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

March 6 – 7, 2019

Chicago, IL

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.

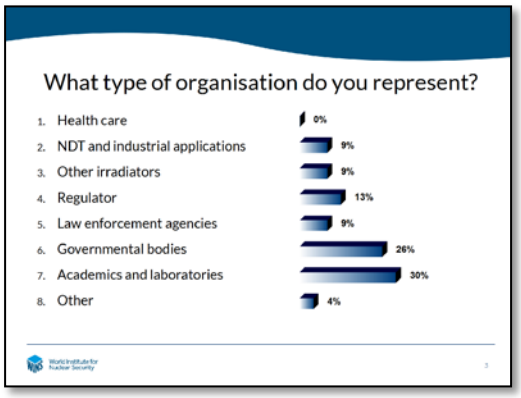
Security culture is one the most challenging aspects—and underlying vulnerabilities—in the practical implementation of security. The workshop explored the role of security culture in a facility's security system and why a strong security culture is so important for protecting radioactive materials. The workshop also explored how disposing of radioactive material or using alternative non-radioisotopic technologies can impact a facility's security culture.

The objectives of the workshop were to:

- Understand the threat to radioactive materials, including the potential motivations of adversary groups and individuals;
- Appreciate the particular threat posed by insiders and how to mitigate the threat;
- Develop a common understanding of what an effective security culture looks like and how it can mitigate threats;
- Identify the respective roles and responsibilities of licensees and regulators in establishing an effective and sustainable security culture;

- Review methodologies for measuring the level of security awareness and good culture in an organisation, assessing the results and implementing change;
- Identify possible incentives to encourage staff to adopt security best practices as a normal part of their daily work lives;
- Identify training opportunities to improve the competency of staff;
- Explore the use of peer review as a method for an independent assessment of security culture and identifying areas for improvements; and
- Explore permanent threat reduction approaches through the adoption of alternative technologies.

43 individuals attended the event from licensees, industry, universities, regulators, emergency response and law enforcement, and government agencies. The U.S. National Nuclear Security Administration (NNSA) and Illinois Emergency Management Agency (IEMA) were key contributors to the workshop development and design.



Workshop Opening Session

Daniel Johnson, WINS Senior Adviser, opened the event and welcomed the group. He provided a briefing on the WINS vision and mission, programme of work, and the WINS Academy, which includes a certification programme for radioactive source security management. He also covered the overall workshop objectives and provided a high-level overview of the security concerns with radioactive sources. **Cristen Ford, Deputy Director Domestic Program, Office of Radiological Security, NNSA** and **Gibb Vinson, Head of Radioactive Materials, IEMA** delivered keynote remarks for the event. Ms. Ford provided an overview of the NNSA's Office of Radiological Security (ORS) programme, while Mr. Vinson provided an overview of the radioactive source threat and risk, emphasising how the participants are all working towards the same goal of reducing the overall threat.

Following the keynote remarks, **Carl Reynolds, Workshop Facilitator**, led table and plenary discussions to develop a common understanding of what is meant by security culture and to identify issues and areas of main interest or concern for the participants. During the discussions, participants associated "security culture" with:

- What happens when managers are not looking
- How each and every person in the organisation understands security
- Sufficient training, awareness, checking, buy-in, conviction, and observation
- Clear individual responsibilities for security

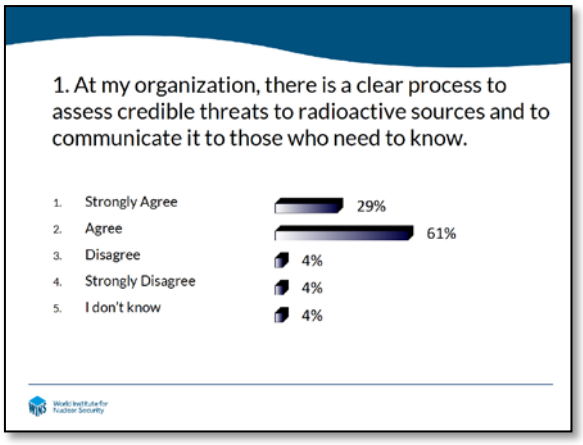
Key security culture considerations identified by participants included:

- The difference between security compliance vs. performance
- The critical importance of the human factor (what employees should do vs. what they actually do)
- The importance of badges, which specify access authorisation levels
- How zoning and protection areas differ
- The importance of background checks to help address the insider threat
- Use of the two-person rule to access specific areas
- Employees understanding of how they are monitored
- Why controlling sensitive information is important

Session 1: Exploring the Role of Security Culture in Mitigating Threats

Key session issues reviewed:

- ✓ Review the various threats to radioactive materials and the potential motivations of adversaries.
- ✓ Understand why security culture is so important for the effectiveness of a security programme.
- ✓ Explore the difference between security culture and security compliance and why this is key to effective security



Each session opened with an anonymous electronic voting session (as shown in the figure to the left) to understand the beliefs and attitudes of the participants in the room. After each vote, the workshop facilitator led a discussion on the results.

