# Workshop on Maintaining Effective Security during the Decommissioning of Nuclear Facilities

# Vienna, Austria - 20-21 November 2019

# REPORT – Draft for Comments

## BACKGROUND

Decommissioning is defined by the International Atomic Energy Agency (IAEA) as the administrative and technical actions taken to allow the removal of some or all of the regulatory controls from a facility. The use of the term ‘decommissioning’ implies that no further use of the facility for its existing purpose is foreseen. The actions taken in decommissioning need to ensure the protection of the workforce and continuous protection of the public and the environment. This typically includes reducing levels of residual radionuclides so that material and buildings can be safely released and reused. From a nuclear security perspective, proper arrangements need to be maintained during the entire decommissioning process and need to be applied in a manner that is commensurate with the security risks posed by remaining nuclear and other radioactive materials.

Since the inception of the nuclear industry, more than 100 commercial power reactors, 250 experimental or research reactors, and numerous fuel cycle facilities have been retired from operation. As of today, only some of these facilities have been fully dismantled. In addition, several States are currently facing anticipated decommissioning needs due to major changes in their nuclear energy mix or high costs for the renovation of their nuclear power fleet and facilities. It is predicted that up to 200 reactors may shut down by 2030 and that around 100 additional reactors will shut down by 2060 worldwide.

The growing numbers of decommissioned facilities are impelling regulators and operators to re-evaluate their security requirements and operation processes while balancing safety and security objectives. Furthermore, the construction of special fuel storage facilities might be necessary and specific protective measures might be required.

Decommissioning is a complex, long-term and costly process that requires States, competent authorities, operators and specialised organisations to work together to tackle multiple challenges and barriers. Each phase of the decommissioning process must be carefully planned, executed and controlled with precision. From a security perspective, this requires identifying a continuously evolving risk, designing and implementing flexible and graded physical security arrangements, addressing cybersecurity threats, protecting sensitive facility security information, managing changes in the workforce (including new personnel and background checks), maintaining a strong security culture, effectively integrating nuclear safety and safeguards requirements and complying with the high standards of operation that the nuclear industry demands.

The World Institute for Nuclear Security (WINS) therefore decided to conduct a two-day international workshop to review and discuss all security matters related to the decommissioning of nuclear facilities.

## OBJECTIVES OF THE WORKSHOP

The key objectives of the workshop were to help participants:

* Identify major security challenges related to each phase of the decommissioning process;
* Develop a better understanding of why the various decommissioning strategies may have an impact on security needs;
* Discuss how security needs related to the decommissioning process can be identified and minimised from the earliest stages of the lifetime of a nuclear facility;
* Identify interfaces between nuclear safety and nuclear security during decommissioning and discussing best practices to prevent and mitigate conflicts;
* Develop a better understanding of how roles, responsibilities and organisational structures may evolve during the decommissioning process and how these changes may impact security;
* Discuss the importance of mitigating insider threats during decommissioning, including ensuring the role of nuclear material accounting and control as well as accurate nuclear material measurements;
* Identify the need for security awareness and competencies for the various staff, in particular non-security professionals, involved in the decommissioning process;
* Discuss best practices for ensuring regulatory oversight which is commensurate to the evolving hazards and risks;
* Identify and discuss possible cybersecurity threats when decommissioning nuclear facilities;
* Discuss and understand the internationally accepted recommendations, requirements, etc., for the security of decommissioned nuclear facilities.

A total of 41 experts from 15 countries and one international organisation attended the workshop. They represented the main stakeholders involved in the decommissioning of nuclear facilities (e.g. nuclear operators, regulators, transport experts, international programme representatives and security consultants). Participants were asked to have open discussions, express their own perspectives, and offer suggestions for improving the security of nuclear and other radioactive materials during the decommissioning process.

 

The event, which was professionally facilitated by Ms Anna Patterson, included expert presentations and group discussions to provide maximum engagement. In addition, an instant electronic voting system was used to allow participants to anonymously share their views on selected questions. Some of the e-voting questions are included in this report.

