Global Material Security

Addressing the Insider Threat

U.S. Department of Energy

National Nuclear Security Administration

NNSA National Nuclear Security Administration

U.S. DEPARTMENT OF ENERGY

Definitions

Global Material Security

- Adversary- any individual performing or attempting to perform a malicious act
- Insider threat- an adversary with authorized access to a nuclear facility, a transport operation, or sensitive information
- Outsider threat- any adversary other than an insider

Insider Definition

Global Material Security

- An insider has ***authorized access*** (either escorted or unescorted) to ***controlled areas***
- Insiders may include:
  - Employees
  - Former employees
  - Contractors/Consultants
  - Suppliers
  - Visitors
  - Industrial collaborators
  - Regulators/Inspectors

Insider Capabilities

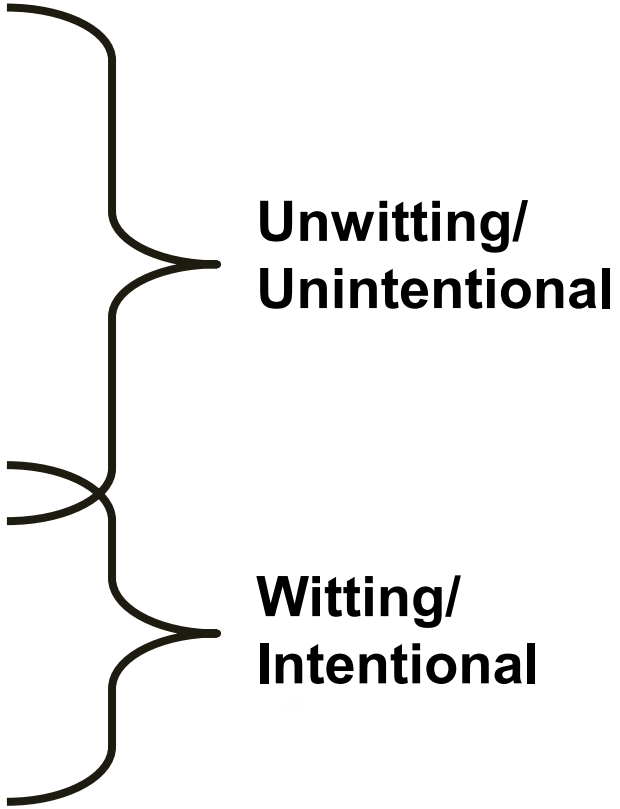
Global Material Security

- Authorized access- defined by what areas of the facility they may or may not enter during different facility states (e.g., during normal work shift, non-operational periods, maintenance outage, or an emergency)
- Authority- power or right to enforce obedience over other people or over certain tasks and equipment
- Knowledge- of targets, facility layout, protection systems, and/or how to acquire and operate special tools and equipment found at the facility

What kinds of insider threats do facilities face?

Global Material Security

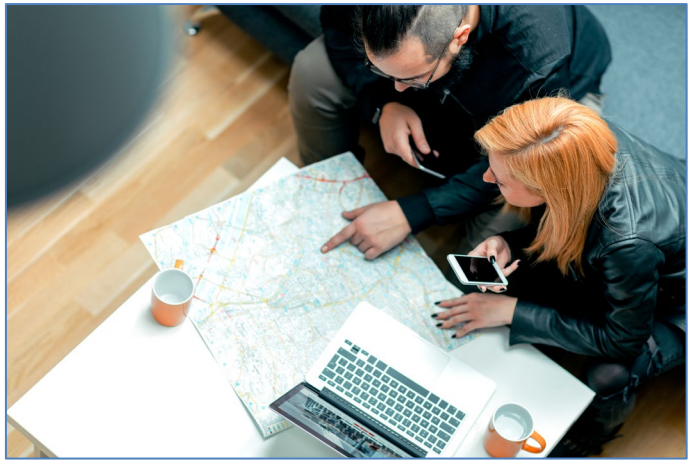
- Training delinquencies
- Illness
- Fatigue
- Lack of attention/concentration
- Petty theft
- Intentional malicious:
  - Theft
  - Sabotage



