World Institute for Nuclear Security

Round Table on the Role of Standards for Strengthening the Security of Radioactive Sources used in Medical Applications

Vienna, Austria. 22- 23 January 2019

REPORT

BACKGROUND

In the last 10 years, many States have markedly increased the security of their radioactive sources. Two important initiatives have strongly contributed to this progress. The first is the Code of Conduct for the Safety and Security of Radioactive Sources that was published by the International Atomic Energy Agency (IAEA) in January 2004. The second is the four Nuclear Security Summits that were held between 2010 and 2016. These summits brought heads of state together from approximately 60 countries to find ways to strengthen global nuclear security and reduce the continuing threat of nuclear terrorism.

Although such initiatives have greatly increased radioactive source security in many States, much remains to be accomplished. In particular, the coordination and integration of various efforts and a stronger involvement of industry and end users. This need is especially true in the medical sector, which routinely uses radioactive sources to diagnose and treat illness. To ensure the wellbeing of both patients and staff, medical facilities around the world take great care to train their staff in the safety procedures that must be followed when using radioactive sources and related technologies. In contrast, however, they may not pay comparable attention to ensuring that the sources remain secure from individuals who desire to steal or sabotage them.

Hospitals, cancer centres, and other medical facilities are necessarily public places. Consequently, it is possible that an individual with malicious intent could gain access to a location where the organisation's radioactive sources are kept, especially if rigorous access controls are lacking. One of the challenges is that devices containing radioactive sources were designed according to criteria related to safety and radiation protection, not to security. It has been shown that a determined adversary with the necessary hand tools could gain access to the sources contained in certain blood irradiator or radiotherapy devices within minutes and remove them from the premises in a portable shielded container with minimal personal exposure to radiation.

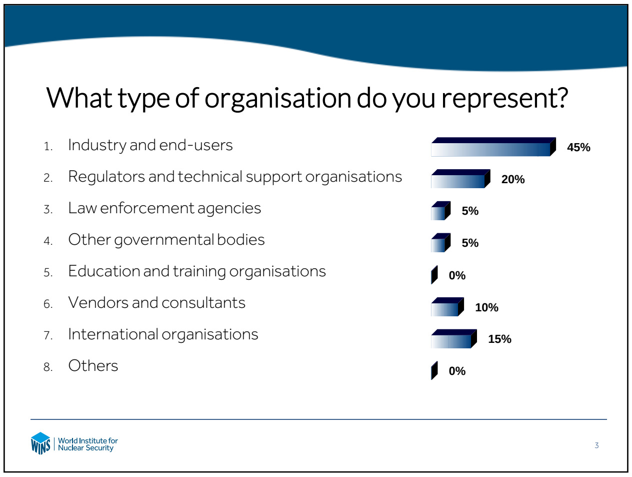
Another important consideration is that few security incidents involving radioactive sources have taken place. As a result, senior management often lack interest in and commitment to radioactive source security. This hampers the development of a robust security culture and leads to minimum implementation of regulatory requirements for the security of radioactive sources. Finally, many medical facilities have failed to ensure that the individuals who are accountable for radioactive source security have the skills and competences necessary to understand their roles and responsibilities for radiological security and can successfully contribute to an effective security programme.

OBJECTIVES OF THE ROUND TABLE

The key objectives of this two-day round table were to discuss the current status of the security arrangements for high activity radioactive sources used in medical applications, identify possible gaps, and explore how innovative approaches could help reduce remaining security vulnerabilities. The event was designed around three main topics:

- Corporate approach to radioactive source security (governance arrangements);
- Security-by-design of devices and associated facilities;
- Competences of individuals with accountabilities for the security of radioactive sources.

Twenty-five experts from eight countries and two international organisations attended the round table. They represented the main stakeholders involved in the security of radioactive sources used in medical applications (medical end users, regulators, device manufacturers, international support programmes and security professionals). Participants were expected to have open discussions and express their own perspectives and ideas for innovative approaches that could help strengthen radioactive source security. They were also expected to brainstorm on the topic and use their different experiences and backgrounds to identify good practices they had observed or experienced and to explore how these could be transferred to radioactive source security.



What type of organisation do you represent?

