Nuclear Material Control and Accountability for Insider Threat Mitigation

Amy Wilson
Director
Y-12 Nuclear Material Controls and Accountability

Patrick Thomas
Program Analyst
Y-12 Nuclear Material Controls and Accountability

Consolidated Nuclear Security, LLC
Physical Security Systems, Protective Force, and Vulnerability Assessment ensure a site can win the fight...

Material Control & Accountability ensures the fight never happens.
Insider Definition

A person who, by reason of official duties, has knowledge of operations and/or security system characteristics, and/or position that would significantly enhance the likelihood of successful bypass or defeat of positive measure should that person attempt such an action.

- An effective program deters, and detects unauthorized acts by an insider

- A best in class program does this while balancing cost and efficiency for meeting the deliverables to the customer.
Nuclear Material Control Objectives – DOE O 474.2

Material containment and surveillance program in conjunction with other security program elements must have the capability to detect, assess and respond to unauthorized activities and anomalous conditions/events.

In coordination with security organizations, material control measures assure that appropriate protection and controls are applied to nuclear materials according to the quantity and attractiveness of the material.

These defined purposes and controls objective are designed to support the Insider Program, which are designed to prevent a single person from defeating layered security features.
Insider Analysis

NMC&A plays an active role in all the steps of the design and monitoring of material security protection design and the Insider Vulnerability Analysis process:

1. Characterize the facility/location with an emphasis on the insider-related safeguards.

2. Identify targets for each insider scenario.

3. Define insider personnel types.

4. Define access, authorities, and knowledge of each type of potential adversary.

5. Validate/Define protective measures designed to defeat potential insider scenarios.
1. Facility Characterization

The NMC&A role for facility characterization is to provide guidance and confirmation of the target information

- Attractiveness level (types and material forms)
- Category (quantities)
- Locations
2. Identify Potential Insider Scenarios

**Collusion** – an insider acting in collusion with an outside adversary force, attempts to relocate SNM outside of an authorized storage location

**Theft** – a single insider acting alone attempts to remove a quantity of SNM from an authorized storage location:

... in a single attempt without detection (covert)

... or is willing to give up detection in an effort to exploit speed and/or authority to remove SNM (overt)

... or by removal of small amounts of SNM over time (protracted/diversion)
# NMC&A Contributing Controls

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Example NMC&amp;A Contributing Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collusion</td>
<td>Data entry personnel and system programmers required to be in HRP</td>
</tr>
<tr>
<td>Covert Theft</td>
<td>Item Monitoring</td>
</tr>
<tr>
<td>Overt Theft</td>
<td>Material surveillance, TID application/removal</td>
</tr>
<tr>
<td>Protracted Theft/Diversion</td>
<td>Inventory, Trend analysis, Process Monitoring</td>
</tr>
</tbody>
</table>
3. Define Insider Personnel Types

Examples of Insiders can include, but are not limited to:

- Operations Personnel
- Facility Maintenance Personnel
- Protective Force Security Police Officers
- Physical Security Systems Representatives
- Vulnerability Assessment Personnel
- Security System Engineers
- NMC&A Accountants
- Material Balance Area Custodian
- Performance Testers
### 4. Define access, authorities, and knowledge

<table>
<thead>
<tr>
<th>Knowledge Examples</th>
<th>Access Examples</th>
<th>Authority Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protective Force tactical information</td>
<td>• Storage areas</td>
<td>• Data entry</td>
</tr>
<tr>
<td>Vulnerability Assessment and/or Physical Security analyses</td>
<td>• Process areas</td>
<td>• Application and removal of tamper-indicating devices</td>
</tr>
<tr>
<td>Material detection thresholds</td>
<td>• Authorized “Hands On” to:</td>
<td>• Prepare material shipments</td>
</tr>
<tr>
<td>Alarm locations</td>
<td>– Highly attractive materials</td>
<td>• Tests/Maintain security alarms</td>
</tr>
<tr>
<td>Material locations and inventory details</td>
<td>– Bulk quantities of material</td>
<td>• Confirm measurements</td>
</tr>
</tbody>
</table>
5. Validate/Define protective measures designed to defeat potential insider scenarios.

NMC&A provides information on:

- Day-to-Day operations
- Potential insider attributes (Knowledge, Access, Authority)
- Potential insider personnel lists
- Performance testing
- Material Surveillance controls
- Process monitoring thresholds
- Inventory controls
Meeting the objectives

Detect, assess and deter

NMC&A elements

Physical security elements

Vulnerability analysis

Protective Force

Personnel security access controls

Prevent the Fight.

Win the Fight.
Key Assumption to NMC&A Controls

Everything else worked.
Key Components

All of these components work together against the insider
Pre-Attack Intervention

Clearance Investigations
• Credit/background checks, personnel interviews, drug testing, criminal history

HRP screening
• Physical/psychological screenings, random polygraphs, annual recertification

Security Driven Procedures
• Approved plans, trained escorts
Layered Access Control/Barriers

Need-to-know Verification
- Read and/or write information access controls
- Badge, pin, and biometrics at various security layers

Separation of Duties
- Lock/key controls, TID Custodians and Applicators
- Identify Verification systems requiring multiple users

Intrusion Detection Systems
- PIDAS, PA, MAA, Storage locations
- Material/metal detectors
- Camera surveillance
Material Control and Accountability Monitoring

Material Surveillance
• Two person rule, material surveillance controls

Process Monitoring
• Input – output = process difference

Inventories
• Measurements, reconciliation, item monitoring

Tamper Indicating Device
• Acquisition and application procedures, integrity verification

Transfer procedures
• Shipment evaluation, transfer checks
MATERIAL CONTROL & MATERIAL ACCOUNTABILITY
ELEMENTS OF THE INSIDER THREAT MITIGATION PROGRAM
Is the target in locked and alarmed storage OR under two-person rule?

- YES
  - Insider analysis would be active/violent; requires collusion

- NO
  - Analyze MITIGATION FACTORS APPLICABLE TO THIS TARGET
    - Tamper-Indicating Devices
    - Material/Container weight (non-man portable)
    - Tools required
    - Technical knowledge needed
    - Locks and alarms
    - Protective Force strategy
    - Material Surveillance
    - Task time
    - Retrieval attempts necessary
    - Inventory frequency
    - Process Monitoring activities
    - Environmental considerations (i.e. heat, vacuum)

  - ANALYZE
    - Is the mitigation Factor(s) adequate for Protecting this target?
      - NO
        - Analyze Insider as “ACTIVE NON-VIOLENT”
          (Covertly assist the adversary by unlocking doors, triggering false alarms, and providing information, will not use physical force or violence)

      - YES
        - Analyze Insider as “PASSIVE”
          (provide information and/or failure to report adversary actions)
Questions
Disclaimer

This work of authorship and those incorporated herein were prepared by Consolidated Nuclear Security, LLC (CNS) as accounts of work sponsored by an agency of the United States Government under contract DE-NA0001942. Neither the United States Government nor any agency thereof, nor CNS, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, use made, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency or contractor thereof, or by CNS. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency or contractor thereof, or by CNS.