WORKSHOP ON RESPONDING TO SECURITY INCIDENTS INVOLVING RADIOACTIVE SOURCES

BALTIMORE, MD, USA

16 APRIL 2018

BACKGROUND

Planning for and managing the response to a radiological security incident at a facility can be extremely challenging if the wrong approach is used. Questions that need to be answered are:

- How are command, control and communication among different departments and organisations best designed and implemented?
- Why is interoperability important?
- What happens if it fails?
- Who has the controlling mind for radiological safety and security?
- What are some common challenges in managing this critical interface?
- What specialised safety training do armed response forces need to receive so they are able to discharge their responsibilities without compromising radiological safety?

To address these issues, the World Institute for Nuclear Security (WINS) and the US DoE Office of Radiological Security (ORS) jointly held a national event on Responding to Security Incidents Involving Radioactive Sources. This workshop attracted 40 participants from a variety of local and national stakeholders representing managers and specialists from the emergency response communities, as well as regulators, government departments and others who want to gain a specialised understanding of the issues and best practices.

OBJECTIVES

The purpose of this interactive, professionally moderated workshop was to give participants the opportunity to identify and address the potentially complex issues (including command, control and communications) that can arise when responding to a radiological security incident.

The workshop aimed to:

- Discuss the findings of the Inner Harbor Thunder table-top exercise (Baltimore) that was held earlier in January 2018 and continue the discussions on selected topics of interest;
- Identify best practices to enhance the resilience of radiological security arrangements against evolving threats;
- Explore options to involve all stakeholders and to establish an effective and sustainable security framework;
- Discuss the roles and responsibilities of internal and external stakeholders involved in radiological security incident management;
- Review the relationship between the licensee and the first responders;
- Explore the principles of interoperability and the range of arrangements that need to be put in place.

WORKSHOP PROCESS

The event, which was moderated by **Mr Carl Reynolds**, focused on issues such as:

1. Identifying how command, control and communication among different departments or organisations are best designed and implemented;
2. Exploring the importance of interoperability and what happens if it fails;
3. Describing and understanding responsibilities for approving the plans and how the planning documentation is structured;
4. Understanding competencies of the guard force and rules of engagement;
5. Identifying and addressing common challenges in managing the critical interface between nuclear safety and nuclear security.

Local and other national stakeholders gave a variety of presentations during the sessions, setting the scene for the discussions that followed. Mr Reynolds guided the discussions using such methods as plenary sessions, table and breakout discussions, and expert panels. An instant electronic voting system (e-voting) was used during the workshop to learn more about participants' opinions and concerns. Some results of these votes are illustrated in this report.

INTRODUCTION SESSION

Presentation

***Mr Jadallah Hammal**, WINS Programme Manager*, welcomed the participants and provided a preliminary overview of the objectives and agenda of the workshop.

Presentation

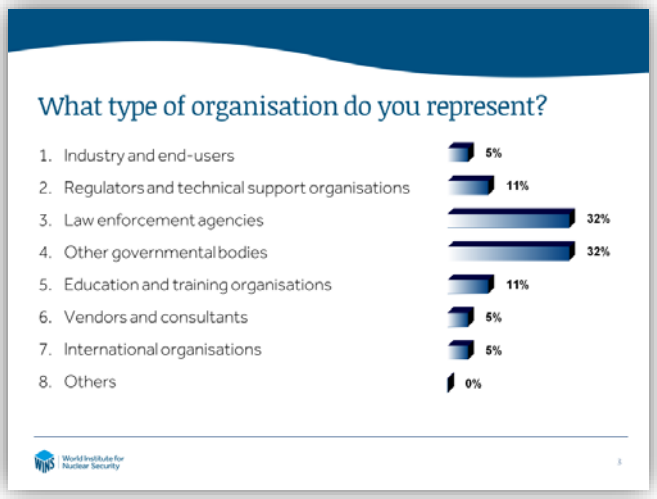
***Mr Dale Whitehead**, Office of Nuclear Incident Policy and Cooperation, NNSA, US DOE,* began his presentation by providing the participants with an overview of the Inner Harbor Thunder table-top exercise (TTX) that was conducted in January 2018 in Baltimore. He highlighted the number of participating agencies and focused on the scenarios that were used during this one-day exercise. He finished his presentation by highlighting some of the key themes that stood out at the end of the TTX. Some of those highlights are listed below:

- Operational Coordination and Communication – leveraging existing resources for immediate response;
- Incident Management – identification of the need for Unified Command during multiple incidents;
- Community Resilience – public awareness and communications coordination.

