Defining the Insider Threat

Patrick Lynch
7 September 2015
Insider Threat Summit

Presentation Overview

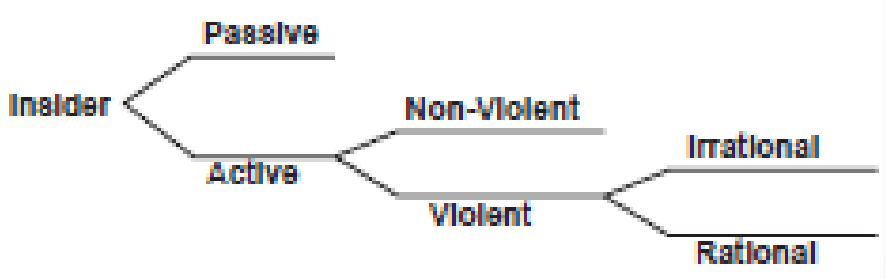
- Define Key Terminology
- Identify Attributes of Insiders
- Discuss Motivating Factors Commonly seen with Insiders
- International Documentation Available
- Mitigation Measures and Planning

Definitions

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

Defining the Insider

- Passive
  - Non-violent
  - Limited role – Supply information to adversary
  - Unknowingly active
  - Coerced
- Active
  - Makes conscious effort to engage
    - Non-violent
    - Violent



Operational Threats

- Malicious insider threat (theft, sabotage)
- Substance abuse (drug/alcohol abuse)
- Malicious mischief (personal theft, vandalism)
- Personal irresponsibility (Loss of laptops, not securing data adequately)
- Lack of training/preparation/contingency planning
- Fatigue/focus (long shifts, personal issues)

Key Attributes

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

Insider Capabilities

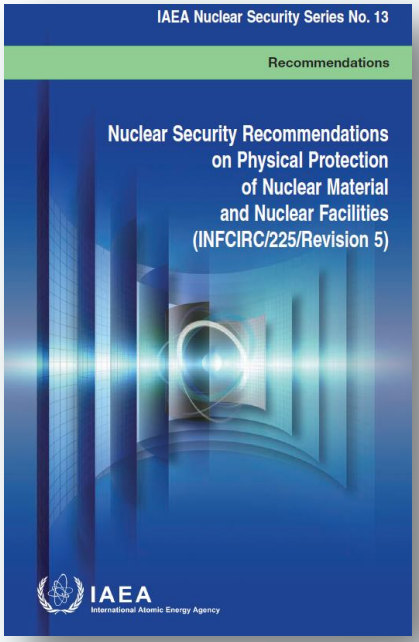
- Authorized access - defined by what areas of the facility they may or may not enter during different facility states, e.g. normal work shift, non-operational periods, maintenance outage, or during a security or safety event;
- Authority - power or right to enforce obedience over other people or over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

The Insider May Have…

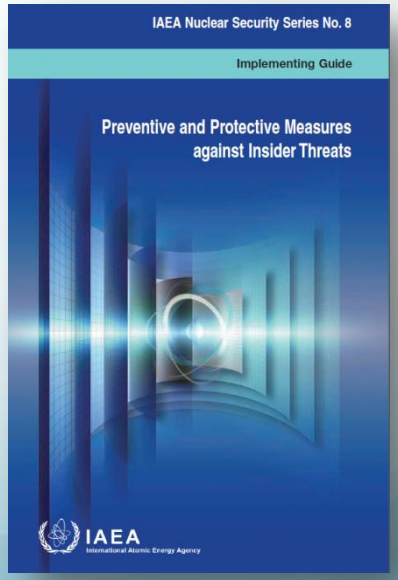
- Ability to by-pass some technical and administrative physical protection measures to commit theft or sabotage
- Ability to complete objectives through a series of separate actions over an extended time period to minimize their chance of detection and maximize their likelihood of success
- Opportunity to select the most vulnerable target and the best time to perform the malicious act

