SAND2021-8137C

IAEA

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

Consultancy Meeting for Planning the Technical Meeting on Computer Security Regulations and Inspections Chair's Report

Date: June 22-24, 2021
Location: Virtual Meeting hosted by IAEA

IAEA Scientific Secretary: Trent Nelson (t.nelson@iaea.org)
Chairperson: Mr. Michael Rowland (mtrowla@sandia.gov)

1 BACKGROUND

Competent authorities in Member States have developed and established regulation for safety and security for nuclear facilities, radioactive materials and associated facilities. These competent authorities have implemented and conducted oversight activities (including inspection programs) to provide assurance that operators are complying with the regulations.

Increasing risks to computer security for nuclear security, demands that computer security regulation must also be developed and implemented. This regulation needs to ensure the protection of sensitive nuclear information and nuclear security functions. This regulation aims to protect the integrity, availability and confidentiality of information and functions of computer based systems having importance to nuclear security.

2 ATTENDEES

The meeting was attended by the following experts who had been involved in the developing and implementing Computer Security legislation, strategies, and computer security programmes.

Full Name	Country
Samo Tomažič	Slovenia (SNSA)
John Sladek	Canada (CNSC)
Daniel Coats	UK (ONR)
Jean-Luc Trolle	France
Laurent Moutenot	France (EDF)
Wolfram Rother	Germany (BMU)
Rick Mogavero	USA (NEI)
Bill Gross	USA (NEI)
Nathan Faith	USA (Exelon)

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

Full Name	Country
Mike Rowland	USA (SNL)
Fred Morris	USA (PNNL-ORS)
Perry Pederson	USA (PNNL)
Jennifer Marek	USA (PNNL)
Jim Beardsley	USA (NRC)
Charlotte Mae East	Australia (ANSTO)
Hitham Shaheen	Egypt
Toni Huhtakangas	Finland (STUK)
Kookheui Kwon	Korea (KINAC)
Renato Luiz	Brazil

3 SCOPE AND OBJECTIVES

The objective of the event was to bring together leading professionals including regulators, operators, stakeholders, and subject-matter experts to:

1. Identify and discuss successes, lessons learned, and challenges in developing and implementing computer security regulations and conduct of regulatory functions (including inspections),
2. Identify key topics and sessions for the Technical Meeting (TM) on Computer Security Regulations and Inspections scheduled for 30 May to 3 June 2022 in Berlin, Germany.
3. Identify potential speakers and chairs for each of these topics and sessions.

4 RESULTS FROM THE MEETING

All objectives were achieved during the CM. These are summarized as follows:

1. The successes detailed during the CM were:
   - Regulations had led to licensees developing a capacity to support computer security and increased protections.
   - The participants had diverse experiences and differing levels of maturity with regulations for computer security. The CM was an effective forum to capture the challenges and lessons learned from Member States.

The participants agreed to the key topics for the TM based upon the first two days of the meeting. The significant and new challenges associated with nuclear regulation and computer security are: (i) a national technical authority with a mandate for computer security creating a need for a coherent

national strategy and coordination among governmental organizations; (ii) development of new regulations either for NSS 13 and NSS 14, (iii) cross-cutting nature of computer security that impacts many regulatory functions, and (iv) tremendous reliance on competence of individuals to evaluate computer security arrangements at licensees especially for performance based regulations. Given these challenges, each challenge was associated with a specific day and topic during the TM.

2. The key topics and sessions agreed to are. (see Table-1 Section 6 for more details):
   - Overall Meeting Topics to fall under State, Legal, Regulatory Frameworks and Functions. Each day has one topic with two sessions for each topic.
   - Day 1 Topic – National Strategy for Regulations on Information and Computer Security for Nuclear Security.
   - Day 2 Topic – Regulatory Framework
   - Day 3 Topic – Regulatory Functions
   - Day 4 Topic – Establishing and Sustaining Capacity for Competent Authorities and Regulatory Functions.

3. Potential Speakers and chairs were identified, but will require time to confirm due to uncertainty with COVID-19 international travel restrictions and approvals to attend the June 2022 TM.
   - Call for Abstracts will be needed for specific sessions. This call will be an objective of the upcoming consultancy meeting in November 2021.

5 MEETING NOTES

22-June-2021 (Day1):

The scientific secretary for the meeting, Mr. Trent Nelson, opened up the CM and presented the focus of the CM with the core objectives. This activity will embark on the establishment of computer security law, regulations, requirement and recommendations for Member States (MS) to establish computer security strategies and programs. Additionally, Mr. Nelson explained how the CMs and TM will form the bases for identifying future IAEA effort in regulations and regulatory functions having importance to computer security for nuclear security.

Mr. Nelson discussed the potential future activities of the IAEA.

1. Non-serial or TecDoc publication
   a. Awareness of State Level Computer Security Strategies (legislation)
   b. Understand approaches in development of computer security regulations

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

2. Workshops and/or Training Courses
3. Sustainability efforts/Member State support, upon request; This includes inspections, national exercises, and assessments).