The Insider Threat

Global Material Security

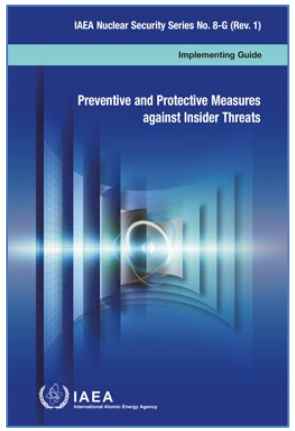
- Because of their access, authority, and knowledge, the insider has
  - Ability to bypass some technical and administrative security measures to commit theft or sabotage
  - Ability to complete objectives through a series of separate actions over an extended time period to minimize their chance of detection and maximize their likelihood of success
  - Opportunity to select the most vulnerable target and the best time to perform the malicious act

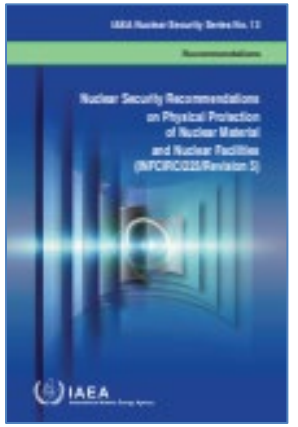


IAEA Reference Documents

Global Material Security

- NSS-13 - Implementing Guide for IAEA NSS No. 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev. 5)
- NSS-8 - IAEA Nuclear Security Series No. 8-G (Rev. 1): Preventive and Protective Measures against Insider Threats

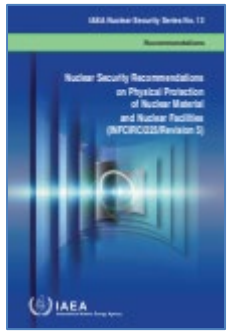




NSS-13 Physical Protection of Nuclear Facilities

Global Material Security

- “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 physical protection system should be assisted by nuclear material accountancy and control measures to deter and detect the protracted theft of nuclear material by an insider.”
- [IAEA NSS No. 13; 3.36]



NSS-8 Preventive and Protective Measures against Insider Threats

Global Material Security

- Presents a systematic approach for protecting against insiders, covering preventive measures to minimize the insider's opportunity to initiate a malicious act, as well as protection measures to detect, delay and respond to, and mitigate, an initiated insider act.

