
  - The DOE has considerable successful experience in secure transportation
  - We are actively working with States, Tribes, local governments, other Federal agencies, and the international community and monitoring output of National Academy of Sciences and Department of Homeland Security's critical infrastructure protection activities
- As we develop our program, we are committed to five fundamental principles: partnering, integrating, innovating, continuously improving, and communicating
- Today, we will focus on one aspect of our security program, risk management

Systems Approach to Risk Management



* Risk Management

★1 Identify Critical Assets

- Determine key assets requiring protection
- Identify undesirable events and expected impacts of asset loss
- Rank assets based on consequence of loss

2 Identify and Characterize Threats

- Identify threat categories and adversaries
- Determine capability of the adversaries
- Estimate impact of threat relative to each critical asset
- Rank threats

3 Identify and Analyze Vulnerabilities

- Identify vulnerabilities of specific assets related to undesirable events
  - Any weakness that can be exploited by an adversary to impact an asset
    - For example -- poor building or equipment design, inappropriate personal behavior, no security training for employees
- Identify existing infrastructure, operations, and countermeasures and their level of effectiveness in reducing vulnerabilities

4 Analyze Risks

- Estimate degree of impact relative to each valued asset
- Estimate likelihood of attack by a potential adversary
- Estimate likelihood that a specific vulnerability will be exploited
- Determine relative degree of risk
- Prioritize risks based on integrated assessment

5 Identify Countermeasures

- Identify potential countermeasures to reduce vulnerability, threat, impact
  - Existing infrastructure and operational practices may inherently reduce risk and the need for countermeasures
- Identify countermeasure benefits in terms of risk reduction
- Identify countermeasure costs
- Conduct countermeasure cost-benefit analyses
- Prioritize options and prepare a recommendation for decision maker

Make Risk Management Decisions

- Based on supportable, defendable, repeatable processes
- Structured and flexible approach that identifies comprehensive mitigation strategies
- The results are:
  - A process for evaluating and enhancing the security features of infrastructure and operations plans and designs
  - Developing effective security procedures, protocols, and countermeasures and options that consider cost and benefits as they relate to risk reduction
  - A 'snap shot' in time that can be updated as the security posture changes

7 Implement Security Program

- Security Plan
- Protocols and Procedures
- Training
- Apply Countermeasures

8 Test, Validate, Exercise

- Drills and Exercises
- Include appropriate Federal, State, Tribal, and local agencies and private transportation providers
- Continually revaluate security posture and identify appropriate enhancements

9 Continuous Improvement

- Adjust Plans
- Monitor Threats
- Enhance Security
- Risk Management is a dynamic, ongoing process