Ed Baldini, ORS Response Program Manager, **NNSA**, opened Session 1 with a presentation on *Threats to Radioactive Sources*. He discussed why it is so important to secure radiological materials, outlined vulnerable targets and reviewed the threat of radiological terrorism from particular groups (non-state actors, homegrown violent extremists, insiders, etc.). Mr. Baldini also discussed the two types of devices that are often used for radiological terrorism, Radiological Dispersal Devices (RDD) and Radiological Exposure Devices (RED).

Table discussions showed a consensus amongst the group that there is an enormous time advantage for someone acting nefariously from inside the organisation. There was also a discussion about upcoming 2020 activities in Chicago and ongoing efforts such as customised training for licensees—including the panoramic irradiator community—and relationship building between sites/licensees and local law enforcement agencies (LLEA).

Following the table discussions, **Gibb Vinson, Head of Radioactive Materials, IEMA,** provided a presentation on the *Current & Future Regulatory Environment for Security*. Mr. Vinson provided a high-level overview of the regulator's responsibilities and discussed materials of concern and associated curie levels. He also reviewed the current and future regulatory environment for security. He stated that security needs to constantly evolve.

Mr. Vinson then provided a detailed observation of major issues seen by IEMA such as transportation, which is (worldwide) the weakest part of nuclear and radioactive material protection. Other areas of regulatory focus include using electronic records, cyber security, disused/unwanted sources, aggregation of sources, and trustworthiness and reliability (T&R) requirements.

Following Mr. Vinson's presentation, participants held table discussions to identify concerns and best practices with security culture. Observations included the following:

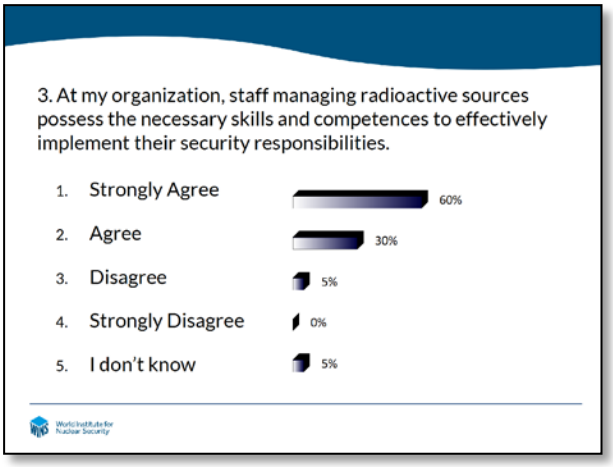
- T&R requirements for sources can be quite onerous, with large numbers of individuals requiring T&R clearance. Shifting to alternative technologies can greatly reduce this burden and ameliorate the insider threat.
- Industrial Radiographers discussed their "good catch" programme where employees can identify a security concern and bring it to management. They are rewarded with company prizes (t-shirt, hat, etc.).
- Small town LLEA are often unaware of the threat posed by radiographic cameras and other sources. The LLEA may not recognise the significance or importance of the information the site has sent them. Training and cooperation are critical and may require regulatory intervention.
- When testing a system notify the LLEA in advance. Do not call the LLEA during a "live test" as this may be dangerous.

- One manager of an operator goes "undercover" and walks around the facility without a badge to see if new staff respond appropriately and question his access credentials.
- Sites need to actually enforce refresher training and change up the refresher training so individuals pay attention. If you have good training, then you have a good start on security culture.

Session 2: Lessons Learned from Strengthening Security Culture

Key session issues reviewed:

- ✓ Review examples of good and bad security practices.
- ✓ Review the factors influencing the culture of an organisation, including how we can influence beliefs, values, understandings and behaviours of people.
- ✓ Identify possible incentives to encourage staff to adhere to security practices as a normal part of their daily duties.
- ✓ Identify common challenges for establishing a good security culture and how to overcome them.



Session 2 opened with a panel discussion on licensee experiences with improving security culture at their organisations. The following three panellists provided remarks:

Irina Craita, Health Physicist, University of Illinois

David Jackson, Radiation Safety Manager, STERIS Applied Sterilization Technologies

Douglas Miskell, Senior Radiation Officer, Applus RTD USA Inc.

