# Online Workshop: Mitigating Internal Threats for Categories 2 and 3 Radioactive Sources

**23 April 2024**

**Draft Report for comments**

# Background

An incident resulting from the inadequate or negligent management of radioactive sources would likely affect normal business operations and the reputation of an organisation. Ultimately, financial losses (loss of the use of facilities, lost business, lost wages, recovery costs, replacement costs, clean-up costs, and medical costs for employees and members of the public) and loss of reputation could constitute a serious crisis for the organisation.

As the threat from terrorism has grown in the last decades, the awareness that radioactive sources could potentially pose a serious security risk has also grown. As a result, States and regulatory bodies have instituted new regulations and end users have developed and implemented security arrangements to mitigate this risk. Radioactive sources can be attractive to both external adversaries and insiders who wish to cause harm, in particular by the theft of the radioactive sources for further malicious use (e.g. in a “dirty bomb” or through deliberate exposure to people).

Radioactive sources have certain inherent characteristics that may increase their attractiveness for use in malicious acts by adversaries. Thousands of sources are used for teletherapy and brachytherapy in the medical sector, over 10,000 industrial sources are being supplied annually for radiography, and more than 300 gamma irradiators are in operation.

Groups and individuals with malicious intent may try to use radioactive sources for achieving their nefarious objectives. These adversaries can either come from outside the organisation (outsiders or external threats) or from within it (insiders or insider threats). Insiders are individuals (such as employees, contractors and suppliers) with have authorised access to a facility, transport operation, sensitive information, or computer and communications system who use their trusted position in support of a malicious act.

Building on its series of events and activities supporting the development of robust and comprehensive arrangements for the security of all radioactive sources worldwide, WINS organised a workshop focusing on mitigating internal threats to Categories 2 and 3 radioactive sources.

Categories 2 and 3 radioactive sources are essential for many medical, industrial, and research applications. Category 2 sources are typically used in industrial gamma radiography, high- and medium-dose rate brachytherapy, and radiography. Category 3 sources are typically used in fixed industrial gauges such as level gauges, dredger gauges, conveyor gauges, spinning pipe gauges, and well-logging gauges. If not properly managed, such sources could cause permanent injury to a person who handled them or was otherwise in contact with them for hours or even few minutes in the case of certain Category 2 sources.

While Category 1 sources are often placed in a heavy, difficult-to-transport devices, many Categories 2 or 3 sources are contained in portable containers or even in capsules that are so small they could be hidden in a pocket or suitcase. Some Categories 2 or 3 radioactive sources are also frequently transported as part of their use and might be vulnerable to theft during transport or when located outside of their home base.

Insider threats are particularly dangerous because they can use their access, authority and knowledge to bypass dedicated physical protection, safety measures and operating procedures. They also might have more time to select targets, identify vulnerabilities and plan and carry out a malicious act. For example, they could tamper with security equipment to reduce the risk of detection or falsify inventory records to steal small amounts of radioactive material, undetected, over time.

# Objectives of the Workshop

The overall objective of this workshop was to exchange experience and lessons learned by various stakeholders when developing and implementing security measures for Categories 2 and 3 radioactive sources and trying to address the internal threats to these sources. In particular, this workshop was an opportunity to:

**Identify practices using Categories 2 and 3 radioactive sources –** Explore how their prevalence and how their particular characteristics can influence their security needs.

**Explore specific threats –** Delve into the unique challenges and risks associated with Categories 2 and 3 radioactive sources, providing a nuanced understanding of potential internal threats within these contexts.

**Share best operational security practices –** Offer a platform for end-users to share experiences, case studies, and best practices in mitigating internal threats related to Categories 2 and 3 radioactive sources.

**Share examples of theft or loss of Categories 2 and 3 radioactive sources –** Learn from these real-life experiences and suggest improvements to current practices.

**Understand the role of regulations –** Discuss how regulations can and should include requirements to mitigate insider threats.

**Highlight the importance of a robust security culture** **–** Better understand how organisational culture matters and the importance of engaging all staff in security matters.

**Support stakeholder engagement** **–** Facilitate collaboration and knowledge-sharing among diverse stakeholders, including regulatory bodies, industry professionals, and government officials, fostering a cohesive global approach to security.

