Insider Mitigation Program for Nuclear Facilities

Joe Rivers
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Concept of the Insider Threat Is Not New

- *Quis custodiet ipsos custodes?* is a Latin phrase attributed to the Roman poet Juvenal from his *Satires* (Satire VI, lines 347–8), which is literally translated as "Who will guard the guards themselves?"

- While the concept of the insider threat is not new, an insider mitigation program must be adaptable to meet the challenges of an ever changing global threat environment.
Legislative & Regulatory Authority Important to Success of Programs

- Insider mitigation programs are more effective with standards that have a basis in law and are codified within a regulatory framework.
  - Establishes minimum requirements which can be inspected by an independent regulatory body to ensure processes and procedures within programs are functioning as intended.
  - Provides oversight and clarity for the facility owners and/or operators
  - Public confidence is enhanced with an independent regulator
  - Regulatory frameworks benefit from processes that provide a means to accommodate changes as necessary.
    - Rulemaking
    - Orders & Generic Communications
    - Guidance documents
Technology Component of Insider Mitigation Strategy

- Advances in technology adapt to the changing threat environment
  - Biometric identity verification tools
    - Hand geometry for access to protected areas
    - Retina scans for access to protected areas
    - Finger print scanning devices
  - Access to criminal history and other robust databases
  - State-of-the-art video surveillance
  - Explosive and metal detection devices
  - Detection devices for drug and alcohol use
Behavior Observation Program (BOP) Component

- Training on warning signs of aberrant or other behavior not conducive to trustworthiness and reliability
  - What to do if you observe aberrant behavior – see something, say something

- Processes in place to address aberrant behavior for the protection of the workers and the facility
  - Hot line
  - Employees assistance program
  - Regular supervisory reviews

- Fair and balanced application of a BOP
  - Consent forms
  - Appeal process
Objective of the NRC Insider Mitigation Program (IMP)

- Licensee oversight and monitoring of the initial and continuing trustworthiness and reliability of individuals by -
  - Minimizing the potential for an insider to directly or indirectly have an adverse impact on the licensee’s capability to prevent significant core damage or spent fuel sabotage.
  - Applies to all individuals following licensee’s initial unescorted access (UA) and unescorted access authorization (UAA) determination and/or certification of UA & UAA.
  - Applies to individuals who retain UA or UAA to the protected and vital areas.
Background of the IMP
At the NRC

• Information Notice (IN) 83-27 “Operational Response to Events Concerning Deliberate Acts Directed Against Plant Equipment”
  ➢ Provided licensees with information about program activities that licensees should consider for preparation and response to insider acts.

• IN 96-71 “Licensee Response to Indications of Tampering, Vandalism, or Malicious Mischief”
  ➢ Report known or unexplained plant conditions inconsistent with routine operations to NRC Operations Center within 1 hr. (10 CFR Part 73.71 – Reporting of Safeguards Events).

• Order EA-03-086 in 2003 required licensees to address the insider threat.
  ➢ Licensees upgraded their security plans in response to the Order.

• 10 CFR 73.55 (b)(9) – IMP – included in 2009 rulemaking
  ➢ Establishes the objective and minimum criteria for an IMP program.
Minimum Criteria of NRC’s IMP

- A security determination (UA & UAA) – Access Authorization (AA) program

- Initial, random, for cause, and post-event testing – Fitness for Duty (FFD) program

- Psychological assessments which may include a medical evaluation – AA & FFD programs

- Annual review by the immediate supervisor – AA program

- Periodic reinvestigation security determination – AA program
  - 3-year for critical group and 5-year all others
10 CFR 73.55(b)(9)(i) - Methodologies employed by licensees to implement an IMP must include elements from:
- The access authorization program described in 10 CFR Part 73.56.
- The fitness-for-duty program described in 10 CFR Part 26.
- The cyber security program described in 10 CFR Part 73.54.
- The physical protection program described in 10 CFR Part 73.55.

