WINS International Workshop on the Security of Radioactive Sources Used in Industrial Radiography and Well Logging Applications

Mexico City, Mexico 23 October 2019

REPORT

INTRODUCTION

In partnership with the VII Pan-American Conference on Non-Destructive Testing (VII PANNDT), WINS held a one-day international workshop on 23 October in Mexico City. The workshop focused on best practices to reduce the risk of theft of radioactive sources used in industrial radiography and oil well logging operations.

Participants at the workshop discussed the best security practices already in place at industrial radiography and oilfield service companies as well as the need to properly integrate people, procedures and security technology. Topics discussed during the event included:

- Credible threats to radioactive sources.
- Characteristics of industrial radiography and well logging sources impacting the need for security.
- Roles and responsibilities of industrial radiography, oil and service companies; nuclear regulators; and other State agencies in ensuring effective security of radioactive sources.
- International recommendations and examples of national requirements for the security of radioactive sources.
- The role of tracking and monitoring equipment and other technologies in improving the security of radioactive sources.
- Best practices for responding to a security incident.

The workshop was attended by approximately 45 participants from Argentina, Belarus, Brazil, Cuba, Egypt, France, Germany, Malaysia, Mexico, Nigeria, South Africa and the United States. Participants came from a diverse background of organisations including operators/licensees, isotope producers,

regulators, government officials and laboratories. The workshop was facilitated by Dan Johnson, Senior Advisor at WINS, and sponsored by the US Department of Energy/National Nuclear Security Administration (NNSA).

OPENING SESSION

Erika Hunsicker, Foreign Affairs Specialist, NNSA, opened the workshop with a presentation on the Office of Radiological Security (ORS), where she oversees projects to enhance the security of mobile radioactive sources, develop 'security by design' for devices that use radioactive sources, and provide voluntary security enhancements at sites that have radioactive material. ORS partners with more than 80 countries to enhance global security by protecting, removing and reducing the use of radioactive sources throughout the world.

ORS is collaborating with industry partners to develop and deploy a Mobile Source Transit Security (MSTS) system to enhance the security of mobile radioactive sources. The MSTS system has been designed to be effective, reliable and affordable. Unlike typical fleet services, which only track the vehicles, MSTS tracks the source itself, continuously monitoring its state of health and confirming its presence via radiation monitoring. The system is also tamper evident. Interested countries can schedule a needs assessment to understand if the system would be compatible with their facilities.

Following Ms. Hunsicker's presentation, Álvaro Acevedo, Project Manager at WINS, made a presentation on WINS, its vision and mission, how the organisation compares to the IAEA, the WINS programme of activities, and special opportunities for women and participants from developing countries.

Mr Johnson closed the introductory session by presenting the pre-event survey of the participants, which showed the following results:

- 95% of participants are familiar with IAEA recommendations and guidance for the management of radioactive sources.
- 85% believe that security is addressed consistently at all stages of the lifecycle in their organisation or country.
- 80% believe that radioactive sources used for industrial applications are more vulnerable during transportation to the job site.
- 70% think regulatory requirements effectively support the management of radioactive sources.
- 65% believe the systems that track and monitor mobile sources are vulnerable to adversary attack.
- Only 50% think that, in their country, the response to a security incident involving a lost or stolen radioactive source would be well coordinated by all the stakeholders involved.
- 40% think that law enforcement is not prepared to respond to a security incident involving a lost or stolen radioactive source.
- Only 30% think that the cost/benefit to installing and using systems to track and monitor mobile sources is financially defensible.
- 25% think that there is no credible threat to the security of mobile industrial sources used by operators in their country.

SESSION I: UNDERSTANDING THE SECURITY NEEDS FOR INDUSTRIAL RADIOGRAPHY AND WELL LOGGING RADIOACTIVE SOURCES

Session I of the workshop opened with a presentation from Yesica Álvarez Rico and César López Garcia, from Mexico's National Commission for Nuclear Safety and Safeguards (CNSNS), on *Threats to Radioactive Sources in Industrial Radiography and Well Logging Applications and Consequences of a Malicious Act Involving Them.* Ms Álvarez and Mr López outlined the definition of a threat, explaining that an adversary needs motivation, intent and capability in order to commit a malicious act. They also touched on the threat assessment process, including the need to evaluate both external and internal threats and the consequences of malicious use of radioactive sources.

Ms Álvarez and Mr López provided an overview of incidents of theft in Mexico (table below), including details on two major incidents reported by the media:

1) The theft of a vehicle that was transporting industrial radiography equipment with an Ir-192 source and activity of 3.63 TBq.

2) The theft of a nuclear densimeter with cesium-137 and americium-241 sources.

