



Technical Meeting on Computer Security Regulations in Nuclear Security

Hosted by the

Government of Germany

through the

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety and BMU

Berlin, Germany

30 May - 3 June 2022

Ref. No.: EVT2102758

Information Sheet

Introduction

Computer security continues to grow in importance as a component of nuclear security as computer-based systems are integrated in nuclear safety, nuclear security, and operational aspects of nuclear and other radioactive material facilities and operations. The increasing computer security threats to the nuclear industry, necessitates the development and implementation of regulations at State level, in order to ensure the protection of nuclear information and computer-based systems used for operations, and in order to maintain the integrity, availability and confidentiality of information for nuclear facilities and materials. The IAEA's Division of Nuclear Security has recognized this need within Member States and the need to develop computer security inspection guides to support States in strengthening their nuclear security regimes. The IAEA has convened numerous events with elements focused either in whole, or in part, on computer security regulation and conducting computer security assessments. Within these, the challenges associated with Computer Security Programme (CSP) assessment and the need for additional guidance in regulatory review have been recurring themes. Member States have also developed regulations for safety and security for nuclear facilities, radioactive materials and associated facilities, as well as inspection programmes for compliance.

Objectives

The objective of the event is to serve as a forum for enhancing interaction and information exchange among international experts for computer security regulations and inspection programmes for nuclear security. The meeting will allow for sharing strategies, practices, needs, and lessons learned on implementing computer security regulations to address computer security as an integral part of nuclear security.

Target Audience

The event aims to bring together leading professionals such as regulators, operators, computer security subject matter experts, and other stakeholders familiar with the implementation of computer security regulations, requirements and inspection programmes in computer security.

Working Language

English.

Expected Outputs

This international forum will allow for the collection of strategies, practices, needs, and lessons learned on implementing and inspecting against computer security regulations within nuclear security regimes. The results of the event will be a compilation of good practice and proposed computer security regulations and inspection requirements; including possible overarching implementation frameworks to address computer security gaps and challenges related to the assurance of computer security for nuclear security. It is expected that the results will be compiled during plenary and working group sessions.

Structure

The event programme will consist of:

- **Plenary Sessions** dedicated to invited speakers related to Computer Security Regulations and Inspections.
- **Working Group Sessions** dedicated to presentations by participants who have submitted an abstract related to the three working group sessions (defined below).
- **Technical Workshops** on Computer Security Strategy, Computer Security Regulations, Implementation of Computer Security Regulations, and an Open Forum for approved participants topics of interest.

The plenary and the working group sessions' organizers will be responsible for the overall scientific content, including selecting the speakers, organizing the technical and discussion sessions, as well as establishing the working groups.

Topics

The plenary sessions will cover the following thematic areas:

- **Initial Development and Implementation of State Computer Security Strategies and Associated Regulatory Frameworks**
Keywords: computer security regulation; computer security strategy; policy; procedures; computer security programs; computer security inspections; computer security.
- **Technical Considerations for Computer Security Regulations**
Keywords: core computer security regulations, computer security design; guidance; requirements, computer security.
- **Progressive Approaches to Enacting Computer Security Regulations**
Keywords: computer security regulatory framework; Baseline computer security model.
- **Implementing and Sustaining Inspection Programmes for Computer Security Regulations**
Keywords: computer security inspection programs, computer security assessments, verification and validation; regulatory compliance.

The working group sessions will cover some of the following topics:

- Identify approaches to computer security strategies.
- Development of key elements for computer security regulations.
- Identify assurance metrics and inspections techniques.

To support the working group sessions, three position papers have been developed on each topic (available [here](#).)

Participation and Registration

All persons wishing to participate in the event have to be designated by an IAEA Member State or should be members of organizations that have been invited to attend.

In order to be designated by an IAEA Member State, participants are requested to send the **Participation Form (Form A)** to their competent national authority (e.g. Ministry of Foreign Affairs, Permanent Mission to the IAEA or National Atomic Energy Authority) for onward transmission to the IAEA by **22 March 2022**. Participants who are members of an organization invited to attend are requested to send the **Participation Form (Form A)** through their organization to the IAEA by above deadline.

Selected participants will be informed in due course on the procedures to be followed with regard to administrative and financial matters.

Participants are hereby informed that the personal data they submit will be processed in line with the [Agency's Personal Data and Privacy Policy](#) and is collected solely for the purpose(s) of reviewing and assessing the application and to complete logistical arrangements where required. Further information can be found in the [Data Processing Notice](#) concerning IAEA InTouch+ platform.

Papers and Presentations

The IAEA encourages participants to give presentations on the work of their respective institutions that falls under the working group sessions topics listed above.

Participants who wish to give presentations are requested to submit an abstract of their work. The abstract will be reviewed as part of the selection process. The abstract should be in A4 page format, should extend to no more than two pages (including figures and tables) and should not exceed 500 words. The abstract should be submitted through the Division of Nuclear Security, Information and Computer Security unit Email: NucSecCyber@iaea.org, and cc: Mr Trent Nelson, Scientific Secretary of the event, Email: T.Nelson@iaea.org, with the subject line "Computer Security Regulations Technical Meeting Abstract" by **22 February 2022**. Authors will be notified of the acceptance of their proposed presentations by **22 March 2022**.

In addition, participants have to submit the abstract together with the Participation Form (Form A) and the attached **Form for Submission of a Paper (Form B)** to their competent national authority (e.g. Ministry of Foreign Affairs, Permanent Mission to the IAEA or National Atomic Energy Authority) or their organization for onward transmission to the IAEA not later than **22 February 2022**.

Expenditures and Grants

No registration fee is charged to participants.

The IAEA is generally not in a position to bear the travel and other costs of participants in the event. The IAEA has, however, limited funds at its disposal to help meet the cost of attendance of certain participants. Upon specific request, such assistance may be offered to normally one participant per country, provided that, in the IAEA's view, the participant will make an important contribution to the event.

The application for financial support should be made using the **Grant Application Form (Form C)** which has to be stamped, signed and submitted by the competent national authority to the IAEA together with the **Participation Form (Form A)** by **22 March 2022**.

Visas

Participants who require a visa to enter Germany should submit the necessary application as soon as possible to the nearest diplomatic or consular representative of Germany.

Organization

Scientific Secretary

Mr Trent Nelson

Division of Nuclear Security
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 VIENNA
AUSTRIA

Tel.: +43 1 2600 26424

Fax: +43 1 26007

Email: T.Nelson@iaea.org

Administrative Secretary

Ms Camilla Semper

Division of Nuclear Security
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 VIENNA
AUSTRIA

Tel.: +43 1 2600 26635

Fax: +43 1 26007

Email: C.Semper@iaea.org

Subsequent correspondence on scientific matters should be sent to the Scientific Secretary and correspondence on other matters related to the event to the Administrative Secretary.