Participants' introduction and expectations

Participants were first asked to use the e-voting system to indicate which sector they represent (e-voting results below). Then they were asked to introduce themselves at their tables and to discuss their expectations coming into this workshop.

E-voting

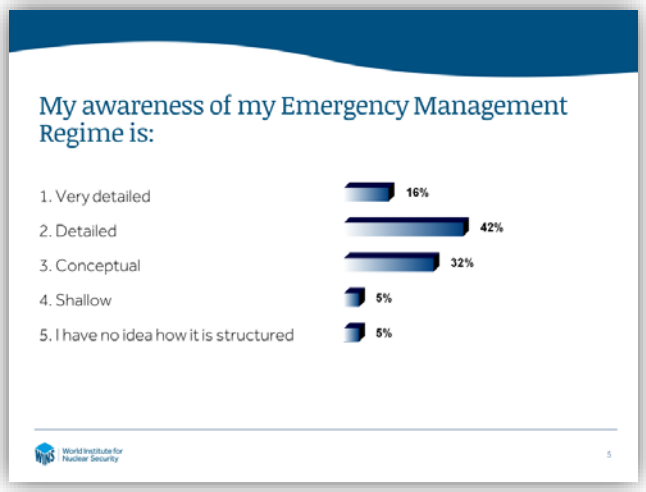


SESSION I: SETTING THE SCENE

The purpose of this session was to help participants understand the emergency management regime that is currently in place in Baltimore. The presentation and discussions that followed explored the role and responsibilities of the key stakeholders that are involved in emergency management.

E-voting

An e-vote was taken to elicit participants' awareness of their emergency management regime. Over 50% indicated that their awareness was detailed while others indicated that more awareness raising would be beneficial. The discussion that followed highlighted that those who had awareness of the emergency management regime got that through joint training and exercises and the exchange amongst colleagues.



Presentation

Mr Anthony Smith, *Baltimore City Mayor's Office of Emergency Management,* opened the Session I by providing an overview of how the office of emergency management operates. He elaborated on how the City Government goes about planning and train for emergencies. He continued by discussing his office's role in coordinating with the Maryland Emergency Management Agency and other regional or state-wide entities. Mr Smith concluded by discussing how his office supports the development of agency level incident management teams and the lessons learned from other major incidents. One of the key recommendations that followed this presentation was to invite an experienced Radiation Safety Officer (RSO) to the City's Local Emergency Planning Committee (LEPC) to share and provide fresh insights.

Group discussion

As a follow-up to the presentation, participants were asked to Consider the stakeholders involved in emergency response in Baltimore and to map the network of relationships and assess those that work well and those that need improving. They were also asked to note and asses those areas that work well and those that could enhance the network of relationships. Some of the discussions are reflected below:

- There is a good awareness between the command and specialist level. However, when points of contact change and/or commanders change – that change may cause a knowledge gap;
- Onsite police forces are usually well informed of radiological security; however, external first responders need to have much more awareness about how to respond to radiological incidents;
- Federal organisations usually work well with the City of Baltimore but there may be other stakeholders that need to be included;
- University Maryland Baltimore (UMB) is strongly linked up with Baltimore police and fire departments; however, this strong relationship is due to UMB having its own police force on site. Relationships are weaker where facilities that don't have police on site, as they don't have the interpersonal connections and/or awareness of who needs to respond to a radiological event;
- Confusion comes with federal assets and state assets and the communication between the various (30+) stakeholders. More exercises are needed to understand the flow of information between the various organisations.

SESSION II: ONSITE EMERGENCY PLANNING AND SECURITY INCIDENT MANAGEMENT

The objectives of session II were to describe onsite emergency planning and radiological security incident management arrangements.

E-voting

An e-vote was taken to elicit whether participants believed that internal stakeholder are effectively involved in the development of incident management strategies. The results of this e-vote are depicted below – indicating that internal stakeholders need further integration into the development of incident management strategies.

