Course Description

- Provides structured analysis approach so participant will be able to:
  - Evaluate the effectiveness of current and/or planned MPC&A systems against an insider threat
  - Identify MC&A technical and administrative measures for insider threat protection
  - Evaluate effectiveness and relevance of measures
    - Scenario development
    - Analysis
  - Identify and evaluate MC&A upgrades that could reduce the risk of insider malevolence.
- Provides new understanding of MC&A and complexities of protracted theft.
- All instruction is focused on the protection of assets from personnel with access to nuclear materials and how to evaluate and protect against an insider threat.
- Instruction is in the form of classroom lectures, discussions, group exercises, case studies, and demonstrations.
- Course Duration: 2 days

Course Objectives

- Reduce risk of insider activities through administrative actions
- Use physical controls to limit insider activities
- Identify MC&A detection elements
- Identify MC&A assessment elements
- Provide appropriate response and mitigations to malicious incidents
- Learn to use Insider Protection Approach systems to evaluate existing programs, or establishing new MC&A programs

Course Examples and Exercises

Hypothetical Facility Overviews exploring examples of administrative and physical MC&A systems with example facilities and targets to discuss how different controls work to reduce the insider threat.
1. Exclude Potential Insiders

Pre-Employment Screening
- Application Process
- Background Checks
- Financial Obligations
- Work History

2. Exclude Further Potential Insiders

For Authorized Personnel
- Periodic Re-Investigations
- Employee Satisfaction Programs
- Escort/Surveillance of Infrequent Workers
- Security Awareness
- Human Reliability Programs

3. Minimize Opportunity

- Compartmentalization of Information and Facility Access
- Inventory Management
- Nuclear Safety/Security Integration
- Safety/Security Inspections
- Quality Assurance Programs
- Materials Surveillance

4. Detect and Assess

- Detecting Abnormal Events: Administrative/Technical/Procedural
- Prompt vs Delayed Detection
- Access Controls, TIDs, Alarms
- Material Accounting, Transfer Procedures, Trend and Statistical Analyses, Physical Inventories

5. Recover, Mitigate, and Prosecute

Response if malicious act is not prevented:
- Recovery of Stolen/Diverted Material
- Mitigation to Minimize Consequences
- Prosecution of the Insider