Key points from the panel discussions included the following observations:

- Security measures need to be changed after an incident, for example after an employee has been downgraded in his or her security level. If not properly handled, an insider that becomes an outsider could still have access to sensitive areas or material.
- There is a general belief that a security incident "won't happen to me" and this belief needs to be eliminated.
- Good security culture has everything to do with human behaviour: what they know and what they don't know, defined security zones, good training, background checks, and effective implementation of security.
- Security culture is the repetition of the same event resulting in the same outcome. An example was provided of trying to get into a facility unbadged without success, but then on the next try access was granted.

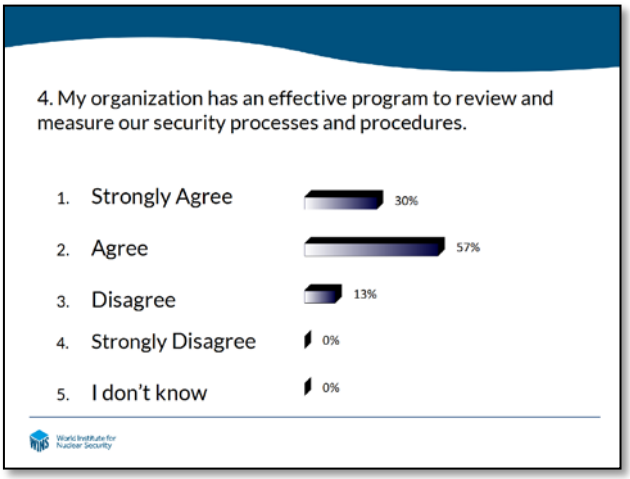
Following the panel presentation, **Gary Forsee, Supervisor Inspection & Enforcement, IEMA**, provided a presentation on *Security Lessons Learned*. This presentation led into breakout groups to examine security culture challenges and solutions. The presentation and exercise focused on identifying good and bad security culture practices, with the following examples provided.

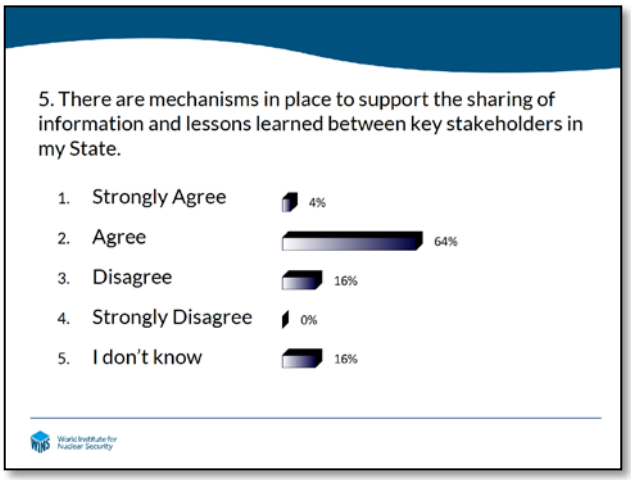
Good Security Culture Practices	**Poor Security Culture Practices**
100% escorting people without T&R; ensuring that the escorts understand the expectations put on them	Less than 100% escorting
Educate people on what needs to be done when an alarm is raised	No continuous training
Effective training & education	Pin-codes written above key pads
Consistent approaches to the implementation of procedures	One-size-fits-all approaches
Ability to continuously re-evaluate and improve	Lack of redundancy
Safety/security culture starts at the top. Management/leadership is involved.	Missing or poor documentation
Security compliance across all levels of the organisation	
An inclusive environment	
Use of metrics, self-assessment and audits	
Relationship building with key stakeholders	
Sharing of information and lessons learned	
Rewards systems	
Clear roles and expectations with personal accountability	
Access control testing and documentation	
Written security policy with SOPs	

Session 3: Methodologies for Assessing Security Culture

Key session issues reviewed:

- ✓ Review methodologies for measuring the level of security awareness and culture in an organisation. Understand how to assess the results.
- ✓ Explore the development of a security culture self-assessment plan for end-users.
- ✓ Explore the use of peer review as a method for an independent assessment of security culture and identifying areas for improvement.
- ✓ Explore metrics for continuously evaluating the level of security culture. How do we demonstrate we have achieved our objectives?





Claudio Gariazzo, Nuclear Engineer, Argonne National Laboratory, opened Session 3 with a presentation on *Security Culture Self-Assessment Tools* for nuclear facilities. The self-assessment tools were developed based on the IAEA's nuclear security culture guidance, in particular IAEA Nuclear Security Series 28, which goes into detail on nuclear security self-assessments. Participants were also encouraged to review the WINS Best Practice Guide 1.4 on Nuclear Security Culture, which contains extensive guidance on self-assessment.