## WORKSHOP PROGRAMME AND KEY FINDINGS

**Day 1: Wednesday, 20 November 2019**

### OPENING SESSION

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

#### Participant Introductions and Expectations

To start the discussions, participants were asked to introduce themselves at their tables and discuss their expectations in coming to this event. Examples included:

* Learning from others; increasing knowledge about decommissioning and security; better understanding the evolution of security needs at various stages of decommissioning; transferring this knowledge back home;
* Sharing experiences and perspectives; adding value to the discussion;
* Expanding list of professional contacts in security and decommissioning matters (networking); maintaining connections after the event;
* Benchmarking practices; finding concrete solutions (no theory) that can be compared with own projects or practices;
* Anticipating security needs during decommissioning and incorporating this information into current plans.

**Ms Sue Perkins, Nuclear Energy Institute (NEI), USA,** offered a keynote presentation on *Maintaining Effective Security During Decommissioning.* She began with the current decommissioning landscape in the US, including various decommissioning strategies, an overview of US plants under decommissioning and some information on regulatory matters. Ms Perkins continued her presentation with a case study describing the security evolutions during the various phases of the decommissioning of a single-unit utility. She then provided the audience with a summary of the main security lessons learned by the utility. Ms Perkins concluded her presentation by highlighting the importance of raising awareness about decommissioning matters amongst all stakeholders, in particular the public and local communities.

#### Follow-up Discussion

In a discussion at tables that followed the presentation, participants were asked to reflect on the key messages delivered by Ms Perkins, as well as on the key issues to keep in mind during the workshop and on the main security challenges that may arise during the decommissioning process.

Participants indicated that decommissioning was for many nuclear operators a new way of working with a very large range of activities involving a diverse workforce. Participants stressed the need for the security department to adapt to operational changes (no routine work anymore) and be ready to deal with unexpected situations. They also highlighted the need for ensuring interaction and harmonisation between the security plan and the decommissioning plan. It was also agreed that it is important to maintain a level of security commensurate with the risk and to avoid over-conservatism in the security requirements.

## SESSION 1 – REVIEWING THE DECOMMISSIONING PROCESS

Session 1 was organised to conduct a review of different decommissioning strategies and better understand who the key stakeholders are. It was also to learn from the decommissioning projects that have already been completed and assess what has been done well and what remains more challenging.

**Mr Vladimir Michal, Department of Nuclear Energy, IAEA,** opened session 1 with a presentation on *IAEA Considerations on Decommissioning.* He started by describing the overarching role of the IAEA and its specialised activities in the field of decommissioning. Mr Michal then quoted the different phases of the decommissioning process, described some of the operational matters related to decommissioning and highlighted some IAEA publications and initiatives (e.g. networks) available to assist various stakeholders during this process. He concluded his presentation by presenting some upcoming IAEA work on the topic.

In complement to the previous presentation, **Mr Simon Carroll, Business Unit Nuclear Decommissioning, Vattenfall, Sweden**, talked about *Vattenfall’s Decommissioning Strategy for Ringhals 1 & 2 in Sweden*. After a short presentation on his organisation and the specialised business unit of decommissioning (BUND), he explained the process followed by Ringhals NPP to prepare for the decommissioning of two of its units while keeping two others in operation. Mr Carroll explained the sharing of responsibilities between Ringhals and BUND and the process for transferring these responsibilities from one to the other. He then described the required work during the planning and execution phases and provided some information on the Swedish national approach to waste management. Mr Carroll concluded his contribution by detailing a number of security considerations, including the suitability of the decommissioning framework, regulatory matters, spent fuel management and integration of security needs from the planning phase.

