25. Preventive and Protective Measures Against Insider Threat

April 29 – May 18, 2018
Albuquerque, New Mexico, USA

Learning Objectives

After completing this module, you should be able to:
• Define the insider threat
• Define insider targets and associated special considerations
• Describe specific measures that may be implemented for prevention of and protecting against insiders
IAEA Nuclear Security Series 13 (NSS-13) and NSS-8

3.36 When considering the threat, due attention should be paid to insiders. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The PPS should be assisted by NMAC measures to deter and detect the protracted theft of nuclear material by an insider.

NSS-8 The objective of this Implementing Guide is to provide updated general guidance to States, and their competent authorities, and operators, on selecting, implementing, and evaluating measures for addressing defined insider threats.

Breakdown of Incidents from January 1993 through December 2014

2727 confirmed incidents have been reported to the ITDB, including the following:

- 442 incidents involved unauthorized possession and related criminal activity (illegal possession, movement, or attempts to illegally trade in or use nuclear or radioactive sources)
  - 16 of the 442 incidents involved highly enriched uranium (HEU) or plutonium
- 714 incidents were reported involving the theft or loss of nuclear and other radioactive material
- 1519 incidents involved other unauthorized activities including unauthorized disposal of radioactive materials or discovery of uncontrolled sources
Insider Categories

- Passive: No action, transmit information
- Active Non-violent: Uses stealth and deceit, not force, against personnel
  - Willing to use covert force against barriers and hardware
  - Aborts if detected and confronted while in the act or is in danger of being identified
- Active Violent: Willing to use force against personnel

Internally motivated or Externally coerced

Potential for Malicious Act

- Ideological, Financial, Revenge, Ego, Psychological, Coercion, Unwitting
- Access, Authority, Knowledge

= Potential Malicious Act

Insider Motivations + Insider Opportunity
Motivations: Insider

- Ideological
  - Fanatical conviction
  - Political conviction
- Financial – wants / needs
- Revenge / Embarrassment – disgruntled employee or customer
- Ego – “Look what I am smart enough to do”
- Psychological – Mentally unstable
- Coercion – Family or self threatened
- Unwitting – Exploited without his/her awareness

Opportunity: Insider

Access
Authority
Knowledge

Insider
Opportunity
Insider Opportunity Attributes: Access

- Authorized work areas – physical access
- Unauthorized access (easy to obtain?)
  - Special temporary access
  - Escorted or unescorted (restrictions on insider during access)
  - Emergency access (fire, medical, police)
- Access to target
  - Duration of target exposure
  - Conditions of target during insider access
- Access to databases and systems
  - Cyber access (e.g., design information, accounting information)
- Equipment access
  - PPS, NMAC, safety, and process systems

Insider Opportunity Attributes: Authority

- Authority over people
  - Designated authority over others
  - Personal influence over others
- Authority over tasks and equipment
  - Assessment of alarms
  - Preparation of sensitive forms
  - Authorization of processes and procedures
- Temporary authority
- Falsified authority
- Exemption from procedures
Insider Opportunity Attributes: Knowledge

- Locations, characteristics, and details of targets
- Details of facility layout
  - May be obtained from records kept outside the facility
- Security system operations and vulnerabilities
- Processes, procedures, and operations
- Safety and radiation protection systems
- Available tools and equipment

Target Characterization—Unauthorized Removal

- Identify all nuclear material to protect against unauthorized removal, considering:
  - Abrupt unauthorized removal (bulk material or discrete items)
    - Unauthorized removal of large quantity of nuclear material during a single event
  - Protracted unauthorized removal (bulk or process materials)
    - Repeated unauthorized removal of small quantities of nuclear material during several events, for example
      - Material moved from facility each time it is taken
      - Material moved into a hidden cache (roll-up) for removal from the facility in one event
Target Characterization—Sabotage

- Nuclear materials
- Process or support equipment needed to prevent radiological consequences

Protection of Facility Systems

- Facility systems that contribute to nuclear security systems can be used by an insider to
  - Indirectly perpetrate attacks
  - Aid an external adversary
  - Mask unauthorized removal or sabotage acts
    - Systems may include PPS, NMAC, safety, and process systems
- Less obvious is information provided by or about detection elements or systems
  - PPS design information, vulnerability assessment information
  - Radiation portal monitor or metal detector limits
  - Physical inventory schedule, accounting information, inventory difference limits
Insider Threat Case Study

- Case studies provide a very good source to illustrate malicious acts by insiders have occurred
- Case study presented is based on independent research from outside IAEA
  - Theft of HEU at the Luch Scientific Production Association, Podolsk, Russia
  - This case study was derived purely from open sources including peer-reviewed academic articles, news reports and government testimony and statements by subject matter experts (SMEs)
    - Minor variations in different accounts, reconciled as much as possible.
  - Wider contextual information on the nuclear security situation in FSU in the early 1990s has also been included