As part of the nuclear security culture assessment process, Mr. Gariazzo recommended reviews of the following:

- Ensure there are clear roles and responsibilities, and these responsibilities are adequately explained to new employees.
- Ensure employees are vigilant and are aware of the insider threat.
- Obtain the commitment of senior management for the assessment.
- Explore if there is a common understanding of security culture.
- Have employees describe the desired security culture.
- Communicate assessment results to all personnel after appropriate review and filtering.
- Identify gaps, root causes and key initiatives for improvements.

Following Mr. Gariazzo's presentation, three participants participated in a panel discussion to review and discuss licensee experiences, successes and challenges with undertaking self-assessment, peer review, and establishing security culture metrics.

> **Nathan Duff, Loyola University Medical Center**, reported that his site conducts comprehensive quarterly self-assessments based on increased controls requirements. He also described the site's process for assessment: the site's Security Director coordinates with the LLEA; the RSO confirms required alarms reports; and site stakeholders are present and documented. Mr. Duff reported that they do not utilise a well-defined written checklist; however, observations are documented and issues are addressed.
>
> **Michelle Crase, Loyola University Health System**, reported that her site's reviews are similar to Loyola University Medical Center. Site staff attended training at the Y-12 nuclear complex; after training the site police were much more supportive. The site saw a huge change in its security culture because of the Y-12 training and the site is continuing to work on improving its safety and security culture.
>
> **James Masicek, The University of Chicago**, informed the group that his site conducts quarterly checks and annual reviews. The self-assessments are good and have shown the need for further coordination with site law enforcement on alarm response.

Discussions during the Q&A explored the mechanisms that are in place to support the sharing of information and lessons learned between key stakeholders. The group agreed that:

- Information is sent by NRC to all licensees.
- Inspection results (primarily best practices) are shared with licensees.
- Licensees communicate issues with each other.

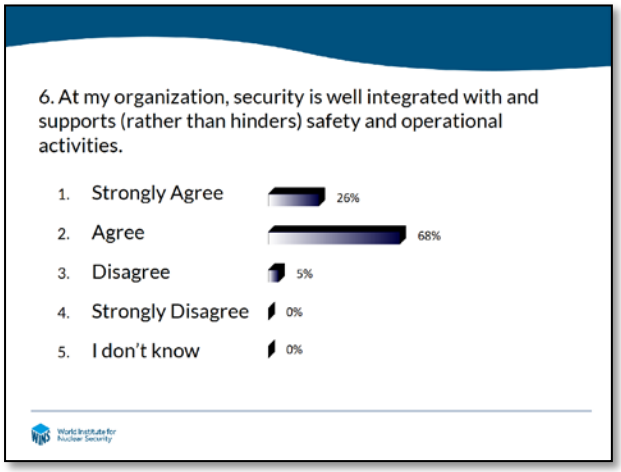
The participants were also asked to share experiences with assessing security culture at licensee organisations. Suggestions included:

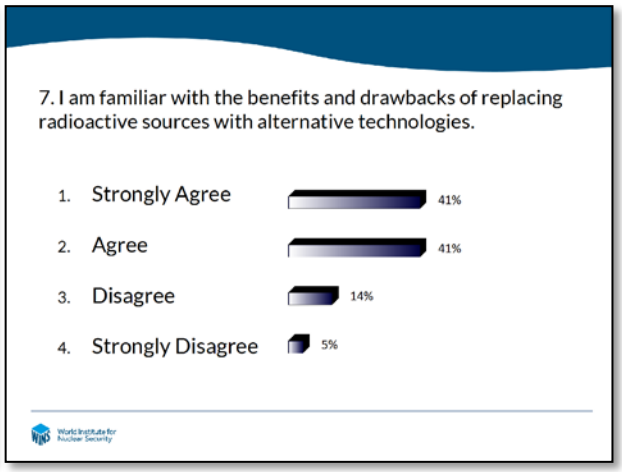
- Get feedback from the employees who have access to sources on what can be done to improve security culture.
- Limit Survey Monkey and similar open survey tools to individuals within the organisation and a very limited group. Otherwise use internal proprietary tools.
- If you are going to use a survey tool the site needs to be cognisant of where the data is going.
- It was suggested to contact IT, as the site may already have a tool available to minimise concerns with confidentiality.

