Knowledge Security Awareness Training

Course Description

- This training seeks to deepen understanding of the definition and role of knowledge security in mitigating the threat to nuclear security and nonproliferation.
- The offering has tailored modules for managers as well as for scientists, technicians, and engineers (STEs) who work in nuclear proliferation-sensitive settings around the globe.
- Components of knowledge security are introduced and discussed in depth.
- Broad historical context and a breadth of case studies is given to contextualize knowledge security in a real-world setting, avoiding abstraction of the concept.
- Managers are provided with information about programs they can implement to support knowledge security at their site and for their staff.
- Course for STEs strengthens awareness of knowledge security as an element of responsible science.
- Curricula encourages engagement in peer-to-peer discussion and practical exercises regarding specific best practices.
- Course Duration: 2.5 days

Forms of Knowledge

Tangible (Explicit)

- Data in written or digital form
- Tangible information can be stolen if not properly secured

Intangible (Tacit)

- Know-how existing primarily in an expert's head
- Intangible knowledge may be extracted, sometimes through elicitation

Defining and discussing forms of knowledge allows participants to understand the relevance of best practices discussed during the course.

Knowledge Security

A system of practices to protect sensitive knowledge in any form (whether tangible or intangible) from being acquired or used by others for harmful purposes.

Key Components of Knowledge Security

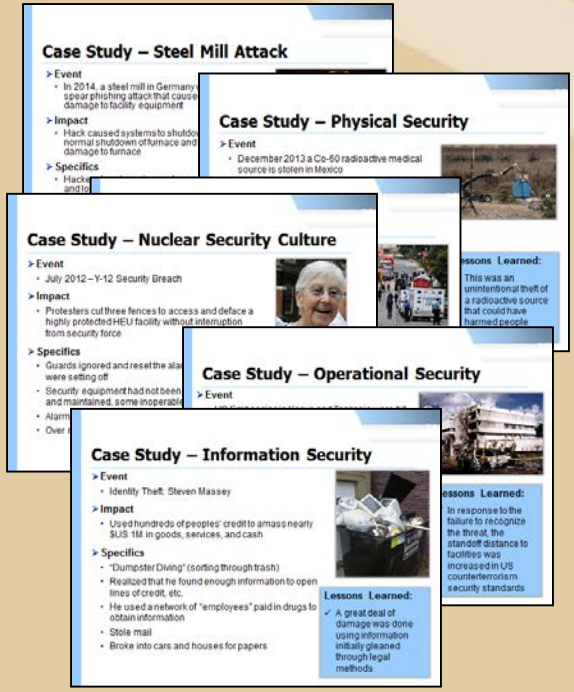
LA-UR-16-25604

Knowledge Security Awareness Training

Topical Areas Addressed

- Nuclear Knowledge Security Threat
  - The Spread of Nuclear Knowledge
  - Adversaries and Threats
- Nuclear Security and Nonproliferation Controls
  - Nuclear Security and Nonproliferation Framework
  - Introduction to the Concept of "Dual Use"
  - Strategic Trade Controls (Export controls)
  - Dual-Use Knowledge and Responsible Science
- Nuclear Knowledge Protection and Best Practices
  - Electronic Communications
  - Publications, Collaborations, Peer Review
  - Business Transactions and Patents
  - Site Visits, Tours, Workplace
  - Informal and Professional Settings
  - Information Release Pathways

Case Studies Highlight Currency and Relevance of Topical Areas



WMD Proliferation Requires Physical Items AND Knowledge

Not only the control of the physical items required for the production of WMD but also control of the knowledge of how to procure and use those items is critical to nonproliferation.

Material

Commodities

\+ Knowledge

Types of Knowledge Release

Active information extraction
•Theft
•Elicitation
Passive information gathering
(may occur through many avenues)
•Business, correspondence, publications, social networking
•Information harvesting

The Knowledge Security Awareness program addresses methods to identify and counter the full spectrum of this threat.

Write → Review → Revise → Release

Example: Best Practice for Information Release

LA-UR-16-25604