IAEA Reference Documents

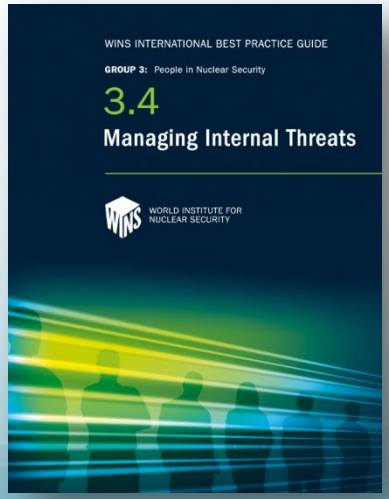
- Nuclear Security Series-13 - Implementing Guide for IAEA NSS No. 13: Physical Protection of Nuclear Facilities



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



- WINS Resources



Common Insider Motivations

- 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

Motivation may determine the type and extent of malevolence

Addressing the Insider

- There is no one solution
- Each individual facility must assess the insider threat specific to that site
- 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
- Motivate the workforce by helping them understand the benefits of the program

Disgruntled Workers

- May represent the most serious threat to the safety and security of the facility
  - May willfully disregard rules/regulations in order to “get even” and can result in serious damage to the organization
  - Sense of right or wrong is overwhelmed by the need to reach a goal such as revenge

Signs of the Disgruntled Worker

- Displays low commitment—refuses to work overtime or come in early
- Complains frequently in an attempt to upset/agitate other workers
- Displays malicious compliance through rigid or narrow behavior
- May be inattentive or disruptive in meetings
- Is prone to frequent angry outbursts or sullen behavior
- May try to steal or damage equipment

Trustworthiness

- Characteristic 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

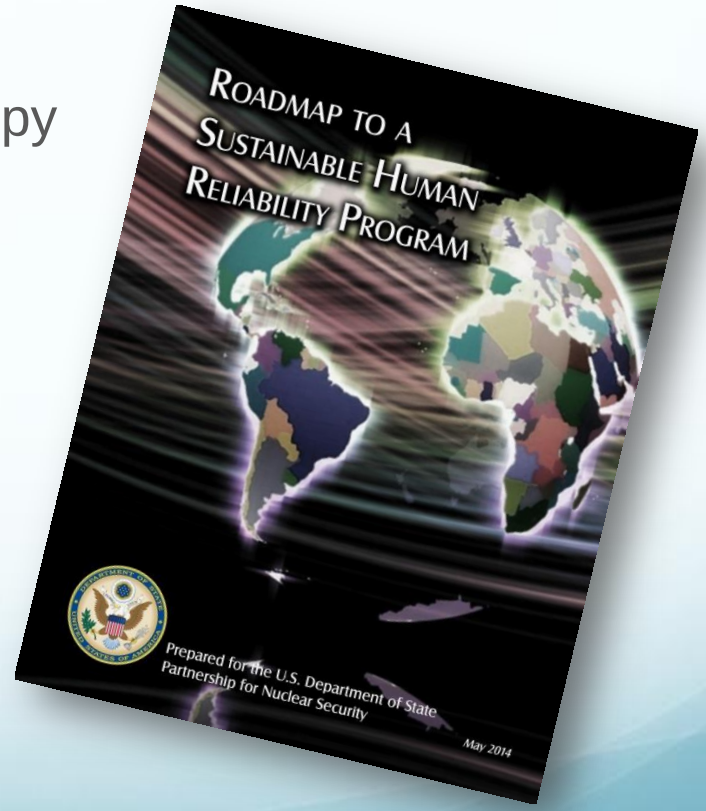
Fitness for Duty (FFD)/Human Reliability Programs (HRPs) are vital in establishing trustworthiness.