# Event Process

More than 280 participants attended the workshop, which was conducted online via Zoom on 23 April 2024 from 14:00 to 17:30, Vienna time. It was held in English.

The workshop was divided into two sessions with a 15-minute break between sessions.

In line with WINS` approach to international workshops, this online event was interactive and professionally facilitated.

The workshop was built around a number of presentations from invited speakers representing the various stakeholders involved in radiological security matters (end users, regulatory bodies and law enforcement agencies), as well as case studies and structured discussions that enabled participants to further explore the topic and share their experience and lesson learned.

An online voting system also allowed participants to provide their views on questions put to the workshop by anonymously registering their opinions.

The workshop was recorded, and the recordings will be made available in the Knowledge Centre of the WINS website.

## Opening Session

Anastasiia Nechytailo, WINS Project Lead, welcomed the participants and made the opening remarks on the importance of the topic and objectives of the workshop. Helene Jewell, Workshop Facilitator, then reviewed the agenda and practicalities with the participants.

**Atkins Case Study**

Two speakers outlined the case of Jared Atkins, one of the few documented incidents of an insider stealing radioactive sources with malicious intent.

* *Operator perspective*, John Lyons (Western Technologies, USA)
* L*aw-enforcement perspective,* (Justin Walker, SummitET, USA)

Mr Walker began by explaining the basic facts of the incident, which took place in April 2019. Jared Atkins, an employee of Western Technologies, used his access and knowledge to steal three radiography cameras with the intention of developing a RED and start a shooter event.

Mr Lyons spoke about the company’s perspective on the incident. He noted that Mr Atkins had no criminal background and had received positive employee reviews. There was some knowledge of issues in his personal life, but they were not considered cause for concern. The first responders initially did not understand the seriousness of the Category 2 radioactive sources that had been stolen. Mr Lyons also spoke about the company’s security modifications following the incident.

Mr Walker highlighted the importance of relationships with the local first responders and ensuring they have sufficient training about radioactive sources and know their locations in the city. He also noted the value of multi-agency coordination to ensure the rapid diffusion of information as well as pre-event planning. He also pointed out that there had been signs of the problems Mr Atkins was experiencing and insider threats could potentially be detected ahead of incidents.

**Discussion**

Following the speakers’ presentation, the participants discussed the lessons learned they could draw from the incident.

They noted the importance of proactivity by management as incidents may occur unexpectedly. They also pointed out the usefulness of coordination between different departments, and the danger that siloing information can pose. They suggested a holistic approach to security combining physical, procedural and personnel security, the creation of contingency plans for various scenarios, and developing security culture within organisations.

### Session 1: Understanding the Risk

**Key issues:**

* What applications use Categories 2 and 3 radioactive sources?
* What are the potential consequences of malicious use of these sources? Which of their characteristics impact security needs and implementation?
* What are the threats to Categories 2 and 3 radioactive sources? What insider threat scenarios should we be prepared for?

**Presentation** on *Industrial, Medical and Research Applications Using Cat 2 and 3 Radioactive Sources*, Agustin Espejo Mancillas (Tecnofísica Radiológica S.C., Mexico)

Agustin Espejo spoke about the industrial applications of Categories 2 and 3 sources. He briefly explained how the category is calculated before detailing the characteristics of devices in the second and third categories. He then went over several examples of Categories 2 and 3 sources used in industry, their applications and their attributes.

**Discussion**

After the presentation, the participants discussed the characteristics of Categories 2 and 3 radioactive sources that impact security matters. Participants noted that these devices are designed to be transported easily and used by multiple people, and sources are most vulnerable during transport. They also pointed out that they are highly reactive and their use can be difficult to monitor. Their location in publicly accessible places such as hospitals and the lack of security culture, awareness or consistent security measures at these organisations were also mentioned as important factors. It was also noted that employees’ training on these sources often emphasises safety rather than security. Specifically, it was suggested that manufacturers could expand their focus on safety features to physical security features.