1.	Industry and end-users	45%
2.	Regulators and technical support organisations	20%
3.	Law enforcement agencies	5%
4.	Other governmental bodies	5%
5.	Education and training organisations	0%
6.	Vendors and consultants	10%
7.	International organisations	15%
8.	Others	0%

ROUND TABLE PROGRAMME

DAY 1: TUESDAY 22 JANUARY 2019

OPENING SESSION

Mr Pierre Legoux, WINS Head of Programmes, welcomed the participants on behalf of WINS, detailed the objectives of the round table, and provided a preliminary overview of the agenda. Mr Legoux also displayed and commented on the most relevant results from the pre-event survey.

Participants' expectations

Participants were asked to introduce themselves at their tables and discuss their expectations coming into this event. Some examples include:

- Review the current status of medical source security and explore options to strengthen current arrangements when needed. Identify an approach to security that is both effective and suitable for the medical environment. Discuss how to develop consistent requirements and practices worldwide.

- Provide a manufacturer perspective. Obtain important/general information on security issues and potential ideas for further development.
- Learn more about the possible use of standards to strengthen radiological security. Learn how feasible such standards might be and the direction in which industry and regulators might go. Discuss whether or not they should start working on an international standard now.
- Network, share experiences, benchmark and update knowledge.
- Participate in interesting, expert-level discussions! Get inspired!

Developing a common understanding and terminology

Participants then discussed their understanding of the word “standard” and how standards can be used to strengthen the security of radioactive sources, especially those used for medical applications. During the discussions, participants mentioned that no standard related to the security of sources currently exists and that establishing such a standard could provide an opportunity to benchmark security practices and measure their effectiveness. Participants agreed that standards already exist in other highly regulated environments and that standards focused either on management or technical areas should be considered. They saw standards as a way to demonstrate performance beyond simple compliance with regulations and to harmonise practices worldwide regardless of the maturity level of regulations in a particular State.

SESSION 1: SECURITY OF RADIOACTIVE SOURCES USED IN MEDICAL APPLICATIONS – A COMPREHENSIVE REVIEW

Session 1 reviewed common practices for ensuring the security of radioactive sources used in the medical sector. It also featured a gap assessment that encouraged participants to identify areas where improvement might still be needed.

Mr Bryan Warren, Atrium Health (USA) delivered a presentation on *Challenges and Opportunities for the Security of Radioactive Sources in Medical Applications*. First, he described the unique characteristics and security challenges of health care facilities (HCFs) and their importance in our societies. He also highlighted how attractive they might be to terrorists and criminals. After listing the radioactive sources that are commonly used in medical facilities, Mr Warren explained the security requirements for HCFs in the US, provided examples of poor security practices, and described some of the improvement measures put in place to improve the situation. Mr Warren then shared some information on US DOE support programmes available to US licensees and highlighted the need to consolidate and disseminate best security practices to achieve effective and sustainable security at HCFS. In his conclusion, he emphasised the importance of taking radiological security seriously and encouraged collective and proactive efforts to convince decision makers at HCFs to invest necessary resources in security matters.

During the follow-up discussions, participants were asked to share their opinions on what had been achieved in terms of the security of radioactive sources used in medical applications and what still requires further attention. Some of the findings were:

- ❑ Regulations usually exist but have reached different levels of maturity. There is a need for harmonising them (consistent requirements to support consistent security arrangements) in the world and to encourage different regulators (safety, security, medical…) to work better together.
- ❑ Overall, participants had mixed feelings about achievements. A lot of room for improvement exists. Two key issues are ensuring a better engagement of senior management in the topic and involving conventional security staff in security programmes for radioactive sources.
- ❑ Competence of the staff is an issue. Security culture amongst the staff is often poor because they lack belief in the threat. Effective and sustainable security will require raising security awareness and culture.
- ❑ Another security risk associated with radioactive sources and radiation devices is the voluntary modification of the settings of the treatment equipment. Such issues should be addressed in the overall risk management framework.