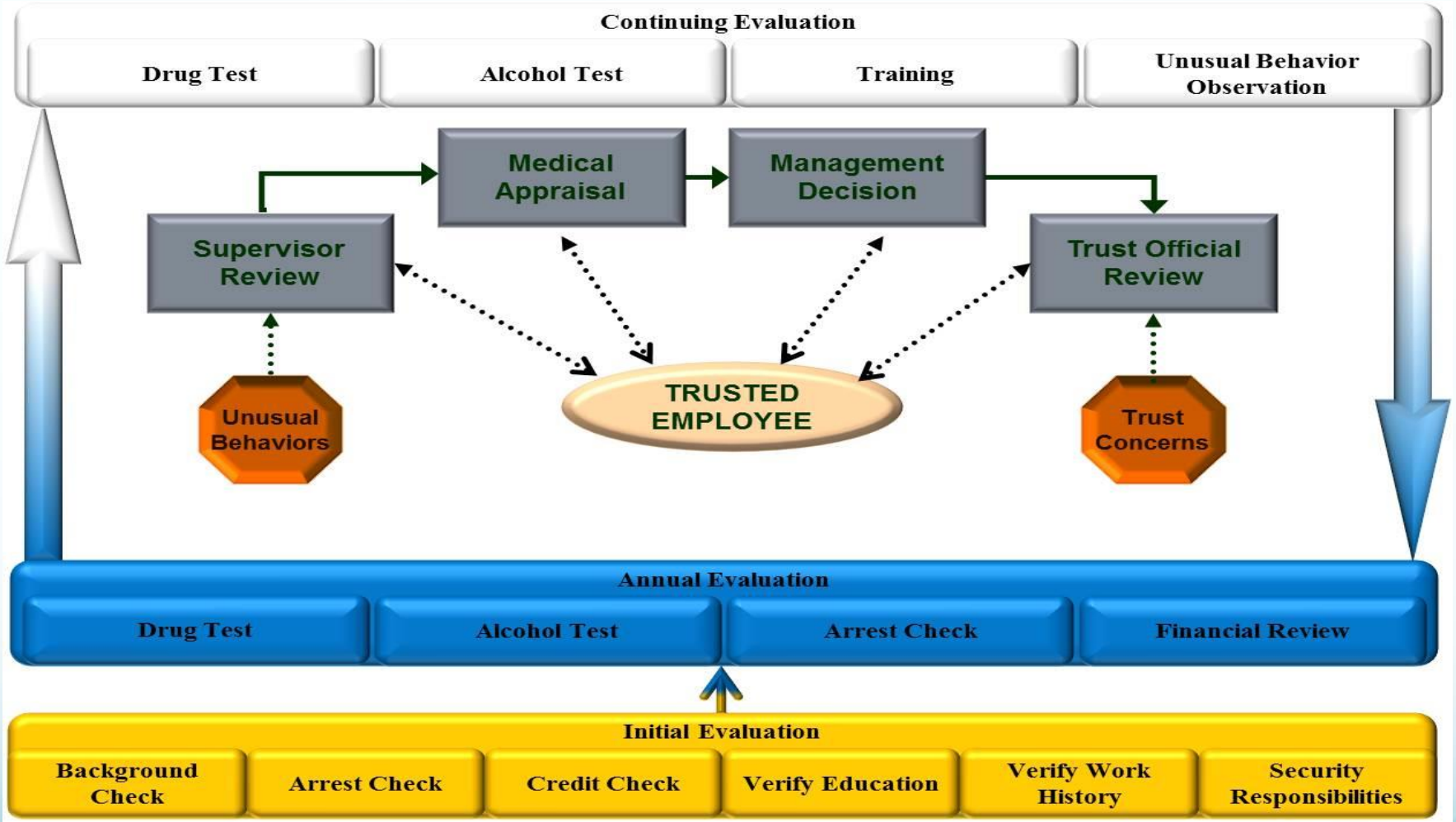
Preventive Measures

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

Mitigating Risks…

- Human Reliability Program (HRP)/Trustworthiness Program
- A security and safety reliability program designed to ensure that individuals who occupy positions with access to certain nuclear materials, facilities, and programs meet the highest standards of:
  - *reliability* (an individual's ability to adhere to security and safety rules and regulations),
  - *trustworthiness* (confidence in an individual based on his/her character) , and
  - *physical and mental suitability*…





Structured Trusted Employee Program (STEP*)

*** STEP is a generic form of a human reliability program created by the Oak Ridge National Laboratory (ORNL), Center for Human Reliability Safety and Security Studies (CHRS^3)**

Summary

- A Human Reliability Program/Trustworthiness Program is a Key Element to Ensuring a Strong Security and Safety Culture
- Important to Tailor the Program to Address Specific Cultural Norms, as well as an Organization/Facility
- International Community has Assistance Programs
- Must Come from the Top