#### Group Discussion

In a small group discussion following the presentations, participants further explored security needs associated with decommissioning matters. Some of their findings included:

* Decommissioning is a normal and expected part of the lifecycle of a nuclear facility and should be anticipated. Overall, decommissioning needs will keep growing in the future.
* Decommissioning is a complex and long-term project. It implies many factors: safety, security, regulations, technical matters, the human factor, financial aspects, public involvement, and disposal and storage of waste and material.
* Good record keeping from the start of a nuclear project is a prerequisite to cost-effective decommissioning.
* Retaining qualified staff is a challenge and usually depends on local job market conditions. It is often easier to keep security staff than engineers. Consider career transition help, training and employment assistance.
* Decommissioning requires specific expertise and only a limited number of organisations/contractors possess such expertise (i.e. risk of bottleneck and delays).
* Different decommissioning strategies exist, and implementation varies a lot from country to country based on local conditions and funding availability.
* A lot of lessons learned have already been consolidated from past decommissioning experience. It is important to transfer these lessons to those starting the process.
* A lot of international guidance for decommissioning is available (however, very little security guidance exists). Significant IAEA support is available, and it is growing (including security).

## SESSION 2 – UNDERSTANDING SECURITY RISKS AND CHALLENGES DURING DECOMMISSIONING

The objectives of Session 2 were to identify the security challenges that can arise during the decommissioning process and review how countries and organisations are developing and implementing strategies to address the security risk.

**E-voting**

In order to initiate the discussions, participants were asked to answer two e-voting questions related to responsibilities for security during decommissioning and on national strategies to address decommissioning and related security matters. They had mixed feelings on how differently security might be implemented when driven by the nuclear operator or a contractor but ultimately, they clearly indicated that security is the responsibility of the operator (licence holder), regardless of whether the work is conducted by the operator itself or outsourced to a contractor. When discussing the results of the second question, participants indicated that many countries have neither established a decommissioning strategy nor have a clear disposal pathway for all waste.

 

**Mr Marco Schraver, Authority for Nuclear Safety and Radiation Protection (ANVS), The Netherlands,** opened session 2 with a presentation on *Security and Decommissioning, a Few Aspects.* After providing some information on the nuclear industry in the Netherlands, Mr Schraver reminded the group of the respective roles during the decommissioning process and detailed the key responsibilities of the licensee. He then explored some particular security aspects to be kept in mind during decommissioning and concluded his presentation by highlighting the recent IAEA publication on *Security during the Lifetime of a Nuclear Facility* (NSS 35-G), which includes some information related to security during decommissioning.

**Mr Bill McGlennon, Sellafield, UK,** then provided a presentation on a nuclear operator’s perspective on decommissioning approaches and challenges. He opened his presentation by briefly describing Sellafield’s site history and activities, highlighting the complexity of the regulatory environment. Mr McGlennon then described the Sellafield organisational model and the basis of the risk management framework. He continued by detailing the responsibilities for security during decommissioning and security priorities. Mr McGlennon concluded his presentation by describing some of the challenges faced by Sellafield during decommissioning activities.

**Follow-up discussion**

Reflecting on the key messages of the presentations, participants further explored security matters related to decommissioning. Some of their main findings are consolidated below:

* Communication and engagement with essential internal and external stakeholders are needed to obtain their buy-in as early as possible.
* The security plan needs to be dynamic and reflect the decommissioning steps. The licensee must continuously prove that the security objectives are still met.
* There are different and evolving risks. The target set changes. Some new risks appear. Access and zoning change as the work progresses.
* There is a need to (re)train security staff and raise their awareness about the evolving risks.
* Since many external contractors are involved, screening procedures are key. Escort needs may increase significantly.
* Anticipating security costs is challenging. Experience from other organisations may provide some starting point.
* Cyber threats need to be considered (e.g. blended attack or tampering with records).

**Ms. Allyn Milojevich and Mr Richard McAfee, Consolidated Nuclear Security (CNS), Y-12 National Security Complex, USA**, concluded Session 2 with a presentation on *Nuclear Fuel Cycle Facility Decommissioning: Nuclear Security Considerations*. After presenting the main missions of the Y-12 complex, they described key questions to be answered when considering the decommissioning of a facility. They then presented some of the major concerns, such as NMAC issues and insider threats, that an operator might face during decommissioning and how facility characteristics may influence the process and security needs. In their conclusion, they highlighted the importance of developing an all-risk approach encompassing materials, information and equipment (classified, proprietary design, subject to export controls, etc.).

