

Nuclear Security for Scientists, Technicians and Engineers

CONTENTS

The WINS Academy Elective on Nuclear Security for Scientists, Technicians and Engineers addresses the role of scientists and engineers in the nuclear security programme, WINS refers to the full range of scientific and engineering disciplines involved in nuclear materials management. A small sample of common disciplines includes:

- Civil Engineer
- Operations Personnel
- Mechanical Engineer
- Design Engineer
- Process Engineer
- Electrical Engineer
- Safety Case Engineer
- Controls and Instrumentation Engineer/Technician
- Research and Development Engineer/Scientist
- Operations Researcher
- Laboratory Technician
- Information Technology Specialist

The goal of the module is to help participants understand the fundamental issues associated with nuclear security in their organisation. The module discusses the potential security threats their organisation faces, the major stakeholders with responsibilities for nuclear security, how the human element and security culture affect security, and the numerous ways in which their jobs and responsibilities intersect with and contribute to security. The module also discusses how to work and communicate with their fellow professionals in the Security Department to achieve mutual goals.

By the end of the module, participants will understand:

- The threats their organisation faces, including those from insiders, and what they can do to help mitigate them.
- Who the major security stakeholders are and what they are responsible for.
- Their personal accountabilities and responsibilities for security.
- The importance of the human element—including security culture and human reliability—in maintaining security.
- The importance of integrating security culture with safety culture.
- The numerous ways in which their work intersects with security and specific steps they can take to increase security where they work.
- The roles and responsibilities of their organisation's security professionals—including the knowledge, skills and training they typically receive.
- How to work and communicate with security professionals to achieve mutual goals.



OUTLINE

UNIT 1: UNDERSTANDING THE THREAT

- 1.1 Threats to Nuclear and Other Radioactive Materials
- 1.2 Threats from Unwitting Actors and Criminals
- 1.3 Threats from Non-State Actors
- 1.4 Cybersecurity

UNIT 2: UNDERSTANDING STAKEHOLDER RESPONSIBILITIES

- 2.1 The IAEA
- 2.2 The State and the National Security Regime
- 2.3 The Regulator and the Design Basis Threat
- 2.4 The Licensee and the Security Programme

UNIT 3: UNDERSTANDING THE HUMAN FACTOR

- 3.1 Insider Threat
- 3.2 Security Culture
- 3.3 Human Reliability
- 3.4 Whistleblowing

UNIT 4: UNDERSTANDING THE INTERSECTIONS

- 4.1 Security by Design
- 4.2 Material Control and Materials Accountancy
- 4.3 IT and IC Systems
- 4.4 Modelling & Simulation
- 4.5 Security Equipment Maintenance

UNIT 5: BRIDGING THE GAP

- 5.1 The Changing Role of the Security Professional
- 5.2 Why and How to Integrate
- 5.3 Security Competence
- 5.4 Cross-Functional Communication
- 5.5 Protecting Sensitive Information
- 5.6 Security Liaison Programme