Overview

- **Facility**: Luch Scientific Production Association, Podolsk (40km South West of Moscow), Russia
- **Date**: Late May to early September 1992
- **Incident**: Theft of weapons-grade HEU – 90% $^{235}\text{U}$
- **Perpetrator**: Leonid Smirnov, Luch Scientific Production Association
- **Impact**: Approximately 1.5 kg was stolen and later recovered (first documented theft of HEU from a nuclear facility in the FSU)
Profile—Leonid Smirnov

- Had worked at Luch Scientific Production Association for over 25 years
  - Chemical engineer working on nuclear reactors for Soviet space programme
  - Major role: Dispense HEU to research teams
- Intended to sell HEU for financial gain, ‘to buy a new stove and refrigerator’
  - Does not appear to have had a buyer in mind, planned to sell to firms in Moscow, thought he’d have ‘no trouble selling it’

Incident Timeline

- Early 1990s dissolution of Soviet Union
  - Reduction in working conditions, wages for nuclear FSU scientists, & hyper inflation => Financial hardship
- Apparently became aware of potential value of HEU from article in Russian newspaper
  - “I read an article on someone stealing 1200 grams of uranium... The idea flashed through my mind... why can’t I do the same? ”
- May 1992 – Started removing small quantities (25 to 70 grams) of HEU as UO₂ powder, while alone in room
  - Siphoned off ~1% of the 3% ‘irretrievable loss’
  - 20 to 25 diversions over a 5-month period
  - Stored the HEU at his home on his balcony in a lead container
Incident Timeline (cont’d)

- 9 October 1992 – Arrested at Podolsk Railroad Terminal with most of the HEU concealed in three lead cylinders within a briefcase
  - Apprehended purely by chance, having bumped into neighbors being followed by police for stealing batteries from their factory
  - Was planning to travel to Moscow to sell the HEU
- March 1993 – Tried, found guilty of stealing and storing nuclear material and sentenced to three years probation

Insider Opportunity Attributes—Smirnov

- Access: HIGH
  - Hands-on access to HEU
- Authority: LOW
  - But did not need the support of anyone else
- Knowledge: HIGH
  - Knew properties of HEU, understood weakness of NMAC and wider security systems
Security System Failures

- Weak nuclear material accounting and control (NMAC)
  - Process allowed for a 3% ‘irretrievable loss’
  - Missing 1.5 kg did not show in balance books
  - Not a weakness unique to Luch:
    - In 1992, employees of Chepetsk Mechanical Plant in Glazov, Russia, exploited 4% allowed inventory loss to diverted LEU
- No remote visual surveillance or two-person rule
- No nuclear material detection system
  - No detection devices (e.g., portal monitors) at facility doors, checkpoints etc.
  - No bag searching upon entrance and exit

Prevention vs. Protection

- Prevention
  - Exclude potential insiders by identifying undesirable behaviour or characteristics, which may indicate motivation prior to allowing them access
  - Exclude further potential insiders by identifying undesirable behavior or characteristics, which may indicate motivation after they have access
  - Minimize opportunities for malicious acts by limiting access, authority, and knowledge, and by other measures
- Protection
  - Detect, delay, and respond to malicious acts
  - Mitigate or minimize consequences
Measures against Insiders

Individuals Applying for Access
- Reduce the number of potential insiders

Individuals with Authorized Access
- Minimize Opportunity
- Act Completed or Interrupted

Individuals with Access to Critical Assets or Vital Areas
- Detect, Delay, Response

Insider Initiates Act

Mitigation

Number of People

Apply Preventive Measures

Apply Protective Measures

Exclude the Potential Insider

- Filter potential Insiders before they have authorized access to a site
  - Examples of Pre-employment Hiring Process
    - Identity verification
    - Work history to determine past work practices
    - References to identify possible undesirable behaviours
    - Background checks to identify criminal activity
    - Credit checks to evaluate financial situation
    - Drug screening to identify substance abuse
  - Deterrence effect
Further Exclude Potential Insiders

• After an individual has authorized access to the site, measures can include the following:

  - Employee evaluations including periodic background checks
  - Trustworthiness programs
  - Nuclear Security Culture
  - Continuous observation programs
  - Employee satisfaction programs
  - Protection of sensitive information
  - Compartmentalization
  - Authorization / revocation of access
  - Adherence to standard operating procedures
  - Sanctions
  - Quality Assurance programs

Minimize Opportunity

• Separation (physical compartmentalization)
• Limitations on individual access (need to know rule) and on persons empowered to give access authorization
• Escorting and surveillance:
  ▪ Protects against unapproved access or actions by visitors or personnel without authorized access
• Need to know protection of information that could be exploited:
  ▪ Location and condition of sensitive targets
  ▪ Shipping schedule
  ▪ Critical elements of system design
Minimize Opportunity (cont’d)