Answering questions from the audience, Ms Milojevich and Mr McAfee stressed the fact that the risk for nuclear fuel cycle facilities is very different from the one for nuclear power plants. Due to possible access to materials, they perceived a higher risk of theft by insiders. They emphasised the need to clarify as early as possible recoverable vs. unrecoverable holdup. They recommended including contaminated materials in the target list and encouraged operators to conduct “wall to wall” surveys. It was agreed that knowledge of historical plant operations and processed materials was essential. They noted that the security posture remains rather stable during decommissioning as long there is accountable material. Ms Milojevich and Mr McAfee finally reiterated the importance of strong vetting mechanisms for people authorised to access sensitive locations and escort procedures for visitors, including short-term contractors.

## SESSION 3 – DEVELOPING PROPORTIONATE SECURITY REGULATIONS

Session 3, the final one of Day 1, was organised to better understand regulatory matters for ensuring effective security decommissioning. It was also to assess whether regulatory changes might be needed to adapt to the decommissioning process and the evolution of the security risks along this process.

**Mr Steve Bennett, Office for Nuclear Regulation (ONR), UK**, delivered a presentation on *Commensurate Regulatory Oversight of Evolving Hazards and Risks.* After a quick introduction of the nuclear security framework in the UK and the role of ONR, Mr Bennet detailed the recent process followed by the UK to move from prescriptive regulations to outcome-focused ones, based on Security Assessment Principles (SyAPs) and the overall responsibilities of the operators for protecting materials and facilities. He then highlighted the importance of a regulatory approach, including inspections and exercises, commensurate to the security risk and taking into account the lifecycle aspects of facilities. Mr Bennet concluded his presentation by a describing the ONR Enforcement Management Model (EMM), which provides the basis for ONR enforcement and follow-up actions to inspection findings.

**Follow-up discussion**

Building on the key messages of the presentation, the participants had a brief discussion to explore regulatory aspects during decommissioning. They clearly highlighted the role of regulations to achieve effective and secure decommissioning of nuclear facilities, and they reiterated the importance of a graded approach (regulations commensurate with risk). Some participants regretted bottlenecks in regulators’ security departments that delayed decisions.

Participants stressed the need for adequate technical knowledge for regulatory staff. Required skill sets may differ significantly from those necessary for facilities in operation. Competent inspectors need soft skills, teamwork, analytical thinking and communication skills. As for operators, long-term knowledge management and retention of experienced staff might be challenging.

## SESSION 4 – ADDRESSING SECURITY OPERATIONAL CHALLENGES

Session 4 was organised to review operational security aspects of decommissioning. It was to better understand who the key internal stakeholders are and what operational challenges may arise during the process, in particular when addressing safety and security interfaces. The session was also an opportunity to listen to those who have already decommissioned their facilities and consolidate some good security practices.

**Mr Guillermo Martín García, ENRESA, Spain**, delivered a presentation on the *Jose Cabrera NPP Security in Decommissioning Project.* Mr Martín first provided some general information on his organisation, ENRESA, and on his facility, the Jose Cabrera NPP. He then summarised the applicable regulatory framework in Spain and described the entire lifecycle of his facility, from building to decommissioning, highlighting how responsibilities have evolved over time. Mr Martín continued by describing the security approaches implemented during the process, including the evolution of the protected areas and the construction and operation of an Independent Spent Fuel Storage Installation (ISFSI). He concluded his presentation by sharing some of the security lessons learned by his organisation.

**Mr Eugenijus** **Sepetys, SE Ignalina Nuclear Power Plant (INPP), Lithuania**, offered a second operator perspective on the topic. After describing the characteristics and operational history of INNP, Mr Sepetys listed the main Lithuanian stakeholders involved in the protection of INPP and highlighted the essential support of international programmes in achieving effective security at INPP. He then described the decommissioning preparation and implementation plan and reported on the progress of the facility dismantling, including the construction of new waste facilities. Mr Sepetys also detailed some challenges for the INPP security department and the entire organisation during the decommissioning process. He concluded his presentation by describing organisational arrangements for security at INPP.

