CYBER NUCLEAR FORUM SPRING 2025 MEETING

Online. Thursday 27 March 2025

Summary

On Thursday, 27 March 2025, the Cyber Nuclear Forum (CNF) organised an online meeting to review the latest CNF developments and discuss future plans. The meeting also featured presentations by invited experts on topics such as governance arrangements for cybersecurity, supply chain security, and lessons learned from a major cybersecurity exercise.

The meeting was attended by 28 individuals from 20 organizations and was moderated by Anno Keizer (Urenco Netherlands), Chair of the CNF, and Todd Warnell (Bruce Power, Canada), Vice-Chair of the CNF Steering Committee. Attendance was limited to Forum members and invited guests. The meeting was not recorded.

CNF Developments

After welcoming the participants, Mr. Keizer thanked the CNF 2025 sponsors (Bruce Power, NEI, and Urenco), emphasizing that the CNF relies on sufficient financial support to operate effectively. He encouraged participating organisations to consider joining the pool of CNF funders. Mr. Keizer introduced the Steering Committee members and summarized developments since the last in-person meeting in June 2024 in Toronto, Canada. He highlighted the range of new ideas and plans and encouraged members to take an active role in Forum activities.

Expert Presentations

Managing Supply Chain Cyber Security Risks by Brian Moss (Bruce Power, Canada)

The session began with two polls to gather participants' perspectives on supply chain risks. First, attendees were asked whether they felt confident that nuclear facilities were taking necessary measures to address these risks—80% expressed confidence. Participants were then asked to identify the main security risks in the supply chain. Key concerns included:

- Unaware workforce / unwitting insider
- Supplier trustworthiness
- Suppliers lacking cybersecurity awareness
- Hidden/unnoticed malware
- Product validation (ensuring the product is uncompromised)
- Fraudulent items or embedded malware due to foreign ownership, control, or interest (FOCI)
- Limited trusted sourcing options
- Embedded cross-national components
- The complexity and opaqueness of IT/OT and adjacent supply chains

Mr. Moss discussed risks posed by suppliers, products, and services throughout the supply chain. He presented options for managing third-party risks (e.g., Business Interruption Review, Trusted Digital Communication, Information Sharing) and highlighted specific cybersecurity concerns. He also introduced IAEA guidance TDL-011 on 'Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain' and NIST best practices. He concluded with MITRE techniques for defending against supply chain threats.

Governance for Cyber Security at Bruce Power by Todd Warnell (Bruce Power, Canada)

Mr. Warnell began by reviewing the definition and key components of a Management System and stressed its role in ensuring standardized processes across an organization. He introduced the Canadian standard N286-12 on Management System Requirements for Nuclear Facilities and outlined its 12 principles. He explained how this standard underpins the Bruce Power Management System (BPMS), which helps the company meet its regulatory, statutory, and business obligations. Mr Warnell then described Bruce Power's Cyber & Information Security Program, emphasizing its layered structure, risk-based approach, and clearly defined security responsibilities. He concluded by detailing the performance oversight processes in place.

NATO Locked Shields - Preparing for large cyber incidents by Martijn Nuijens (NRG, the Netherlands)

Mr. Nuijens began by describing NRG's IT/cyber incident detection and escalation procedures. He listed activities used to prepare for incidents (e.g., tabletop exercises, penetration tests, red teaming) and introduced the NIST framework for incident response (NIST 800-61 Rev.2). The second part of the presentation was dedicated to the NATO Locked Shields 25 which is an annual exercise organised by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDOE) since 2010. Such exercises enable cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects. Over 4,000 individuals from 40+ countries are expected to participate in Locked Shield 2025. Mr. Nuijens concluded by sharing key lessons from the 2024 exercise, including the importance of assuming systems are already breached and managing staff stress during active incidents.

CNF Future Plans

Mr. Keizer and Mr. Warnell presented CNF's future plans, which include:

- Strengthening the membership selection process
- Expanding representation, especially in the Americas and Asia
- Building relationships with external entities (WNA, WANO, IAEA, etc.)
- Enhancing external communications
- Developing a formal CNF business plan

Mr. Keizer provided an update on the CNF Autumn 2025 meeting, scheduled for 7–10 September in Amsterdam, the Netherlands. It will include site visits to NRG's High Flux Reactor and the Pallas construction site.

Mr. Keizer then asked the participants to indicate which topics they would like to see covered during the Autumn meeting. Most quoted topics included the following ones:

- (Cyber) Insider Threats
- Artificial Intelligence
- Vulnerability Management
- Governance and Metrics
- Cybersecurity by Design
- Exercises

Mr. Keizer closed the meeting by thanking all participants and speakers for their contributions and discussions.