Presentation

Mr. Kenneth Brenneman, *University of Maryland, Baltimore, MD, USA,* opened Session II with a presentation titled "University of Maryland, Baltimore's (UMB) Security Preparedness / Response". He began by describing UMB's security plan and how it is structured around a multi-layered alarm and monitoring system that would detect unauthorized access. He concluded by addressing the content of the training UMB provides their responding officers and the types of equipment these have at their disposal once they respond to an alarm.

Presentation

Mr. Patrick J. McDermott*, Rutgers University, NJ, USA,* provided an additional perspective by presenting Rutgers University's "Security Preparedness and Response for Sources of Concern". He began his presentation by highlighting the important work Rutgers has been doing with the Office of Radiological Security and the timeline and key milestones of this collaboration. He continued by elaborating on how Rutgers continuously works with local mutual aid partners (such as police and fire); County Health Departments; County HazMat units; New Jersey State Police; and others. Mr McDermott went on describing how important relationships are in building the necessary confidence and trust and how all these elements can lead to effective training and engagements amongst various stakeholders. He concluded by describing the various types of training events Rutgers has had and the topics they addressed.

Group discussion

Participants were then asked to break into groups and to identify the types of information a facility needs to know about offsite responders and the information the offsite responders need to know about the facility. They were also asked to address how this information is communicated to one another, and what potential issues may arise in terms of communication. Following are some key findings of this breakout.

What does the operator need to know about the offsite responders?

- Response time;
- Identification protocols for offsite response;
- Tactics, training, equipment;

What do offsite responders need to know about the operator?

- Operator's emergency procedures;
- Risk exposure;
- Access arrangements;
- Layout of the facility;

How is this information communicated to one another?

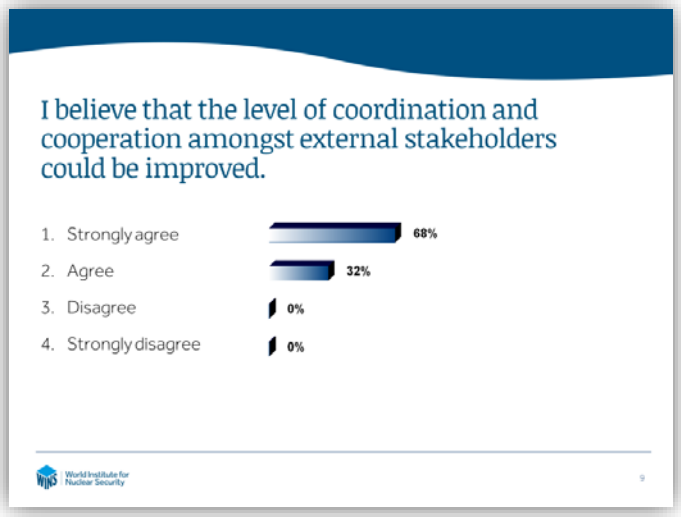
- Knowledge sharing and planning;
- Creating and complying to a memorandum of understanding – clarity of command remains difficult sometimes;
- Interpersonal relationships - building trust and confidence;
- Regular exercises – training on personal radiation detectors (PRDs) is essential;
- Working groups and interoperability meetings.

SESSION III: OFFSITE EMERGENCY PLANNING AND RADIOLOGICAL SECURITY INCIDENT MANAGEMENT

Session III was designed to broaden the understanding of principles of interoperability and joint working and to discuss the range of offsite arrangements that need to be put in place, and how to address the public and their concerns.

E-voting

An e-vote was taken to elicit whether participants believed that the level of coordination and cooperation amongst external stakeholders could be improved further. The results are depicted below indicate that there remains room for further collaboration and relationship building. There is a plethora of entities that respond to such events and coordinating them is a challenge:



Presentation

Mr Brian Welsh, *Joint Emergency Services Interoperability Programme (JESIP), United Kingdom*, provided the group with a UK view of interoperable working and some common challenges the institutions have been facing over time, such as lack of communication between commanders and responders, lack of understanding or proper sharing of risks and information, inadequate training and lack of audit process. He then described the joint approach taken by the relevant stakeholders and communications and engagement strategy which included the joint doctrine, training, testing and exercise and joint organisational learning. He concluded by emphasising the need for common systems and appropriate standards for establishing and maintaining interoperability and the importance of team work and team effort, open, honest relationship and focusing on the same goal.