**Follow-up discussion**

Reflecting on the key messages of the presentations, participants further explored operational security matters related to decommissioning. Some of their main findings are consolidated below:

* Proper engagement with internal stakeholders is essential. The security department needs to understand the process and the associated risks to offer efficient security services. Security staff may need specific training to understand the decommissioning process.
* Security plans and procedures need to be dynamic and flexible enough to adapt quickly to the different phases of decommissioning operations.
* Security measures may need to be increased or reduced proportionally to the presence or absence of materials in the area. The security footprint may change frequently.
* It is important to inform the staff and contractors of security changes in a timely manner (organise meetings; target senior management and task them to cascade the information down; collect feedback from staff and implement changes if needed).
* In addition to spent fuel management issues, the process generates significant amounts and different types of radioactive waste. The associated security risk needs to be assessed and measures tailored to that risk.
* At the end of the process, security is significantly reduced and usually focuses on a limited number of storage areas.
* There is a need to communicate effectively with the regulator to avoid any misunderstanding or issue.
* There is a need to maintain adequate industrial security all through the process. Operators often experience petty theft. New technologies, such as tracking tools, may contribute to the protection of expensive equipment.
* Emerging threats, such as cyber, drones, etc., also apply to decommissioning activities and sites.
* Many operators use the services of contracted security staff and are satisfied with the service.
* There is often a need to improve security culture. Addressing safety and security cultures together is recommended.
* Networking and sharing of operational experiences with other operators are clearly beneficial.

At the conclusion of Session 4, **Mr Ben Whittard, International Nuclear Services (INS), UK** provided the group with a perspective on transport security matters during decommissioning. Mr Whittard first introduced INS and its capabilities in international transport services all along the nuclear fuel cycle. He then highlighted why transport issues are essential and what types and modes of transport are related to decommissioning. Mr Whittard concluded his presentation by describing five strategic and four tactical (operational) challenges faced by INS when implementing transport operations.

**Break-out groups**

Participants were then offered the opportunity to further discuss four topical areas (transport security; nuclear material accounting and control (NMAC); cyber security; collaboration among internal stakeholders). A brief summary of the discussions is reflected below:

Transport security

* Transport still remains an area with possible vulnerabilities, or at least it could be seen as “attractive” for adversaries.
* Transport needs should be considered as early as possible in the decommissioning plan. You need to anticipate what waste/material will be generated and will require transport. Decommissioning involves frequent, high-volume transport of low-level waste.
* You need to draft generic transport security plans for routine activities and specific ones for special cases.
* Whenever possible, consolidate materials to reduce the number of transports.
* As with other nuclear operations, drones are a potential threat. The primary objective is to detect the UAV (not intercepting or neutralising it).
* Efforts should be made to reduce predictability of the transport and to control information (challenging because multiple stakeholders are involved).
* Transfer of security responsibilities is essential and needs to be agreed upon in advance.

Nuclear material accounting and control

* Lack of robust NMAC procedures may lead to vulnerabilities and material diversion opportunities.
* The nuclear process may retain material (hold-up), and the quantities might be difficult to assess before dismantling. Strong access control needs to be maintained until clean-up/dismantling is achieved.
* You need to designate who is accountable for the materials.
* You need a plan to anticipate what you may find (the type of materials and quantities), how much of it will need to be removed and when you will need to remove it.
* Safeguards staff need to efficiently interface with security people.
* The accountable material group should communicate with security.

Cybersecurity

* Cybersecurity is an area of increasing risk and concern.
* There is a need to educate staff and adapt practices. Social engineering is a common attack vector.
* Cybersecurity requirements are not fully established and clear. What is the role of the DBT for cyber threats? How do you apply it to decommissioning activities?
* Operators would welcome more guidance from regulators.