- Confidentiality (security of information)
- Quality Assurance
  - Provide confidence that specific requirements are satisfied for all activities important to prevention of and protection against insider
- Separation of Duties
  - Establish checks and balances to ensure that one person does not have sufficient access, authority, and knowledge to conduct malicious activities without detection
  - Example: Work order authorized by a supervisor is required and verified by security before two operators can access a vault to remove material for processing

Detect, Delay, and Response

![Diagram showing the process of reducing the number of potential insiders through applying preventive and protective measures.](Image)
Detection of Insider Actions

- A malicious insider may pick the most opportune time for action, so a continuous timeline or order of actions may not be applicable
  - Detection is possible only after initiation of malicious action
  - Detection may be a function of the number of events
  - Actions may be extended over long periods of time if not detected
- Detection may be by
  - Personnel (e.g., guards, co-workers)
  - System (e.g., protection, operations, or safety alarms)

Detection of Insider Actions (cont’d)

- A malicious insider tries to minimize detection using:
  - Deceit and stealth rather than force
  - Plausible deniability to prevent correct assessment
- A malicious insider may:
  - Test the protection system with “normal mistakes” prior to initiating malicious act
  - Take advantage of tools at their work location
- Correct assessment may be difficult and may require analysis or investigation
Examples of Detection Systems

- Physical Protection System
  - Entry and exit control
  - Surveillance
- NMAC System
  - Material control
  - Material accounting
- Operations System
  - Observation by personnel
  - Operational process alarms
- Safety System
  - Criticality / fire alarms
  - Safety inspections

Detection – NMAC System

- Material Accounting – Detects abnormalities in amounts of material through:
  - Item and bulk inventories
  - Material measurements and characterization, including weight and isotope content
  - Ensuring measurement accuracy and precision goals
  - Accurate accounting records and documentation
Detection – NMAC System (cont’d)

- Material Control – Tracks material movement and maintains continuity of knowledge of nuclear material by implementing administrative and technical measures, such as:
  - Strict procedures for nuclear material movements
  - Periodic administrative checks to detect gross anomalies
  - Tags and seals (e.g., TIDs)
  - Tie Downs
  - Two-person rule

NMAC Detects Irregularities that Require Response or Investigation

- Scheduled Inventory
- TIME
- Scheduled Inventory

Investigate and Respond
- Disabled Portal Monitor
  - Violation of 2-person rule
  - Investigate and Respond

Investigate and Respond
- Errors in Accounting Reports
  - Unauthorized entry
  - Investigate and Respond

Investigate and Respond
- Suspicious Admin Check
  - Broken TID
  - Investigate and Respond

Emergency Inventory

Investigate and Respond
- Investigate and Respond
- Investigate and Respond
Detection – Operations and Safety Systems

- Operations Process Information
  - Can be used to detect small anomalies in material accounting
  - Should be analyzed to determine what information could be used to detect abrupt or protracted theft
    - Identified information should be shared with the Security System
    - Alarm generated with this information should be investigated in a timely manner
- Investigation of safety alarms could indicate malicious activity in a timely manner
  - Certain alarm conditions, including activation of passive safety systems,* should be reported immediately to security
  - Identify such alarms and establish a procedure for reporting

* Independent of human actions

Delay – Insider

- Purpose of delay for insiders
  - Complicate their tasks
  - Increase the time required to complete the task
  - Provide additional opportunities for detection
- May be provided by
  - Personnel
  - Procedures
  - Physical barriers
    - Most effective barriers require contraband items or special skills to defeat, and are located close to equipment or material
    - Use multiple layers of different physical or procedural barriers requiring different resources, logistics, training, tools and skills
Response

- Every employee and contractor should be trained to:
  - Detect a malicious act
  - Transmit the alarm according to specified procedures
  - Protect self and facility
  - Reverse, mitigate, or minimize a malicious act
- Response is complicated by the fact that the insider may not be identified
  - Response procedures should assume response personnel may be an insider

Mitigation

- Ensure the site has a plan to mitigate consequences if protection systems fail
Insider Cyber Threat

- Insider cyber threat may include:
  - Indirectly perpetrating a physical attack
  - Masking malicious acts
  - Aiding an external adversary
  - Destruction, disclosure, or modification of data
  - Denial of service
- Potential cyber insiders – system administrators, maintenance personnel, operators, developers, integrators
- Specific protection measures
  - Identification and authentication (credential)
  - Password protection
  - Event logging and auditing
  - Mitigation and recovery (redundancy, backup, and recovery procedures)
  - Establishing media devices, such as USB devices, as contraband

Key Takeaways

- An external adversary is not the only threat to consider
  - Insider could take advantage of authorized access, complemented by authority and knowledge, to commit a malicious act
- Identify all nuclear material to protect against unauthorized removal and/or sabotage by an insider
- Use both preventive and protective measures to develop effective nuclear security system against insider threat
  - NMAC procedures are important in detection
  - Consider cyber security systems