SENER SECRETARÍA DE ENERGÍA

RELACIÓN DE EMERGENCIAS RADIOLÓGICAS

CNSNS COMISIÓN NACIONAL DE SEGURIDAD NUCLEAR Y SALVAGUARDIAS

2010 – 2018						
Fecha	Material Nuclear o Fuente Radiactiva Involucrada	Lugar del Evento	Robo o Extravío	Cantidad Involucrada	Denuncia ante CNSNS/MP/PGR	Destino Final del Material
12 de enero de 2010	Americio-241/Berilio-Cesio-137	Campeche	Extravío	1	CNSNS	No recuperado, material confinado en el pozo
24 de marzo de 2011	Americio-241/Berilio	Pozo de Villahermosa, Tabasco	Extravío	1	CNSNS	No recuperado, material confinado en el pozo
24 de marzo de 2011	Cesio-137	Pozo de Villahermosa, Tabasco	Extravío	1	CNSNS	No recuperado, material confinado en el pozo
14 de julio de 2011	Cesio-137	Papantla, Veracruz	Robo	1	CNSNS	Recuperado y devuelto al propietario
14 de julio de 2011	Americio-241/Berilio	Papantla, Veracruz	Robo	1	CNSNS	Recuperado y devuelto al propietario
02 de mayo de 2012	Iridio-192	Hermosillo, Sonora	Robo	1	CNSNS	Recuperado y devuelto al propietario
06 de noviembre de 2013	Cesio-137/Americio-241/Berilio	Pozo Yoka, Ciudad del Carmen, Campeche	Extravío	1	CNSNS	No recuperado, material confinado en el pozo
02 de diciembre de 2013	Cobalto-60	Tepojaco, Hidalgo	Robo	1	CNSNS/MP/PGR	Recuperado y confinado
07 de enero de 2014	Tritio (H3)	Pozo KU	Extravío	1	CNSNS	No recuperado, material confinado en el pozo

Group discussions after the presentation revealed that in most cases, sources are inadvertently stolen during vehicle theft. Although the perpetrators do not intend to use the sources maliciously, the psychological effect of such incidents is still large, media reporting can be alarmist, and the public is not well informed about the possible effects.

Another key concept discussed was the 'attractiveness' of radioactive material. Participants identified that radioactive materials might be attractive to an adversary if their physical form is easy to disperse with the potential to inflict great harm and if the package is highly portable and easier to steal (e.g. industrial gamma radiographic devices or density/moisture gauges).

SESSION II: SHARING EXPERIENCES AND LESSONS LEARNT IN DESIGNING AND IMPLEMENTING SECURITY PROGRAMMES

Zulkefle Bin Hussin from the Malaysian Atomic Energy Licensing Board (AELB) provided a presentation on *Regulatory Requirements for the Security of Industrial Radiography and Well Logging Radioactive Sources.* Mr Bin Hussin outlined the legislative and regulatory structure in Malaysia, which oversees 1,193 licensees and 8,939 radioactive sources. Malaysia has adopted the IAEA's Code of Conduct on the Safety and Security of Radioactive Sources, which has supporting documents on:

1. Categorisation of Radioactive Sources
2. Security of Radioactive Sources
3. Guidelines on Import and Export of Radioactive Sources

Mr Bin Hussin described the security measures adopted for radioactive sources in Malaysia in detail, with specific examples of the protection elements implemented. He noted that they are still undertaking a cost/benefit analysis on GPS tracking systems for all mobile sources.

Like the colleagues from Mexico's CNSNS, Mr Bin Hussin provided an overview of major security events in Malaysia and the police and media response to those events (table below).

STATISTICS ON SECURITY EVENTS (2012-2018)

NUM.	EVENT	ACTIVITY	LOCATION	YEAR
11.	***THEFT***	Industrial Radiography	Paka	2012
12.	***THEFT***	Gauging	Pasir Gudang	2012
13.	***LOST***	Gauging - Oil Logging	Labuan	2014
14.	***LOST***	Industrial Radiography	Sipitang	2014
15.	***UNAUTHORIZED POSSESSION***	Unknown	Kuala Lumpur	2015
16.	***THEFT***	Missing Sources (Gauging)	Kemaman	2016
17.	***THEFT***	**Industrial Radiography**	**Klang**	**2017**
18.	***LOST***	Industrial Radiography	Shah Alam	2018

Table discussions following the presentation focused on the need for regulators to be proactive and practical rather than reactive and punitive after an incident. The licensee-regulator relationship is key and requires effective communication channels.

Participants had a keen interest in the decision-making process for the adoption of tracking and monitoring systems. Currently, there is no international harmonisation on what tracking systems to use or what features they should have. It is also unclear whether the regulator or the licensee would pay for the cost of introducing a tracking device.

SESSION III: ENHANCING SECURITY ARRANGEMENTS DURING ALL OPERATIONAL PHASES

Session III of the workshop included three demonstrations of tracking and monitoring systems for mobile and fixed radioactive sources. Demonstrations were provided by:

- Philip Kilfoil, GammaTec
- Jean-François Moreau, Nuc21
- Fred Mauss, Pacific Northwest National Laboratory (PNNL)

Following the demonstrations, Mr Kilfoil and Mr Moreau joined Ms Kathy Pappas, Mistras Group, and Mr Blake Kluse, PNNL, for a panel discussing opportunities and challenges in tracking and monitoring radioactive sources during transit. A major point of discussion was the need to do a cost-benefit analysis in order to determine whether a State and/or licensee should use tracking and monitoring systems. The demonstrations also showed the different gradients of tracking technology, from simple and lower-cost systems to robust systems that have a higher cost.

