

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

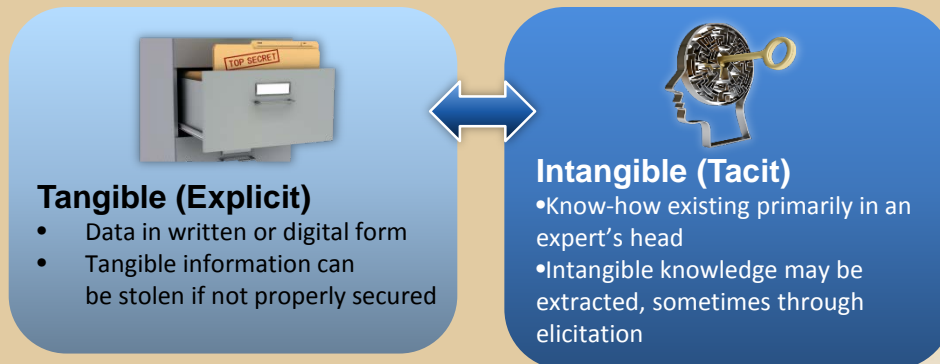
Knowledge Security

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



Forms of Knowledge



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

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

Case Study – Steel Mill Attack

- > Event
 - In 2014, a steel mill in Germany suffered a cyber attack that caused damage to facility equipment.
- > Impact
 - Hack caused systems to shut down, normal shutdown of furnace and damage to furnace.
- > Specifics
 - Hackers used social engineering and insider access.

Case Study – Physical Security

- > Event
 - December 2013 a Co-60 radioactive medical source is stolen in Mexico.

Case Study – Nuclear Security Culture

- > Event
 - July 2012 – Y-12 Security Breach
- > Impact
 - Protesters cut fence to access and deface a highly protected HEU facility without interruption from security force.
- > Specifics
 - Guards ignored and reset the alarm when they were setting off.
 - Security equipment had not been tested and maintained, some inoperable.
 - Alarm system was not working.
 - Over 100 people entered the facility.

Case Study – Operational Security

- > Event
 - Identity Theft: Steven Massey
- > Impact
 - Used hundreds of peoples' credit to amass nearly \$100,000 in goods, services, and cash.
- > Specifics
 - “Dumpster Diving” (sorting through trash)
 - Realized that he found enough information to open lines of credit, etc.
 - He used a network of “employees” paid in drugs to obtain information.
 - Stole mail.
 - Broke into cars and houses for papers.

Case Study – Information Security

- > Event
 - Identity Theft: Steven Massey
- > Impact
 - Used hundreds of peoples' credit to amass nearly \$100,000 in goods, services, and cash.
- > Specifics
 - “Dumpster Diving” (sorting through trash)
 - Realized that he found enough information to open lines of credit, etc.
 - He used a network of “employees” paid in drugs to obtain information.
 - Stole mail.
 - Broke into cars and houses for papers.

Lessons Learned:

- This was an unintentional theft of a radioactive source that could have harmed people.
- In response to the failure to recognize the threat, the standoff distance to facilities was increased in US counterterrorism security standards.
- A great deal of damage was done using information initially gleaned through legal methods.

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