Discussion

Mr Reynolds conducted a brief discussion with several local participants to see whether some of Mr Welsh's findings resonated with them. Some of the discussions that emerged highlighted the:

- Need to strengthen the relationships amongst local, regional, and State entities;
- Need for more resources to tackle conflicting priorities and to alleviate the need to compete with other entities for funding;
- Need for clear and effective MOUs that indicate who is in charge and which mean the same thing for all the stakeholders involved.

Panel on communicating with the Public

A handful of participants were asked to discuss their perspective on a variety of issues such as - communication, messaging, how to manage the thirst for information, and how to deal with social media and misrepresentation of the facts. Some of the challenges that were raised included:

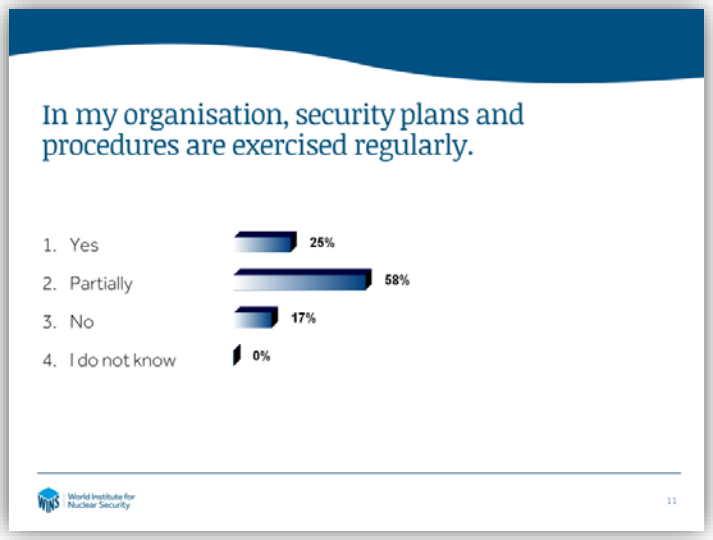
- What resources do you have to manage and operate your communications?
- Who coordinates between different stakeholders?
- Which organisation has primacy? Does this change during an event - what might trigger a change?
- How do you get messages agreed in the moment, as things change dynamically?
- Who decides what messages are appropriate?
- What communication channels do you use, and which are the most effective? Do you know what channels your public uses (TV, radio, social media apps etc)?
- How do you counter media you are not in control of? (Twitter, FB, other social media? TV stations etc)
- What experiences do you have of what works and what doesn't work...or works less well? Do you understand why this is so?
- What are your key recommendations with regards to communicating with the Public?
- Are there any patterns in public behaviour that are consistent across incidents of varying nature?

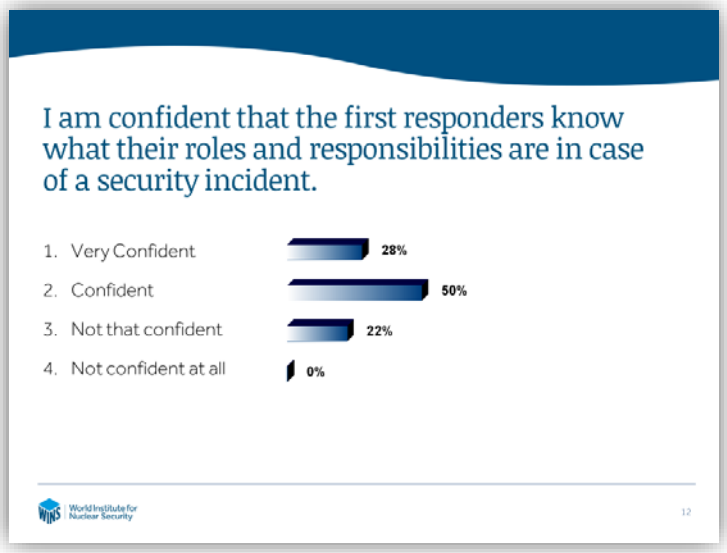
SESSION IV: TRAINING AND EXERCISING PLANS AND PROCEDURES

The objective of Session IV was to discuss the competencies of the response force and some effective exercises and tools that can be used to train and exercise the response force.