IAEA NSS documents primary objective is to aid in the development of a National level computer security program, which is included across all the computer security guidance documents that contains all the building blocks to develop computer security programs.

Mr. Fred Morris, PNNL (USA), presented on the legislative and regulatory frameworks for computer security as it applies to nuclear security and defined what we need to do: Build computer security into national nuclear security regimes. The key concepts and challenges discussed were:

- Prescriptive vs. Performance based approach, or a combination of both. This was an important theme and area of discussions for most of the CM.
- How to build computer security into a national security strategy.

The timeliness of regulatory oversight was a key question to Mr. Morris. The general consensus was that technical aspects of computer security require closer to real-time assurance; whereas programmatic aspects could be monthly or quarterly.

Mr. Samo Tomazic, SNSA (Slovenia) presented on the regulatory and legal aspects important to nuclear security in Slovenia. The key concepts and challenges discussed were:

- A separate National Technical Authority for Cyber and/or Information Security. Established by a legislative act/law with a mandate to protect critical infrastructure from cyber-attacks. This was a key theme of nearly all further discussions.
- Interfaces between organizations within a Member State, as well as its licensees is critical to ensure that protections and response are effective in reducing risk to nuclear security to an acceptable level.
- Reporting of cyber-attacks and non-compliances is important in providing the necessary data to guide improvements of computer security programmes.

Mr. John Sladek , CSNC (Canada), presented on current status of Canadian efforts. Mr. Sladek discussed the following:

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

- The update of Nuclear Security Regulations, focused on detection and response; adopting a preference for a protective rather than a preventive approach.
- The update of the Design Basis Threat (DBT) to include a more detailed description of the adversary's cyber-skills.
- Update of the Canadian National Standard N290.7-14 to include Defensive Architectures.

The above updates to Nuclear Security regulation to migrate from preventive to protective approaches, as well as regulatory instruments that are more "cyber-aware" is a key common theme from those experts having established computer security programmes for nuclear facilities.

Mr. Toni Huhtakangas, STUK (Finland), outlined the interfaces and relationships within the Finnish Government and STUK. A key common element was:

- Finland has a national technical authority for cyber and/or information security.

Mr. Huhtakangas discussed the strong reliance of IAEA publications in development of STUK regulatory guides.

Renato Luiz, CNEN (Brazil), outlined Brazil's nuclear security regime. Key common elements with the other speakers were:

- Other government degrees on Information Protection (national) and Cybersecurity (national*)*

Key challenges for CNENB detailed were:

- Inspections are one of the biggest challenges.
- Need to build capacity in Nuclear Cyber Security and support Cyber Security Culture at Licensees.
- Exercises

Day 1 Summary:

The key elements of Day 1 discussions were:

1. Large reliance on IAEA publications and publicly available National Regulations (e.g. US NRC)
2. Many Member States have a national Technical Authority for Cybersecurity. State Level Strategy and Capacity plays an important role. Interfaces and capacity efforts are necessary.

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

3. Demand for greater support and international information exchange on Regulations and Inspections.
4. Potential Topics for TM and updated during Day 3. The final result of these discussions is listed in Table-1 of Section 6.

23-June-2021 (Day2):

Mr. Michael Rowland, SNL (USA), opened with the summary of Day 1 of the CM. He indicated that the TM Scope could be quite large, and future CM discussions will likely need to limit this scope. Mr. Nelson indicated that the next IAEA Computer Security Conference is tentatively scheduled for June 2023

Ms. Charlotte East, ARPANSA (Australia), discussed the Australian Nuclear Security Regime. Key common elements were:

- Reliance on IAEA to support regulatory development.
- Capacity building activities, with IAEA seen as a key organization to support these activities.

New elements were:

- Importance of IAEA IPPAS missions in driving advancements and improvements in computer security regulations.
- Use of Maturity model concepts to evaluate programmatic advancement and sophistication for computer security.
- Demand for information and computer security support in nuclear security domains other than nuclear material and nuclear facilities.

Mr. Kookheui Kwon, KINAC (ROK), discussed the Republic of Korea's Nuclear Security Regime. Key common elements were:

- Reliance on IAEA and US NRC guides to support regulatory development.

New elements were:

- Timelines for important regulatory activities (every three years):
    - Threat Assessment
    - Regulatory Development and Updates
    - Inspections

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

    - Exercises
- Challenges in Risk Management and prioritization of computer security activities (i.e., what assets/systems or processes to focus on?).

Mr. Dan Coats, ONR (UK), discussed the UK's approach and design of computer security regulations. Key common areas included:

- Reliance on IAEA Guides
- Maturity model concepts
- Risk Management and Threat Assessment
- Performance (e.g. outcomes focused) vs. Prescriptive based regulation.

New elements were:

- Hierarchical approach; Security Assessment Principles to Cyber Security Principles, to Technical Assessment Guides.
  Need for example use cases.