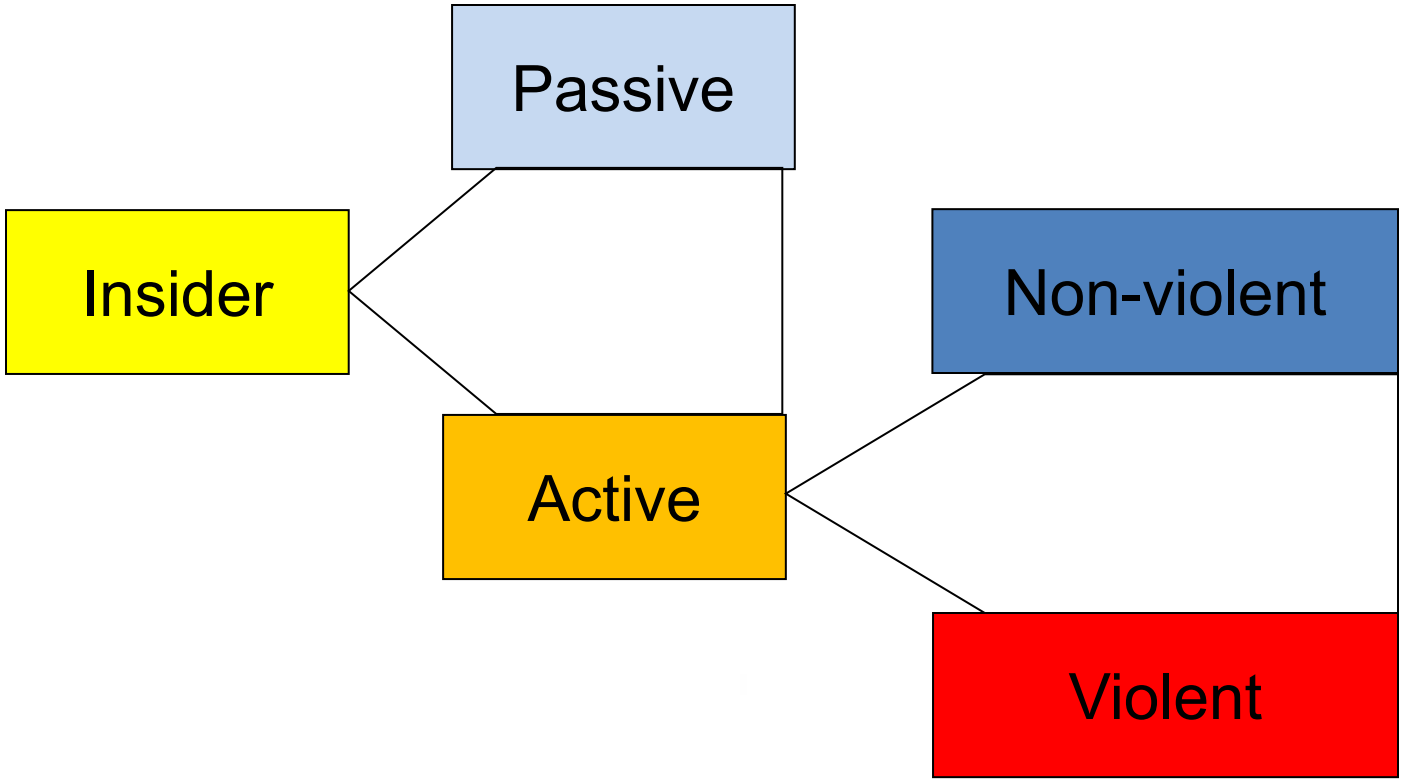
Common Insider Motivations

Global Material Security

– Ideological– fanatical conviction
– Financial– wants/needs money
– Revenge– disgruntled employee or customer
– Ego– “look what I am smart enough to do”
– Psychotic– mentally unstable but capable
– Coercion– family or self threatened

Insider Characteristics

Global Material Security



Target Identification

Global Material Security

- Nuclear material
- Buildings and equipment
- Components, systems, and functions

When evaluating the potential targets, consider sabotage and protracted theft as well as abrupt theft.