**Presentation** on *Internal Threats and Their Relevance to Categories 2 and 3 Radioactive Sources*, Stacy Snook (Protective Security Lab, UK)

Stacy Snook introduced various definitions of insiders and the core attributes that insiders have. She also addressed the key variables to categorising insiders before outlining the most common motivations of insiders. She discussed the known trends regarding insiders’ traits, noting that research was limited and outdated, and described potential protective factors within organisations.

**Discussion**

Following the presentation, the participants discussed credible internal threat scenarios to Categories 2 and 3 radioactive sources. Some of the scenarios mentioned included intention to harm a colleague or boss, deliberate or inadvertent release of sensitive information (including on social media or during communication with civil society), and collaboration between insiders. It was also noted that insiders could exploit weaknesses in measures or regulations at an organisation. Sabotage and theft were also highlighted as potential insider incidents.

## Session 2: Mitigating the Risk

**Key issues:**

* What are usual regulatory security requirements for Categories 2 and 3 radioactive sources?
* What can we learn from those implementing insider threat mitigation measures for Categories 2 and 3 radioactive sources?
* How do you demonstrate that implemented security arrangements are sufficient to mitigate the insider threats to Categories 2 and 3 radioactive sources?

**Presentation** on *Mitigating Security Risks of Category 2 & 3 Sources in Medical Research Facility University Health Network (UHN)*, Raina Park (UHN, Canada)

Raina Park opened her presentation by introducing the University Health Network and the types of sources the organisation uses. She then described the regulator’s requirements for the security of these sources and how they apply to technical and administrative security measures. Next, she spoke about the trends among reportable incidents that had occurred at the organisation and the UHN’s process for implementing improvements in response to challenges.

**Discussion**

In light of the presentation, the participants discussed best practices for designing and implementing effective security measures for Categories 2 and 3 radioactive sources against insider threats. The paramountcy of security culture and awareness about the importance of security was highlighted, as well as designing security systems to cover delay, deter, detect and deny. They noted that cameras were helpful but also had shortcomings. Alternative technologies were recommended to eliminate the risk. Additionally, participants spoke about encouraging employees to engage with security measures regularly, escalate concerns, and observe potential risk signs for insider threats.

**Presentation** on *The Ukrainian Experience with Radioactive Source Security in War Time*, Oleksii Petrov (SSE Central Enterprise for RW Management)

Oleksii Petrov spoke about the challenges the SSE Central Enterprise for RW Management has faced during the war and their strategies for mitigating them. After introducing the organisation and its work, Mr Petrov discussed some of the particular difficulties the organisation had faced: increased gamma radiation measured in exclusion zone, damage to and theft of equipment and facilities, and suspension of licences. He noted that in response, the physical protection system and procedures had been updated, security checks on employees conducted, cybersecurity measures enhanced, and specific training for staff implemented. He highlighted the importance of adhering to and continuously improving technological procedures as well as robust physical protection systems.

**Presentation** on*Demonstrating Readiness to Mitigate the Insider Threat*, Ruth Asaba (Atomic Energy Council, Uganda)

Ruth Asaba explained that insider threat mitigation programmes should be assessed in terms of the available technology installed, use of procedures at workplaces, the level of staff training and a vulnerability assessment. She continued to explain the evaluation of security arrangements in terms of the fundamental factors of detection, delay and response. Ms Asaba then outlined the signs of a healthy insider threat mitigation culture and signs of potential issues. She concluded by outlining the role of regulation in insider threat mitigation through promotino of nuclear security culture, enforcement regarding procedures and training programmes, ensuring sufficient management systems and verifying the roles and responsibilities of workers.

**Discussion**

In view of the presentation, the participants discussed best practices for assessing the effectiveness of insider threat mitigation arrangements. Participants spoke about the importance of penetration testing as well as testing through scenario-based exercises, drills and simulations. They also highlighted the importance of a risk assessment and incident reporting, as well as feedback from staff and KPIs related to their performance. Evaluation of training programmes was noted as an important part of evaluation, and peer review was also mentioned as an effective evaluation technique.

## Closing Session

Ms Jewell summarised the event and Ms Nechytailo closed the workshop, thanking the presenters for their contributions and the participants for the discussion. In responses to a poll about their assessment of the workshop, 98% of the participants responded they were either satisfied or very satisfied.