SESSION 2: STRENGTHENING THE GOVERNANCE ARRANGEMENTS FOR THE SECURITY OF RADIOACTIVE SOURCES USED IN MEDICAL APPLICATIONS

Session 2 reviewed the key elements of a security programme for radioactive sources used in medical applications and identified the responsibilities of the main internal and external stakeholders. It also discussed how to demonstrate that governance arrangements for security are adequate and the role of regulatory inspections and other mechanisms to support this demonstration. Finally, the session offered an opportunity to explore options for increasing the interest in and commitment of senior management to radiological security matters.

Mr Jim Thurston from the Royal Marsden Hospital (UK) opened the session with a presentation titled the *Role of Peer Review in Assessing the Security of Radioactive Sources used in Medical Applications*. He began by reminding participants about the definition and purpose of peer reviews and how they are usually used in the medical sector in the UK. He then presented lessons learned from two pilot peer reviews for the security of radioactive sources conducted at medical facilities in the UK in 2018. Mr Thurston concluded his presentation by highlighting the feasibility and potential added value of such peer reviews, especially as a continuous improvement tool, and the need for a lead organisation to establish and coordinate the process.

Ms Jodi Ploquin from the Alberta Medical Services (Canada) then offered a presentation on *Quality Standards and Accreditation Mechanisms*. After providing a definition of accreditation and detailing the steps leading to mature safety and security cultures, she described the role of the Health Standards Organization (HSO), which is an accreditation body in Canada that develops quality standards for the medical sector. In particular, she discussed Required Organizational Practices (ROPs), which are evidence-based practices that address the key areas of medical practice. She also highlighted the similarity of selected ROPs, such as the one for Narcotics Safety, with the topic of the round table. Finally, Ms Ploquin compared the respective scope and mechanisms of the licensing process, which is a required process, with the accreditation approach, which is followed on a voluntary basis.

Mr Legoux explained that WINS had conducted a study related to the development of a quality standard for the security of radioactive sources and of an associated accreditation mechanism. He said that the study found it was feasible to develop a quality standard within 18 months and offer it to medical practitioners. The major questions in this regard are how to fund the development of such a standard, the willingness of health care facilities to participate in it, and facilities' readiness to pay for accreditation services.

As a follow-up discussion, participants were asked to share their experiences in peer review and accreditation practices, explore the relevance of peer review and accreditation to radiological security, and discuss how they could strengthen governance arrangements.

Participants agreed that in most cases, roles and responsibilities for radioactive source security are clearly established and that Radiation Safety Officers, or individuals in similar positions, usually coordinate security practices and drive the momentum. On the other hand, participants noted that it might be risky to rely too much on one person because it could lead to a lack of resilience if the person leaves the position.

Participants agreed that senior managers need to better engage in security matters and that efforts initiated by field practitioners (bottom-up approach) should be completed and coordinated at the highest level of the organisation (top-down approach). When addressing senior managers, it is essential to speak their language and develop a business case for security. Experience suggests that involving senior clinicians (who may be relatively accessible), may provide a channel to the ear of chief officers that RSOs cannot achieve alone.

Discussions also highlighted the fact that peer reviews do exist in all sectors and that they should be implemented in our area. Participants clearly saw peer reviews as a way to encourage and demonstrate excellence, whereas the primary purpose of audits and inspections is to ensure compliance with set requirements. However, multiple challenges must be resolved to establish a systematic regime of peer reviews (e.g. cost, availability of peers, a leading organization, etc.).

Participants finally agreed that accreditation mechanisms are common practices in the medical sector and that further work should be conducted to develop a way forward. They concluded that accreditation would bring security to the attention of senior managers.

SESSION 3: STRENGTHENING THE SECURITY-BY-DESIGN OF DEVICES AND ASSOCIATED FACILITIES

Session 3 reviewed and discussed the existing initiatives for strengthening the intrinsic robustness of devices containing radioactive sources to protect against unauthorised removal. In particular, the session assessed the efficiency of design modifications and their potential operational and financial impacts. Finally, the session provided an opportunity to explore security certifications for devices containing radioactive sources and to learn from the process for developing a standard in a different sector.