Addressing the Insider

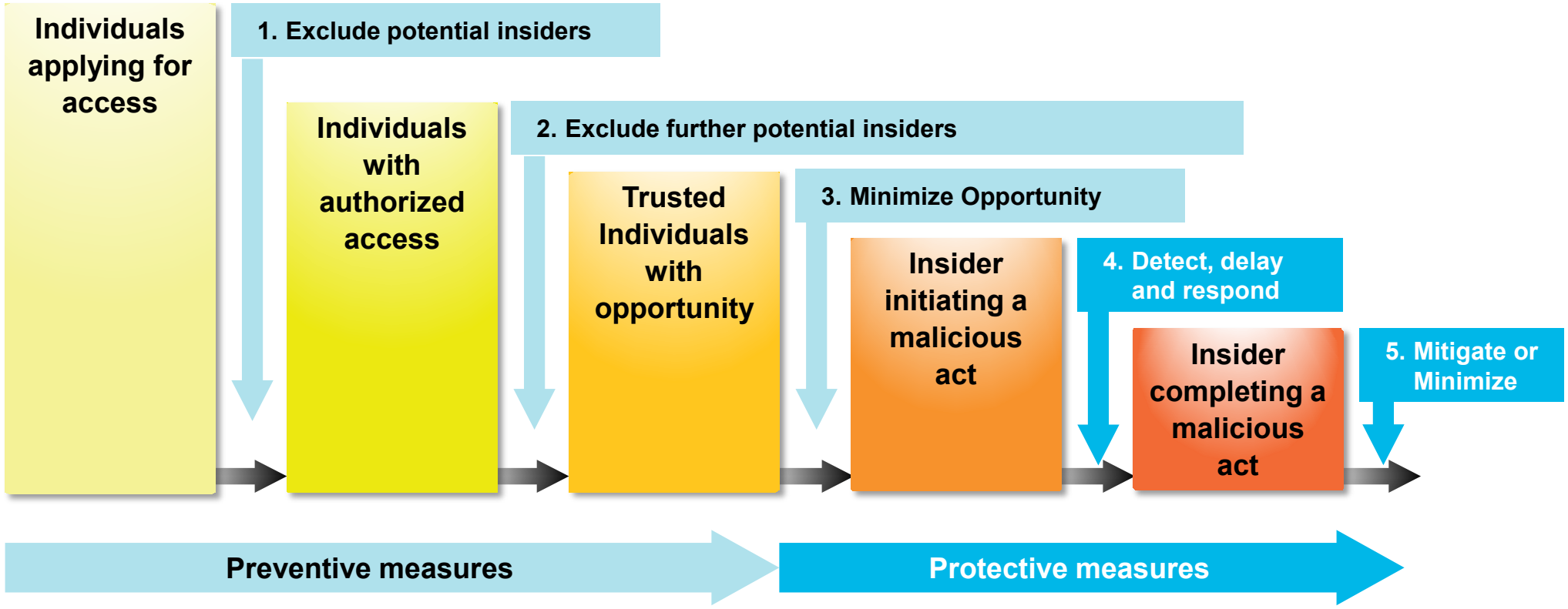
Global Material Security

- There is no one solution
- Each individual facility must assess the insider threat specific to that site
- The best way to mitigate insider actions is to create a programmatic approach designed to detect acts through technical and nontechnical means
- Systematically implement the design
- Utilize proven practices to provide a great deal of detection and deterrence of insider acts
- Customize and test for the specific facility

When addressing the insider, there is no one answer solution

Measures Against Possible Insiders

Global Material Security



IAEA Nuclear Security Series No. 8: Preventive and Protective Measures against Insider Threats

IAEA Nuclear Security Series No. 8: Preventive and Protective Measures against Insider Threats

Preventive Measures

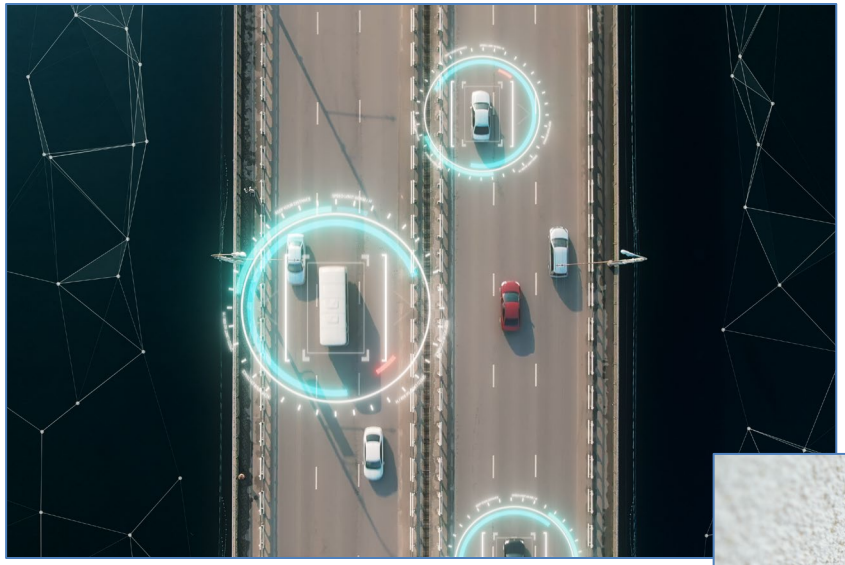
Global Material Security

- Identity verification
- Trustworthiness assessment
- Escort/surveillance
- Security awareness
- Confidentiality
- Quality assurance
- Employee satisfaction
- Compartmentalization (of data, activities, and physical areas)
- Sanctions

