World Institute for Nuclear Security

In partnership with Canada

Workshop on Mitigating the Cyber Insider Threat in the Nuclear Sector

03-05 September 2024. Vienna, Austria

Draft Agenda

Day 1 - Tuesday 03 September 2024

09:00-09:45 **Introduction Session**

Welcome remarks, workshop objectives and agenda (WINS)

Workshop process and practicalities (Rachel Nott, event facilitator)

Introduction of participants (All)

09:45-10:30 **Session 1: Understanding the Insider Threat and its Relevance to Cyber Security at Nuclear Facilities**

Key issues

- What is a cyber insider threat? What are cyber insider threat characteristics?
- How do physical and cyber insider threats differ? What do they have in common?
- Why is the cyber insider threat relevant to the nuclear industry? What features make the nuclear industry more or less attractive to becoming a target of cyber insider threats?

Presentation on cyber insider threats (attributes and characteristics)

Case studies on intentional and unintentional cyber insider threats

10:30-10:45 **Coffee Break**

10:45-13:00 **Presentation** on social and behavioural sciences in support of insider threats identification and characterization

Presentation on a Nuclear operator approach to identify credible cyber insider threats

Break-out groups to identify and discuss scenarios of concern at nuclear facilities

13:00-14:00 **Lunch**

14:00-15:30 **Session 2: Developing a National Strategy to Mitigate the Cyber Insider Risk**

Key issues

- What are the main elements of a strategy to mitigate the cyber insider threat risk?
- What stakeholders are involved? Are we satisfied of their involvement, cooperation and coordination?
- What international and national guidance documents exist to support the mitigation of the cyber insider threat?

Presentation on Developing a national strategy to address the cyber insider risk in the nuclear sector

Discussion to identify relevant stakeholders and assess their current contribution to risk reduction

Presentation on Developing an Industry-level approach to the cyber insider risk

15:30-15:45 **Coffee Break**

15:45-17:15 **Presentation** on IAEA activities in the area of cyber insider mitigation

Discussion on the role of INFCIRC/908 and other international initiatives

Presentation on Learning from other industries/critical infrastructures

17:15-17:30 **Wrap up of Day 1** – What have we learned?

17:30-19:00 **Workshop Reception – Networking opportunities**

19:00 **End of Day 1**

Day 2 – Wednesday 04 September 2024

09:00-09:30 **Summary of Day 1 and Objectives of Day 2**

09:30-10:30 **Session 3: Designing and Implementing a Cyber Insider Threat Mitigation Programme**

Key issues

- What are the elements of a state-of-the-art cyber insider threat mitigation programme?
- How does vetting and human reliability programmes contribute to reducing the cyber insider threat risk?
- How do you embark all employees and contractors into your cyber insider threat mitigation efforts? How do you address specific needs at all stages of the employee lifecycle?

Presentation on the main elements of a cyber insider threat mitigation programme

Presentation on a nuclear operator experience Designing and Implementing a Cyber Insider Threat Mitigation Programme

10:30-10:45 **Coffee Break**

10:45-13:00 **Session 3 (Continue)**

Presentation on developing a comprehensive cyber security culture, including facilitating the reporting of serious concerns

Presentation on addressing the cyber insider threat in the supply chain

Break-out groups to identify and discuss challenges and opportunities when designing and implementing a Cyber Insider Threat Mitigation Programme

13:00-14:00 **Lunch**

14:00-15:30 **Session 4: Detecting and Responding to a Security Incident involving a Cyber Insider**

Key issues

- What are potential indicators of undesired behaviour or precursors of malicious activity?
- What are good practices for a timely assessment and response to cyber insider actions?
- What is the role of technology, in particular artificial intelligence, in supporting the detection of and response to incidents involving a cyber insider threat?

Case Study on detecting anomalous insider activities and conducting a timely assessment

Presentation on a nuclear operator experience detecting and identifying cyber insider threats

Discussion on challenges identifying red flags and effectively responding to a cyber insider threat

15:30-15:45 **Coffee Break**

15:45-17:15 **Vendor session**

- The role of technologies in supporting detecting cyber insider threats
- Artificial Intelligence in support of insider detection

17:15-17:30 **Wrap up of Day 2** – What have we learned? What remains to be addressed?

17:30 **End of Day 1**

Day 3 – Thursday 05 September 2024

09:00-09:30 **Summary of Day 2 and Objectives of Day 3**

09:30-10:30 **Session 5: Measuring the Effectiveness of a Cyber Insider Threat Mitigation Programme**

Key issues

- How can cyber insider threat mitigation programmes be measured for their effectiveness?
- What leading and lagging indicators characterise a cyber insider threat mitigation programme?
- How can we integrate the cyber insider threat risk into the overall risk management approach?

Presentation on measuring the effectiveness of a cyber insider threat mitigation programme

Presentation on a nuclear operator experience reporting on the performance of its cyber insider threat mitigation programme

10:30-10:45 **Coffee Break**

10:45-12:30 **Session 5 (Continue)**

Presentation on developing an integrated risk management approach

Break-out groups to identify and discuss indicators characterising a cyber insider threat mitigation programme and its performance

12:30-13:30 **Lunch**

13:30-14:30 **Key findings, main take-aways and next steps**

14:30-15:00 **Conclusion session**

- Evaluation session
- Closing remarks

15:00 **End of the workshop**