Mr Michal Kuca from Sandia National Laboratories (USA) opened the session with a presentation titled *Security by Design*. He began with an overview of the role that the US DOE/NNSA Office of Radiological Security plays in helping to strengthen the security of radioactive sources worldwide. He then described in detail the In-Device Delay (IDD) voluntary programme. The programme provides substantial delay time against an adversary who attempts to remove the source from the device and can be installed during the manufacturing process or retrofitted at an end user's premises. Mr Kuca highlighted the success of this programme, which involves some of the largest device manufacturers in the world and has led to the installation of hundreds of IDD kits in the US and internationally. He said that significant progress has been made in the last decade for the security of sources and encouraged participants to build on this success by developing a harmonized approach to radiological security for medical devices that involves all stakeholders. He also said that developing an international industry standard would be one way to achieve such an objective.

Ms Anita Nilsson, AN Associates (Sweden) reinforced Mr Kuca's comments with a presentation titled *Establishing an International Security Standard for Medical Devices Containing High-Activity Radioactive Sources*. Building on the agreed need for strengthening the security of radioactive sources used in medical applications, she offered a way forward for designing effective security for the medical environment. Ms Nilsson explained how developing an industry standard would validate a certain level of security and strengthen the involvement and contribution of major stakeholders (industry and end users) without negatively impacting the use of the sources. Finally, she described two international standards organisations, the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), and the steps that need to be taken to propose a new standard to them.

Mr Ben Brodsky, Sandia National Laboratories (USA) delivered the final presentation of Session 3 titled *Lessons Learned from Developing ISO/DIS 35001 on Biorisk Management for Laboratories and Other Related Organisations.* He began by providing some background information on biological hazards and bio risk management, highlighting the fact that in 2014 no standard for the safety and security of biological materials existed. Mr Brodsky then described the options and processes that are followed to convert existing guidance into a global performance benchmark for biorisk management. He concluded his presentation by explaining why the ISO standard option was selected and what the main steps were that eventually led to the publication of the draft standard.

In parallel to these presentations, participants had the opportunity to discuss the IDD kits, review the possible role of industry standards, and discuss the challenges and opportunities that exist when establishing industry standards. Following are some of the major points from the discussions:

- ❑ IDD kits have been developed and installed in 600+ devices. Several manufacturers are systematically considering security by design from the early stages and have modified their designs over time.
- ❑ IDD kits have limited costs and operational impacts. (Manufacturers have usually absorbed the cost of design modification). Customers have accepted both new designs and retrofitted devices, but they have not pushed strongly for making IDD kits a requirement.
- ❑ Installation of IDD kits requires formal authorisation from regulators, but experience shows this is not usually an issue.
- ❑ There is still limited communication about and marketing for extra delay/security features. It is difficult for an end user to take credit for the added delay if blueprints are classified and exact resilience to the threat is kept confidential. A standard would encourage better communications and enable end users to receive credit for these features.

- ❑ Preliminary work for reaching out to standards organisations has been conducted. Quite a few challenges remain, however, and it is necessary to develop a better understanding of the standard development process. A better understanding of the experiences and lessons learned by other sectors would be very valuable.
- ❑ Developing a standard is clearly a long-term effort. It took a very long time for the bio community to define and agree on the scope of the safety and security standard. We need to develop a common understanding of "standards" and associated scope as early as possible.

DAY 2: WEDNESDAY 23 JANUARY 2019

After listening to a quick recap of the key findings of Day 1 and to the agenda and objectives for Day 2, participants were asked to form sub-groups and make the case for an industry security standard for devices containing high activity sources. In particular, they were asked to suggest a possible scope for such a standard, prepare a justification to be submitted to an international standards organisation, identify expected counter arguments against such a proposal, and propose answers to them. Findings from the exercise include:

Scope of the Standard

It should either be a technical standard that focuses on the device (similar to ISO 2919 on *Radiological protection - Sealed radioactive sources - General requirements and classification*) or a management standard with a broad scope that includes devices, facilities, people, etc. (similar to ISO 13485 on *Medical Devices Quality Systems*).

Pending questions:

- Should the standard focus only on medical facilities or also target other facilities such as universities and research centres?
- What security issues should be covered (physical security, information security, personnel security)?
- Would it be possible to expand an existing safety standard to include the security issues?
- What devices and sources should be covered by the standard? Category 1 and 2 only?