10 CFR 73.56 (f) & 10 CFR 26.33 - Behavior observation
- Behavior observation program includes elements from the IMP, AA, and FFD.
- Implementation by licensees is documented in the physical security plans that are a condition of their license.
Defense-In-Depth Strategy
(Continued)

• Guidance
  ➢ NRC Guidance
    ➢ RG 5.66 - Access Authorization Program for Nuclear Power Plants
    ➢ RG 5.77 - Insider Mitigation Program (currently under revision as DG-5044)
    ➢ RG 5.76 – Physical Protection
    ➢ RG 5.71 – Cyber
  
  ➢ Industry Guidance
    ➢ NEI 03-01 - Nuclear Power Plant Access Authorization Program
    ➢ NEI-03-04 - Guideline for Plant Access Training
    ➢ NEI-06-06 - Fitness-for-Duty Program Guidance for New Nuclear Power Plants
    ➢ NEI 03-12, Security Plan Template
Integration of Safety & Security Culture Components

- Background Investigation
  - Criminal History Check

- Insiders Mitigation Program
- Fitness for Duty Program
- Behavior Observation Program

NRC Inspection & Oversight
Examples of What to Look For In the IMP

• Tampering with equipment and/or systems
  – Valves out of proper position
  – Fluid levels (DORL 4 Belgium incident)
  – Workers in areas where they have no business

• Aberrant behavior or unexplained absences from work
  • Disgruntled employee
  • Radicalization or extremist views
    • Shariff Mobley incident in 2010

• Drug or alcohol abuse

• Affiliations with criminal elements
Warning Signs

Questionable Affiliations

- Security force member (Critical Group) at nuclear plant active member of outlaw motorcycle gang
  - Never returned to work after being interviewed about his affiliations by access authorization staff at the plant.
Disgruntle Employees With Unescorted Access

- November 1979 - Two employees working at Surry Nuclear power plant attempted to damage new fuel assemblies.
  - One employee had served aboard ship in the U.S. Navy’s nuclear program
  - Both employees had been granted unescorted access to a vital area in the plant
  - Both employees were convicted of intentional damage to a facility which furnishes electric power to the public and sentenced to two years in prison
  - The Nuclear Regulatory Commission issued information notice 79-12 to all nuclear power plants to share the information with the licensees that own and operate the plants.
$ Socio-Economic Impact $  

Tampering Incident  
At Belgian Nuclear Plant  

• August 2014 - Belgian energy company Electrabel reported that its Doel 4 nuclear reactor would stay offline until the end of year after major damage to its steam turbine was caused by a leak of 65,000 liters of oil.

  – Reuters news quoted a spokesman for GDG Suez which is the French parent company - “There was an intentional manipulation”.

  – Prosecutors familiar with the incident would not confirm that it was sabotage and they would not exclude sabotage either.

$ 37 Million to repair turbine in Germany

$ Loss of ~ 1 gigawatt of generating capacity to consumers during colder months & reduced company earnings for GDG Suez.
Offsite Behavior Matters

- NRC regulations require self-reporting of any criminal charges or arrests
- Two Senior Reactor Operators (Critical Group) arrested for aggravated car-jacking and fled to Venezuela
- Two Non-licensed Operators arrested for aggravated assault on and obstructing a peace officer at offsite party.
“Four Exelon employees arrested in the last 18 months”

“When Burhman was convicted in May of 2013, we questioned Exelon’s behavioral monitoring and screening program, which is designed to detect aberrant behaviors before they cause problems on-site. According to sources, Exelon has still not made changes to the behavioral observation program, despite the recent string of failures in the last 18 months”.

IMP Enhancements & Program Outreach

• Interaction and coordination with other Federal partners (FBI, DHS, TSC, DoD, and International counterparts).
  - (Advances in technology) Rap Back through FBI CJIS and ABIS through DoD.
  - SAVE system through Citizenship and Immigration Services

• Frequent interaction with industry and NEI
  - Participation in access/fitness-for-duty quarterly task force meetings

• On-going review and updates to regulatory guides and NRC endorsed NEI documents (industry standards).
  - RG 5.77 is being updated as part of the 5-year cycle
  - NUREG/CR-7183 – Published June 2014
Questions