Protective Measures

Global Material Security

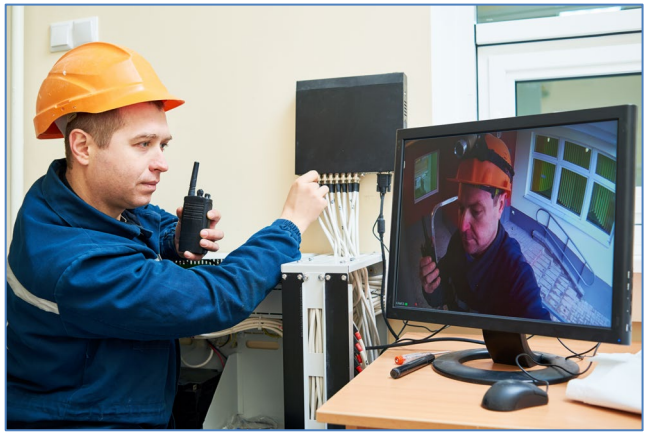
- Detection
- Delay
- Response



Detection

Global Material Security

- Alarms must be assessed to be effective
- Longer delay may be necessary for insider detection
- Sample elements
  - Two-person rule
  - Access control
  - Tracking personnel within facility
  - Contraband detection
  - Monitoring (alarms, processes, operations, inventory)
  - Certification, inspections, and audits



Delay

Global Material Security

- Increase task time of adversary
- Delay penetration of area
  - Locks
  - Barriers requiring skill/special tools
  - Multiple layers
  - Personnel
  - Redundant equipment
  - Auto shutdown/closure

Response

Global Material Security

- May be made by operations or security personnel
  - Typically operations personnel respond to the act to reverse, mitigate, or minimize it
  - Security personnel typically respond to insiders
- All employees should be trained to react and transmit alarms as necessary

Comprehensive Approach to Insider Mitigation

Global Material Security

- Layered defense
  - Technical
    - Multiple protection layers utilizing detection and delay
    - MC&A
  - Administrative/Personnel
    - Procedures
    - Instructions
    - Sanctions
    - Access control rules
    - Confidentiality rules

Technical Solutions to Insider Risk

Global Material Security

- Sensors/Alarms
- CCTV
- Access control systems
- Locks/TIDs
- Barriers
- Measuring devices
- Inventory, reporting, and accounting systems

Non-Technical Solutions to Insider Risk

Global Material Security

- Screening
- General awareness
- Observation and reporting
- Trustworthiness programs

General Standard for Granting Privileges

Global Material Security

- A comprehensive, common sense judgment
  - Made after consideration of all the relevant information, favorable or unfavorable
- Whether the granting of access authorization would
  - Endanger the common defense and security
  - Be clearly consistent with the national interest