Session 3 concluded with a small group exercise. The participants were asked to break-out into small peer groups to focus on designing a self-assessment or peer review for a radioactive source licensee. The exercise concluded with a role play session to simulate an interview, with the resulting interviews identifying security culture weaknesses, the importance of understanding security requirements and regulations, and a general list of questions that could be asked in a self-assessment:

- Do we have a security policy?
- Do we have security Emergency Operations procedures?
- Do you understand what suspicious activity/behaviour is?
- Can you recognise an employee vs. non-employee (i.e. badging)?
- Do you feel confident to report a security issue?
- Do you know who to report a security issue to?
- Do you know the difference between a security, fire, or other alarm?
- Do you know where the emergency/security contact list is?
- Do you know the difference between sensitive and non-sensitive information?
- What metrics need to be gathered to get a baseline of where the security culture resides?

Session 4: Sustainable Security and Permanent Threat Reduction





Key session issues reviewed:

- ✓ Review methodologies for measuring the level of security awareness and culture in an organisation. Understand how to assess the results.
- ✓ Explore the development of a security culture self-assessment plan for end-users.
- ✓ Explore the use of peer review as a method for an independent assessment of security culture and identifying areas for improvement.
- ✓ Explore metrics for continuously evaluating the level of security culture. How do we demonstrate we have achieved our objectives?

Session 4 opened with a presentation from **Kevin Hacker, Officer, Chicago Police Department**, on the *Chicago Public and Private Partnership (CP3)* programme. Kevin described the structure of the organisation and explained that the Department Counterterrorism Center falls under the Chicago Fusion Center and CP3 Program. The programme was established for:

Information Sharing
A Nationwide Suspicious Activity Reporting (SAR) Source
SAR Entry, Vetting and Sharing
CP3 was developed as a Portal that puts out a weekly security brief and provides a library with best practices. The potential exists to load critical information, such as elements of target folders, behind a secure portal that can be accessed "just in time" by a responding LLEA.

The afternoon session concluded with an in-depth discussion on alternative technologies that began with a presentation from **Aaron Galvan, CIRP Project Manager, PNNL**, on *Support Programs for Adopting Alternative Technologies & Permanent Threat Reduction*. His presentation was followed by a panel discussion on licensee experiences with adopting alternative technology. The panellists were:

Nikki Kurak, System's Manager, Bronson Health Group

Carolyn MacKenzie, Radiation Safety Officer, University of California, Berkeley

Randall Kimple, Associate Professor, University of Wisconsin

The panel highlighted specific lessons learned regarding the pros/cons associated with switching to new x-ray technologies. Highlighted reasons that a site may decide to transition to x-ray included:

- Easing the burden of T&R training
- Reducing the burden of documentation
- Costs associated with regulator/state requirements for enhanced security
- Space limitations
- Equipment reliability improvements
- Ease of use
- Reduced dosimetry needs.

However, there were a number of challenges and lessons learned noted, including increased power fluctuations and the need to condition x-ray tubes (they work better with more use). There were also challenges noted in re-doing radiation policies and trouble-shooting breakdowns, servicing and warranties.

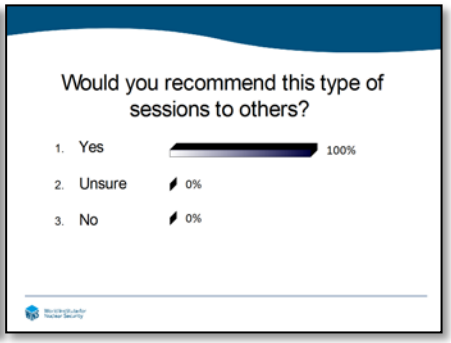
Conclusion

There was a final table exercise on participant actions to improve their security culture and better integrate security with safety operations. Key actions highlighted included:

- Set up surveys for their organisation to establish areas of improvement.
- Look to the Nuclear Threat Initiative's database of security incidents to demonstrate real-life examples.
- Identify what the regulator can do help facilitate interactions and assess the status of a site's security culture.

In his concluding remarks, Daniel Johnson from WINS thanked participants for their active contributions to the workshop, which had made the event a success. In particular, he thanked NNSA and IEMA for their substantive and deep contributions to the workshop. He encouraged all of the participants to consider the WINS Academy for their personal and staff professional development.

Overall, participants responded positively to the workshop with the following anonymous assessments at the end of the event:



Specifically, participants enjoyed interacting with a wide variety of stakeholders working together to improve security. They appreciated the opportunity to share information and lessons learned, while learning how technology and culture can work together to improve security. One participant noted that the event helped raise their security culture awareness to a new level, while another stated that the workshop opened their awareness beyond the standard “meeting the requirements” mode of thinking.