Mr. Perry Pederson, PNNL (USA), discussed Metrics for Measuring computer security effectiveness. The common elements were:

- Performance vs. Prescriptive Based regulation
- IAEA support for capacity building/sustainability.

New Elements were:

- Types of Metrics (1) Nominal; (2) Ordinal; (3) Interval; (4) Ratio
- Demands on regulator competence and capability for evaluating performance based approaches.
- Testing, Verification and Validation, and pen testing.

Mr. Jim Beardsley, US NRC (USA), presented on US Nuclear Power Plant Cyber Security Rule (Regulation) Implementation Lessons Learned 2009-2021. The common elements were:

- Regulations for NPPs needs to be optimized and further refined. NPP regulation had been established and inspections for all reactors completed. Results captured in Self-Assessment reports - ML19175A210/ ML19175A211
- Risk Management, threat assessment, and prioritization were very challenging.

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

- Performance based approaches demand an advanced level of cybersecurity expertise.
- Capacity and sustainability efforts are necessary.

Mr. Rich Mogavero, NEI (USA), presented on the same topic as Mr. Beardsley with focus on implementation area. Key common elements

- Regulations for NPPs needs to be optimized and further refined/evolved.
- Performance vs. Prescriptive based approaches.
- Risk Management and Threat Assessment
- Inspections, ongoing monitoring and assessments, and exercises are key areas for improvement.
- Training and awareness.

Key new areas were:

- Need to advance DiD protective strategies
  - DCSA
  - Detect, Delay, Respond to, Recover From.
  - Protective Measures concept that minimizes or eliminates the adversary's access to one of the five attack pathways.

24-June-2021 (Day 3)

Mr. Nelson and Mr. Rowland summarized the results of Days 1 and 2, and discussed potential TM topics and sessions. The results of the Day 3 discussions are found in Table 1 of Section 6.

6 RECOMMENDATIONS FOR PLENARY SESSIONS, TECHNICAL SESSIONS, AND WORKSHOPS

The proposed Topics and Sessions are listed in Table 1 below.

Date	Topic	Session	Action
30 May 2021	Introductions	N/A	Trent Nelson – IAEA and Host Speakers.
	National Bases and Strategies	International/National Framework and Bases	Trent Nelson – IAEA Legal Conference for potential Chair.

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

Date	Topic	Session	Action
			Participants – National Policy and Legislative Subject Matter Experts (e.g., BMU, ITU, NRCan)
31 May 2021		Regulatory Bases for Information and Computer Security for Nuclear Security.	Wolfram – investigate ENSRA participation. Participants – newcomer countries, mature NPP countries, other domains of nuclear security (NSS 14, NSS15)
	Regulatory Framework	Specificities and Constraints of particular Nuclear Security Domains[1]	Chair – needs detailed knowledge of all three Nuclear Security domains. Participants – Subject Matter Experts involved in nuclear regulations or national requirements of one or more domains.
		Performance vs. Prescriptive based approaches	Chair – needs detailed knowledge of international and national approaches to regulation. Next CM – develop Call for abstracts as this is an area of high concern.
1 June 2021	Regulatory Functions	Updating and optimization of regulatory activities	Chair –NPP regulator with a mature process for update to regulation (e.g., KINAC)

[1] This Session discusses specific requirements and constraints associated with information and computer security for nuclear security. For example, how does NSS 14 domain differ from the NSS 13 domain (e.g., capability and capacity of licensees to dedicate resources to computer security).

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

Date	Topic	Session	Action
			Next CM – develop call for abstracts and invited speakers. Participants need to be either updating their programmes or have updated.
		Licensing and Oversight Activities	Chair – RF or Asia Trent Nelson – reach out to WANO, FANR, DOE-ORS, and IAEA-MAFA (w.r.t. IPPAS)
2 June 2021	Development and Sustaining Regulator and licensee Capacity.	Development of Competence (individual) and Capability (process/organization) at competent authorities	Chair – France Wolfram – BMU (Human Resources) Trent Nelson - NSGC Member (cross-cutting)
		Sustainability and R&D	Chair – TBD NPP Operator Regulator TSO/National Labs. Next CM – develop call for abstracts and invited speakers.
3-June 2021	Report and Chairs Panel Discussion and IAEA Closing.		

Table 1 – Sessions and Topics of TM (post CM1)

INTERNATIONAL ATOMIC ENERGY AGENCY

Chairperson's Report from Consultancy Meeting on Computer Security Regulations and Inspections

Planning Activities for the Technical Meeting

7 CONCLUDING REMARKS AND NEXT STEPS

The next CM will be focused on further refining the session topics, identifying and confirming chairpersons for each session, and developing the call for abstracts for those sessions indicated in Table 1 above.

8 ATTACHMENTS

Attached are the following documents:

1. Agenda.
2. Speaker PPTs are found on NUSEC: https://nusec.iaea.org/portal/User-Groups/Computer-Information-Security/Technical-Meetings/TM-Regulations/CM-Planning-2021 .
3. PowerPoint/rough notes on Days1 through 3 of the CM.