Trustworthiness & Reliability

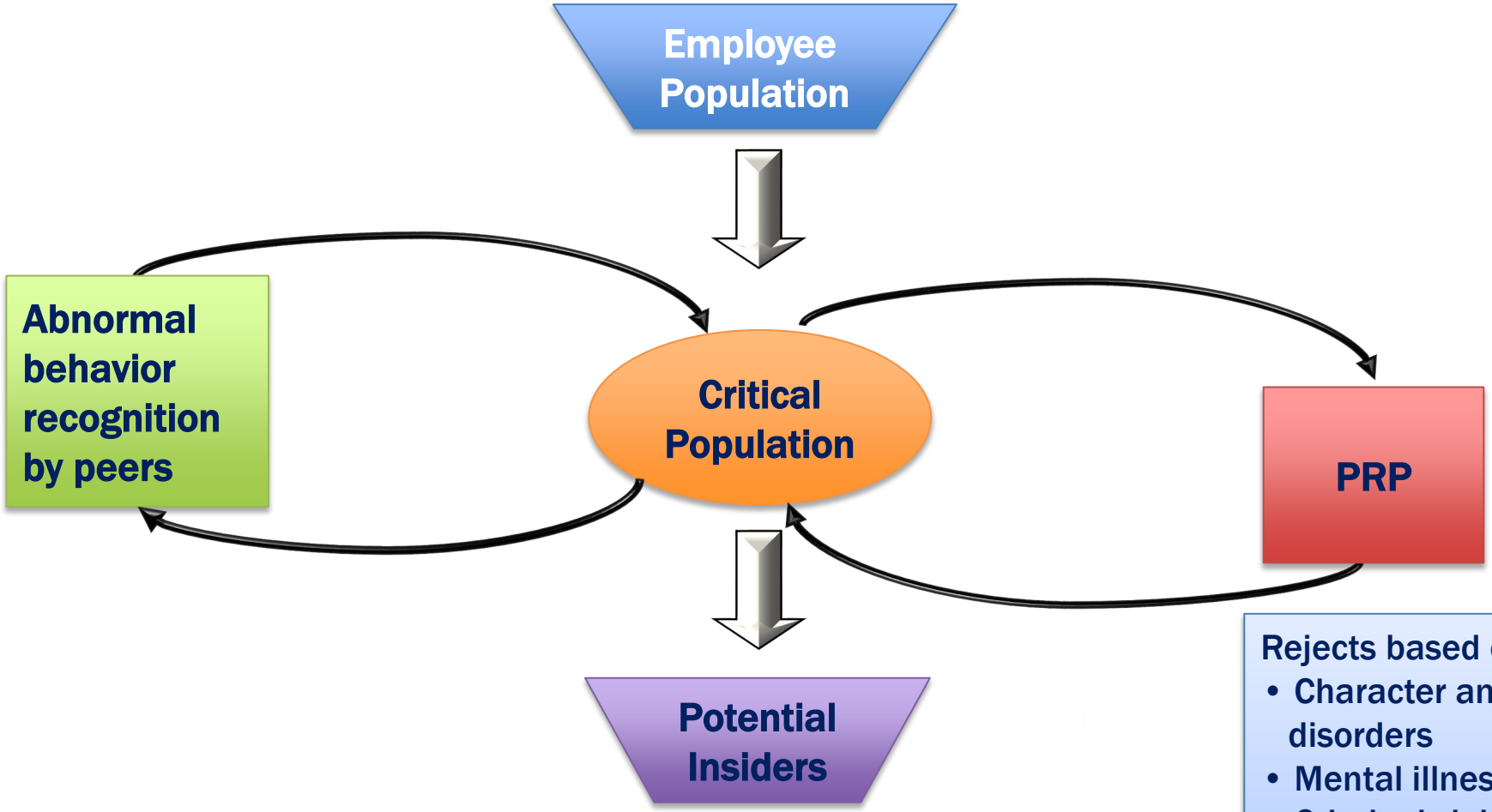
Global Material Security

- Characteristics of an individual who can be depended upon to
  - Follow both procedures and societal rules in protecting materials and information
  - Choose behavior that follows the rules rather than engage in behavior that may be personally rewarding but compromises security

Human Reliability Programs (HRPs) can be vital in establishing trustworthiness and reliability.

