Strengthening Radioactive Source Security:
Assessing and Establishing an Effective Security Culture

World Institute for Nuclear Security

INTRODUCTION

Radioactive materials play an important role in medical, research and commercial facilities. Many of these facilities are open to the public and cannot be locked down like other facilities that use similar materials. These public facilities implement security systems to protect the radioactive materials; however, a facility's *security culture* can make or break the security system.

Security culture is a term used to describe the beliefs and behaviours people exhibit in relation to security. It is one of the most challenging aspects—and underlying vulnerabilities—in the practical implementation of security. This workshop will discuss the role of security culture in a facility's security system and why a strong security culture is so important for protecting radioactive materials. The workshop will also explore how disposing of radioactive materials or using alternative non-radioisotopic technologies will impact a facility's security culture.

Chicago, Illinois

6–7 March 2019

WORKSHOP OBJECTIVES

- To understand the threat to radioactive materials, including the potential motivations of adversary groups and individuals;

- To appreciate the particular threat posed by insiders and how to mitigate the threat;

- To develop a common understanding of what an effective security culture looks like and how it can mitigate threats;

- To identify the respective roles and responsibilities of licensees and regulators in establishing an effective and sustainable security culture;

- To review methodologies for measuring the level of security awareness and good culture in an organisation, assessing the results and implementing change;

- To identify possible incentives to encourage staff to adopt security best practices as a normal part of their daily work lives;

- To identify training opportunities to improve the competency of staff;

- To explore the use of peer review as a method for an independent assessment of security culture and identifying areas for improvements; and

- To explore permanent threat reduction approaches through the adoption of alternative technologies.

Strengthening Radioactive Source Security:
Assessing and Establishing an Effective Security Culture

TARGETED AUDIENCE

- **Representatives from organisations that use radioactive sources (medical, academic and industry);**

- **Representatives from radioactive source producers, device manufacturers and service (maintenance) companies;**

- **Representatives from regulatory authorities; and Representatives from professional associations and international organisations.**

FACILITATED WORKSHOP

Participation will be limited, so please let us know as soon as possible if you wish to attend this event. Attendees will be expected to meet their own costs for travel and accommodation, but all the workshop related costs will be met by the organisers. No registration fee is required.

In line with WINS' innovative approach to Best Practice Workshops, this event will be interactive and professionally facilitated. The workshop will be built around a number of presentations, group discussions and case studies to further explore the topic.

An Instant Electronic Voting system will be used to allow participants to anonymously vote using keypads, providing their views on questions put to the workshop participants. Discussions will be subject to "Chatham House" rules (what was said can be reported but not attributed).

The discussions will be supported by the following publications:

WINS International Best Practice Guides 1.4 on *Nuclear Security Culture and 5.1 on Security of High Activity Radioactive Sources*

WINS Performance and Evaluation Series: *Peer Review Guidelines to Assess the Security of Radioactive Sources Used in Medical Applications*

WINS Special Publication: *Considerations for the Adoption of Alternative Technologies to Replace Radioactive Sources*

REGISTRATION INFORMATION:
Bettina Lock
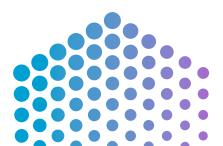World Institute for Nuclear Security
bettina.lock@wins.org

Strengthening Radioactive Source Security:
Assessing and Establishing an Effective Security Culture

DAY 1

SESSION I:
FOUNDATIONS OF SECURITY CULTURE

- Review the various threats to radioactive materials and the potential motivations of adversaries.

- Explore the particular threat posed by insiders.

- Define security culture and why it is so important for the effectiveness of a security programme.

- Review the factors influencing the culture of an organisation, including how we can influence beliefs, values, understandings and behaviours of people.

- Review examples of good and bad security practices; identify attitudes and behaviours contributing to such practices.

- Explore the difference between security culture and security compliance and why this is key to effective security.

SESSION II:
METHODOLOGIES FOR ASSESSING SECURITY CULTURE

- Review methodologies for measuring the level of security awareness and culture in an organisation. Understand how to assess the results.

- Explore the use of peer review as a method for an independent assessment of security culture and identifying areas for improvement.

- Explore the development of a security culture self-assessment plan for end-users.

- Explore metrics for continuously evaluating the level of security culture. How do we demonstrate we have achieved our objectives?

DAY 2

SESSION III:
ESTABLISHING AN EFFECTIVE SECURITY CULTURE

- Identify the respective roles and responsibilities of the various radioactive source stakeholders (e.g. end-users and regulators) in establishing a robust and sustainable security culture.

- Explore how we can integrate security culture into an overarching and comprehensive organisation culture integrating security, safety and operations.

- Understand how we progress from awareness to culture. How can we transform concepts into actions?

- Identify the usual challenges and possible solutions to overcome them. Define steps and good practices leading to a strong security culture.

- Identify possible incentives to encourage staff to adhere to security practices as a normal part of their daily duties.

- Identity training approaches to improve the competency of staff.

- Identify lessons learned from other disciplines and sectors.

SESSION IV:
CONSIDERATIONS FOR THE ADOPTION OF ALTERNATIVE TECHNOLOGIES

- Discuss alternative technologies and their impact on an organisation's security culture;

- Review of the key considerations for adopting alternative technologies;

- Review of available alternative technologies;

- Understand the challenges for adopting alternative technologies;

- Understand support available via the Cesium Irradiator Replacement Project;

- Review of good practices for planning and implementing the transition to alternative technologies.