Module 2

System Effectiveness Evaluation Process

A standard sequence of steps to evaluate system effectiveness regardless of analysis methodology
System Effectiveness Process

- VA Team Selection and Preparation
- Target and Threat Characterization
- Facility and System Characterization
- Vulnerability Search and Scenario Development
- System Effectiveness Evaluation
- System Upgrade Evaluation

VISA
# VA Team Selection

## VA Core Team Members
- Vulnerability analyst
- MC&A specialist
- Physical protection specialist
- Facility operations
- Performance testing
- Protective force

## VA Support Team Members
- Facility management
- PP maintenance
- MBA custodians
- MC&A measurements
- Nuclear material handlers
- Shipments
- Waste management
- Safety
- Nuclear criticality
- Other managers and experts as needed

## VA Team Selection Criteria
- Experience
- Team diversity
- Integration
VA Preparation

• Gather documentation
  - Engineering Drawings & Blueprints
  - Photographs
  - Performance Assurance Information
  - Facility Operating Procedures
  - Current MC&A Procedures
  - Emergency Procedures
  - Security Alarm Test Reports & Procedures
  - Security Alarm Maintenance Procedures

• Tour the site
  - General Site
  - Buildings
  - Processes
Target Characterization

- Identify targets to be evaluated:
  - Nuclear materials
    - Theft Targets
      - Discrete items
      - Bulk materials
    - Strategies
      - Abrupt Theft
      - Roll-up
      - Protracted Theft
  - Sabotage Targets
    - Radiological
    - Facilities and Equipment
Target Characterization
(continued)

- Material quantity
- Material locations and flow through the facility
  - Identify vulnerabilities and determine attack opportunities
  - Consider rollup
Target Characterization (continued)

• Rollup
  ▪ The accumulation of smaller quantities of special nuclear material to a target category
  ▪ MPC&A Measures may be less restrictive for smaller quantities
    • Physical protection
    • Surveillance measures
    • Access controls
    • Inventories (less frequent, smaller samples)
  ▪ Determine if credible
Target Characterization
(continued)

• Document Target Material Descriptions:
  ▪ Location
  ▪ Outer and inner container descriptions (size, weight)
  ▪ Nuclear material description (size, weight, configuration, portability, enrichment, etc.)
  ▪ Accessed/secure frequencies
  ▪ How often material is removed from container
Target Prioritization

More attractive

Least Protection

Smallest quantities

Level of protection is consistent with consequence of loss.

Most Protection

Largest quantities
“Less Than Target Quantity”

• Based on incidents reported to IAEA, only a few involved seizures of kilogram quantities of weapons-usable nuclear material. Most involved very small quantities.

(See Appendix A for details.)
Threat Characterization

• **Design Basis Threat**
  - Defines the threat MPC&A systems must perform against
  - Based on threat assessment
  - Periodically reviewed and revised
Threat Characterization (continued)

- Threat definition
  - Types of adversaries
    - Insiders
    - Outsiders
    - Insider/Outsider collusion
  - Range of adversary tactics
  - Capabilities
  - Motivation
Facility Characterization

Process

• Philosophy
  ▪ Document major assumptions
  ▪ Methodical and comprehensive

• Steps
  ▪ Gather information
    • Documentation
    • Interviews
  ▪ Obtain or develop facility schematics for analyzing possible adversary paths and target(s)
  ▪ Characterize MPC&A measures
  ▪ Identify facility states (shifts, hours of operation, configuration)
Facility Characterization (continued)

• Gather information related to key targets
  ▪ Site, facility, and MPC&A system components
  ▪ Physical protection plans and procedures
  ▪ Security posts, plans and procedures
  ▪ Material control and accountability plans/procedures
Facility Characterization (continued)

- Information sources:
  - Facility tours
  - Architectural diagrams
  - Interviews with management and workers
  - Safeguards and security and material control and accountability plans
  - Maintenance and operating procedures
  - Safety analysis reports
  - Previous vulnerability assessments, audits, surveys, etc.
Facility Characterization (continued)

MPC&A Functions

Detect & Assess
- Intrusion Sensing
- Alarm Communication
- Alarm Assessment
- Entry Control
- Measurements
- Radiation Monitoring
- Inventory

Delay
- Passive Barriers
- Active Barriers

Respond
- Engagement:
  - Communication to Response Force
  - Deployment of Response Force
- Neutralization
Facility Characterization (continued)

• Protective Force
  ▪ Staffing levels and locations for all different operating shifts
  ▪ Equipment (weaponry, ammunition, body armor)
  ▪ Communications equipment (radios, pagers, cellular telephones)
  ▪ Training and capability
Vulnerability Search and Scenario Development

• Exploit potential vulnerabilities
• Develop for each specific adversary type
  ▪ Insider scenarios
  ▪ Outsider scenarios
  ▪ Insider/Outsider collusion scenarios
Insider Scenario Development

• Define personnel types
  ▪ Access to facility and target locations
  ▪ Hands-on
  ▪ System maintenance
  ▪ Supervision
  ▪ Material movement
  ▪ Shipment requirements
  ▪ Remove material
Insider Scenario Development (continued)

• Group Insiders
  ▪ Combine personnel types
    • Same authorized access
    • Authority over protection
    • Knowledge
    • Similar safeguards performance
  ▪ Group Attributes
    • Hands-on
    • MC&A records
    • Transfer material
    • Alarms
    • Security
Insider Scenario Development (continued)

• Range of insider tactics
  ▪ Exploit knowledge
  ▪ Abuse authority
  ▪ Tamper with components
  ▪ Shield material
  ▪ Falsify records
  ▪ Hide material
  ▪ Create emergency
  ▪ Defeat delay
Outsider Scenario Development

- Determine needed information
- Plan approach to facility
  - `Foot, vehicle, or airborne`
- Entry method
  - Deceit
  - Stealth
  - Overt action
Outsider Scenario Development
(continued)

**Attack Plan**

- Develop Adversary Force Organization
- Identify Equipment and Weapons
- Consider Pre-Attack Activities
- Develop Concept of Operation
- Develop timeline
Outsider Scenario Development
(continued)

Example Adversary Team

- Team 1
  - Sniper Team A
    - West Sniper 1
    - South Sniper 2
  - Breach Team B
    - Fence/Wall Breacher 1
    - MG/RPG 2
  - Cover Team C
    - Driver 1
Outsider Scenario Development
(continued)

- **Facility entry considerations**
  - Doors / surface / windows
  - Barrier penetration
  - Explosive entry or hand/power tools

- **Material Acquisition**
  - Target task time
    - Tie-downs
    - Containers
  - How much material and what type
  - Weight