E-voting

As an introduction to the presentations and group discussions, participants were asked a series of questions regarding training and exercising plans and procedures. The results are illustrated below:





Presentation

Mr Carl Holland, Montgomery County Police Department, MD, USA, gave a presentation on "Law Enforcement Pre-Alarm Prevention and Response Operations". In his presentation he addressed the role of law enforcement in preventing radiological / nuclear terrorism and emphasised how law enforcement agencies with their unique skill sets (e.g. situational awareness, interrogation skills, detention/arrest authority, and use of force) provide the "last line" of defence. He continued, by describing two types of law enforcement prevention programmes – "inside-out" and "outside-in". In the "inside-out" approach source security is stressed and police protect and monitor known sites. Whereby in the "outside-in" approach, the interdiction of radiological sources out of regulatory control is stressed. Mr Holland, continued by stating that many Law Enforcement Agencies are adopting a blended approach where personnel are trained and equipped to do both fixed site protection / response as well as interdiction of unknown sources. He then went on to explain the four pillars to this blended approach: PREPARE; PARTNER; PROTECT; and PROVIDE. He concluded his presentation by discussing the various radiological exercises the Montgomery County Police Department conduct and emphasised once more that all stakeholders should look for opportunities to build and maintain a pre-alarm relationship that reinforces the security culture needed in today's threat environment.

Group Discussion

As a follow up to the presentation, the participants were asked to discuss the types of exercises their organisations use and which exercises they think are effective and why. They were also asked to discuss how to ensure that "lessons identified" from security exercises are translated into "lessons learned" and improve operational effectiveness.

The discussions that followed focused on the artificiality of training and exercise drills. It was pointed out that usually the most well versed and trained individuals are put forward to exercise certain scenarios and that this may cause a sense of false confidence because those individuals will not always be on duty when an incident or an emergency occurs. Furthermore, it was highlighted that when attempts are made to bring in other staff members off the "bench" and

get them involved – the political pressure of running such large-scale exercises successfully sometimes overshadows the benefit of having new and less experienced players in the game. Overall, the discussion on lessons learnt revolved around validating training methods, equipment, and the team response – both the individual response and the operational plans. It was highlighted that adding the complexity of having to deal with radiation into existing training operations would be beneficial and cost/time effective.

SESSION V: WAY FORWARD AND CONCLUSION

The final session of the day focused on highlighting some of the opportunities for improvement and on identifying the remaining challenges. The main purpose being to identify lessons learned and next steps. Participants were asked to break into groups to discuss the following questions:

- What are some of the things you thought of that you might want to implement at your organisation?
- What are the opportunities for improvement and remaining challenges?
- What will you do differently going forward?
- What does Baltimore (if anything) need to do differently? Who is going to make it happen? And who do you need to collaborate with to make it happen?

The participants pointed out that in case of a radiological incident, the internal response is usually satisfactory, but that all stakeholders need to work more on organising and conducting a successful external response. They also said that the web of communication is huge and confusing and it does not produce the desired outcome and does not enable the necessary flow of information. Another point the participants mentioned is the complexity of response and the need to reduce it and simplify it since sometimes there is a large amount of groups responding which can be counter-productive. However, the participants indicated that sometimes there is a lack of awareness of all resources, tools and assets available for proper response to an incident which makes the response less effective.

E-voting

The e-voting system was used to obtain a final evaluation. Participants indicated that they were very satisfied with the event, that it had been an excellent and useful learning experience, that Mr Reynolds had been an effective facilitator, and that they would recommend the event to others. The results are illustrated below:

In their closing remarks, representatives from the US DoE Office of Radiological Security and WINS emphasised that the success of the workshop was largely due to the active contributions of all participants. They praised the willingness of the group to learn from the speakers' team and from each other despite a challenging topic. They added that the discussions had shown that participants (and likely the stakeholders they were representing) had a strong appetite for increasing their capabilities to strengthen their already existing incident management programmes.