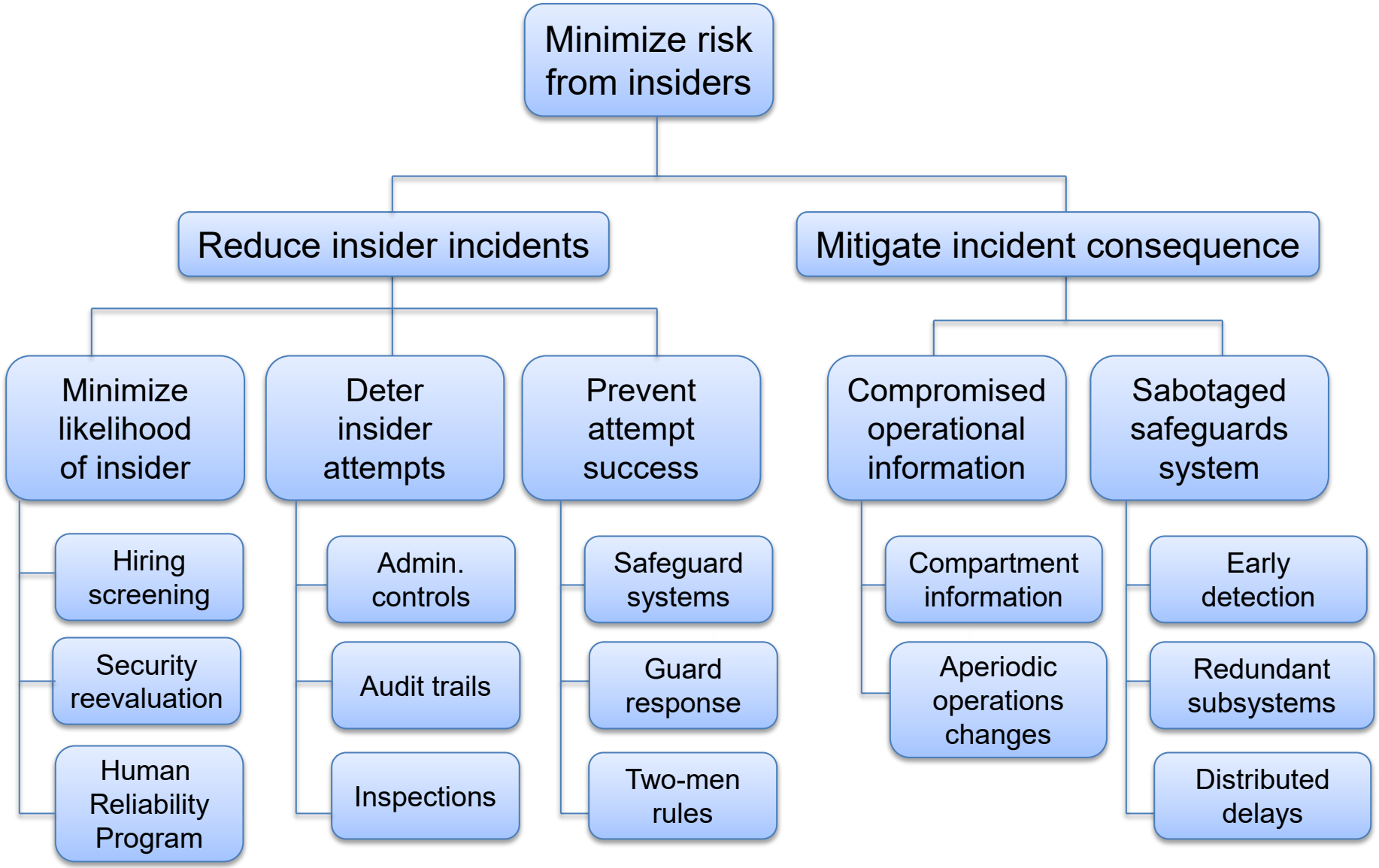
Employee Monitoring

Global Material Security



Rejects based on:

- Character and behavior disorders
- Mental illness
- Criminal violations
- Financial problems
- Family problems, etc.