The panel discussed challenges associated with tracking and monitoring systems, including cybersecurity, water resistance, battery life, communication limitations in remote areas, general rugged design needs, the need for radiation monitoring, and barriers to adoption by licensees and device users. Some of these issues have not yet been fully mitigated, although participants generally agreed that limited tracking systems clearly have an advantage over no tracking system.

Participants also identified the key importance of education and training, as well as the development of a security culture, which solves many of the problems that technology cannot address. Organisations need a process/procedure to effectively transfer knowledge internally and maintain a robust nuclear security culture.

SESSION IV: RESPONDING TO A SECURITY INCIDENT INVOLVING INDUSTRIAL RADIOGRAPHY OR WELL LOGGING RADIOACTIVE SOURCES

Joseph Schwartzel, MELE Associates, presented on *Responding to a Security Incident Involving Mobile Radioactive Sources*. Key issues identified by Mr Schwartzel included:

- Mobile sources are frequently lost or stolen due to human error and due to their usage conditions. Radiography cameras go missing relatively frequently.
- Sources pass through multiple police jurisdictions while transiting to/from job sites, complicating the responsibility for response.
- Local police may not always understand the potential implications of a lost/missing source, and thus may not properly prioritise such an event or report it to higher-level law enforcement agencies.
- Because mobile sources are so widespread geographically, the scale of education and training needed for the huge numbers of law enforcement agencies and police officers makes it challenging. It is necessary to rely on State and Regional agencies to spread a 'common operating picture', or shared understanding of the impact and proper response to a missing/lost/stolen source.
- ORS is working to develop clear reporting procedures to help ensure that the right organisations are contacted and provided with the pertinent information.

After the presentation, participants organised into multiple breakout groups of licensees, regulators and source suppliers to discuss timely response to a security incident involving mobile radioactive sources. Key points from the discussions included the following:

Delays in reporting by licensees

Licensees need to feel supported in reporting a potential event to the regulator/State. Participants cited examples of incidents that licensees didn't report because they didn't want to report an irregular situation (such as a missing source) and make themselves liable to regulatory sanction, before fully understanding whether the situation was truly reportable.

Licensees may also delay reporting a lost source in the hopes of finding it or resolving accountability for the source before punitive sanctions are applied. Participants said a more collaborative relationship between regulators and licensees would improve security outcomes.

Lack of training

Many countries have insufficient training opportunities for first responders and end users on dealing with an incident involving the theft or loss of a source. Drills and exercises can help to ensure an appropriate response in case of an incident. Several participants provided examples of how exercises are organised in their State.

Remote locations

Sources are often used at remote sites or construction areas without communications coverage. Furthermore, because these locations are so remote, organising a rapid response and knowing where to go is complicated for the responders.

Communication between stakeholders

ORS emphasises the importance of stakeholder engagement in its programmes, and participants agreed with this approach. The regulator and other relevant agencies need clear points of contact. In some cases, participants only knew the point of contact for the regulator; other relevant agencies must also be accessible.

CONCLUSION

The workshop concluded with a session for participants to identify their key takeaways and actions upon returning to their home organisations. Participants vowed to take actions such as addressing communication problems with their regulator, re-examining their security systems in light of the discussions, and further investigating the tracking and monitoring systems demonstrated.
Dan Johnson provided a recap with the following key workshop findings:

1. Because their portable nature makes them 'attractive', mobile sources are susceptible to theft or mishandling. Theft of mobile radioactive sources is typically inadvertent, and malicious actors usually have not identified these sources as a target.

2. Effective ongoing engagement and communication with all stakeholders is critical, including with the public/media during an incident.

3. Regulations can be reactive and punitive rather than proactive. This can make licensees reluctant to report incidents.

4. The different tracking systems discussed have not been harmonised. Differing State requirements make this issue difficult to address.

5. The cost of an incident can be very high for the licensee involved, running into the millions of dollars. These costs need to be understood to fully evaluate the cost benefit of using a tracking system.

6. Security culture, education and training play an important role in mitigating the risk of theft or loss of sources. Organisations need to address the human factor and consider the insider threat.

7. Cost is the critical component for user acceptance of mobile tracking systems.

8. Challenges such as cybersecurity, water resistance, battery life, communication limitations in remote areas, general rugged design needs, the need for radiation monitoring, and barriers to adoption by licensees and device users will arise for tracking technologies. Stakeholders understand, however, that tracking solutions will not be perfect.

9. Multiple police jurisdictions can be involved in a case of loss during transport and are complicated to navigate. An intermediary liaison organisation is needed.

10. Technological solutions that trigger an elevated response during an incident need to be established.