Justification of the Standard

- There is a gap. There are no harmonized rules and practices for addressing the robustness of devices against unauthorised removal of the sources.
- ISO standards provide an international reference, so being part of it would raise the profile of radiological security and support consistent implementation of security worldwide, independent of the maturity of the regulations.
- Senior management and organisations are already familiar with the use of standards and would quickly implement the standard if they opt for it.
- A standard would support security benchmarking between devices or facilities (depending on the type of technical or management standard applied).

- Development and adoption of standards could be seen as part of a global commitment to enhancing radiological security (e.g. as a follow-up to the political commitments made during the nuclear security summit process and reiterated through INFCIRC/910).

Counter Arguments

- There is already a lot of on-going work being conducted by the international community (IAEA, WINS, major countries, etc.) to support the development of good regulations and the implementation of effective security arrangements. Significant progress has been made in these last few years, so let's complete this work first.
- There are multiple competing requirements and expectations placed on the industry and end users; due to limited resources, a new standard might not be a priority for all organisations and countries.
- Because threats are permanently evolving, specifications for a standard might become obsolete quicker than the ISO revision process (5 year+).
- There are already too many standards. We should first consider integrating security matters into an existing standard before creating a new one.
- Multiple devices contain sources. Are we sure a single standard will cover all or at least most of them?

SESSION 4: STRENGTHENING THE COMPETENCES OF INDIVIDUALS WITH ACCOUNTABILITIES FOR THE SECURITY OF RADIOACTIVE SOURCES

The fourth and last session of the round table was organised to explore the processes in place to identify necessary competences for the people involved in the security of radioactive sources used in medical applications. It also reviewed the education and professional development opportunities that currently exist for radiological security and discussed the need to develop tailored opportunities for the medical sector. Finally, the session provided an opportunity to review practices to measure the competence of the people involved in the security of radioactive sources and to discuss what the role of certification in developing and demonstrating competence might be.

Ms Rhonda Evans, Head of the WINS Academy, opened Session 4 with a presentation titled *Strengthening the Competencies of Individuals with Responsibility for the Security of Radioactive Sources: The Role of Certification*. She began by describing some key issues, in particular the development of proper competence, for ensuring effective and sustainable radiological security. She also described the role of certain stakeholders in defining required competencies for radiological security and explained how certification can contribute to the development of competence and maintenance.

Ms LeeZa Duval from the Canadian Nuclear Safety Commission (CNSC) then provided a regulatory perspective in a presentation titled *Identifying and Providing Necessary Skills and Competencies for Individuals with Radiological Security Accountabilities*. She reminded participants about the essential need to understand the threat and possible consequences in the process of developing competencies. She also provided examples of actions that can be taken to raise security awareness and establish a strong security culture, stressed the importance of addressing cyber threats, and highlighted the role of exercises in demonstrating security achievements. Finally, Ms Duval encouraged participants to stay connected and to share information and lessons learned through various domestic and international working groups and forums of exchange.

Brief follow-up discussions were held to review the process for assessing the competence of people involved in radiological security and to discuss their professional development opportunities. It was agreed that describing, implementing and assessing the competences required for radioactive source security is very challenging, but some countries have done it. Participants also mentioned that job descriptions (e.g. for RSOs) usually lag behind the introduction of security responsibilities. Most of them don’t address this subject.

WAY FORWARD AND CONCLUSION

As the last activity of the round table, participants were asked to form groups based on their stakeholder origin (end users, industry, regulators, international organisations and programmes) to discuss the main findings of the event and share some of their take-aways and possible follow up actions. Examples of these actions included better engaging with professional associations, especially on peer review issues, developing joint safety and security newsletters, conducting further work on accreditation possibilities, and developing a competency framework for staff involved in radioactive source security.

In his concluding remarks, Mr. Legoux thanked participants for their active contributions during the round table, which made the event a success. He encouraged them to continue exchanging their ideas and experiences in protecting radioactive sources used in medical applications, as well as to share lessons learned with the entire community. He also committed WINS to building on this success and to continue offering opportunities for information exchange and professional development to all of the stakeholders involved in nuclear security.

In their evaluation forms, participants expressed a high level of satisfaction with the event, saying it had been a very useful learning experience that they would recommend to others. In their individual comments, participants confirmed this evaluation and said they particularly valued the amount of information shared during the two days, as well as the diversity of the audience and their respective perspectives.