Minimize risk from insiders
Reduce insider incidents
Mitigate incident consequence
Minimize likelihood of insider
Deter insider attempts
Prevent attempt success
Compromised operational information
Sabotaged safeguards system
Hiring screening
Security reevaluation
Human Reliability Program
Admin. controls
Audit trails
Inspections
Safeguard systems
Guard response
Two-men rules
Compartment information
Aperiodic operations changes
Early detection
Redundant subsystems
Distributed delays

Insider Case Studies

Global Material Security

- Open discussion of insider threat examples

Case Study – Doel Nuclear Power Station

Global Material Security

- Located near Doel, Belgium
- Plant contains four 2nd generation, pressurized water reactors, with a capacity of 2900 MW
- Operated by Electrabel

Doel 4 Timeline

Global Material Security

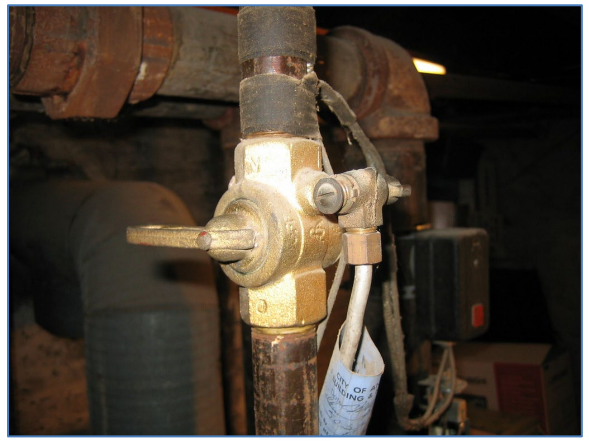
- Morning - Doel 4 turbine operating normally at 1500 rpms
- Mid-day - Workers notice increase in temperature of lubricating oil in turbine in nun-nuclear side of at Doel-4 NPP
- Workers search for cause of temperature increase (including inspection of emergency oil drain line) and find emergency fire valve is in normal, closed position
- 37 minutes from start of incident, 65,000 liters of lubricating oil drains from turbine. Turbine grinds to an abrupt stop with severe damage to the rotor blades and shaft

August 5, 2015

Doel 4 -- Investigation

Global Material Security

- Workers discover that emergency oil drain valve had been intentionally opened and the act concealed
- Valve had been secured using padlock, which was missing
- Valve had been opened, its handle removed and re-attached to simulate closed position



Subsequent investigation

Doel 4 – Incident Summary

Global Material Security

- Intentional act of sabotage by an insider
- One person, 5 minutes, 6.25 Trillion VND (250 Euro) in repair to damaged turbine, loss of income, and restart; potential energy crises
- GDF Suez spokesperson was quoted "..no outsiders had penetrated into the plant.."
- Lengthy criminal investigation
- Reactor back online December 19, 2014

Additional Insider Incidents

Global Material Security

- Turkey Point Nuclear Generating Station
  - 1/8” hole drilled in stainless steel pipe connected to pressurizer of Unit 3; covered with insulation to hide; found during testing
- Byron Generating Station
  - Purchasing manager found ordering 3 times many of the materials actually required; would sell 2/3 of them on eBay; all were stamped with Exelon logo
- Indian Point Energy Center
  - Supervisor falsified documentation on diesel fuel which was going into safety system; likely not intended to be malicious but covering himself for not doing his job; Individual was fired and prosecuted

A Worst Practices Guide to Insider Threat

Global Material Security

- Lessons learned
  - Don't assume that serious insider threats are NIMO (not in my organization).
  - Don't assume that background checks will solve the insider problem.
  - Don't assume that red flags will be read properly.
  - Don't assume that insider conspiracies are impossible.
  - Don't assume that organizational culture and employee disgruntlement don't matter.
  - Don't forget that insiders may know about security measures and how to work around them.
  - Don't assume that security rules are followed.
  - Don't assume that only consciously malicious insider actions matter.
  - Don't focus only on prevention and miss opportunities for mitigation.

Summary

Global Material Security

- The insider threat presents unique problems to both safety and security
- Proactive programs will help identify and deter potential insiders
- Continuous observation and employee awareness are critical mitigation elements

QUESTIONS/COMMENTS

Global Material Security