Collaboration among internal stakeholders

* Good interface between safety and security is essential. Establishing robust professional relationships increases risk prevention and mitigation.
* Clear accountabilities are essential. They facilitate understanding and acceptance.
* Security should be seen as a business enabler, not an impediment.
* Establish early engagement with all. All stakeholders must understand the industrial process and the associated safety, security and emergency preparedness needs.
* Education and training should be made available whenever necessary.
* All discussions should include good record keeping and be kept for long-term knowledge management. Organise panels to review challenges and identify solutions jointly.

## SESSION 5 – MANAGING CHANGES IN THE WORKFORCE AND ORGANISATIONAL STRUCTURES

The final session of the workshop was designed to assess whether changes in the ownership, business model or organisational structure might be a risk to security. It was also to discuss what actions might be needed to keep the workforce motivated and maintain a positive nuclear security culture.

**E-voting**

As a start to Session 5, participants were asked to answer an e-voting question on the preparedness of nuclear organisations to assess and anticipate the potential impact of cessation of activities and decommissioning on the workforce. A majority of the participants believed operators are aware of the potential risk and are already taking necessary measures. They mentioned that HR departments were usually involved in the process, which goes far beyond security matters, and were trying to address the issue has soon as the decommissioning decision had been taken.

**Mr Pekka Pyy, Department of Nuclear Energy, IAEA**, delivered a presentation on *Managing and Leading Organisational Change*. Mr Pyy started his presentation by highlighting the numerous status changes that usually occur during the lifecycle of a facility and describing some good practices for successfully managing these changes, in particular during the transition periods. He then detailed the multiple IAEA publications related to managing the change and, based on selected IAEA guidance, described the process for leading the change, including implementing the SCARF methodology (status, certainty, autonomy, relatedness, fairness). Mr Pyy concluded his presentation with some considerations on maintaining security matters during organisational changes.

**Follow-up discussion**

Reflecting on the key messages of the presentations, participants continued to explore the topic and offered the following considerations:

* Don’t only manage change, lead the change (head and heart): Inspire and create a culture of change.
* There is a learning curve to change management. Organisations and managers should learn from their mistakes.
* Some changes are slow and known ahead of time, others are sudden. Senior leadership needs to be aware of that and be ready (with training and procedures) to react.
* Organisational change differs from technical changes and must be handled properly as a project.
* Changes need to be discussed before being implemented. A risk and opportunity assessment needs to be conducted first.
* Staff will react as humans, with emotional components.
* Decisions need to be explained. You need relay (champions). Seek support from leaders at all levels.
* Successful change requires a plan and clear responsibilities and accountabilities. You need a Plan and a Plan B!
* Changes often have impact outside the organisations (e.g. the local community, contractors, etc.).
* Different work categories and stakeholders require different types of communication. No one size fits all.
* HR is essential. Implement nested processes, putting the individual at the centre in each case.

## WAY FORWARD AND CONCLUSION

In the last activity of the workshop, participants were asked to form small groups, reflect on what they had heard and discussed during the past two days, and identify concrete steps they would personally or collectively take to improve security during decommissioning. Participants then discussed the main findings of the event as a whole group and shared a few of their takeaways and possible follow-up actions.

In his concluding remarks, Mr. Legoux thanked the participants for their active contributions, which made the event a success. He encouraged them to build on the key findings of the event and to contribute proactively to the strengthening of security during decommissioning. He also committed WINS to building on this success and to update WINS’ programme of work to reflect the priorities expressed by the participants. Mr Legoux also confirmed that WINS will produce a new international best practice guide on the topic and will release it by the end of Q1 2020.

During the evaluation session, 100% of attendees expressed satisfaction with the event and 97% indicated they would recommend this type of event to others. In their individual comments, participants confirmed a high level of satisfaction and said they particularly valued the quality of the speakers, the expertise of the participants, the amount of information shared during the two days, and overall the atmosphere of trust and exchange.