IAEA

Átomos para la paz y el desarrollo

الوكالة الدولية للطاقة الذرية
国 际 原 子 能 机 构
International Atomic Energy Agency
Agence internationale de l'énergie atomique
Международное агентство по атомной энергии
Organismo Internacional de Energía Atómica

Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Phone: (+43 1) 2600 • Fax: (+43 1) 26007
Email: Official.Mail@iaea.org • Internet: https://www.iaea.org

In reply please refer to: CN-313; EVT2102337
Dial directly to extension: (+43 1) 2600-24838

La Secretaría del Organismo Internacional de Energía Atómica (OIEA) saluda a los Estados Miembros del OIEA y tiene el honor de señalar a su atención la celebración de la **Conferencia Internacional sobre Seguridad Informática en el Mundo Nuclear: la Seguridad Física en aras de la Seguridad** (denominada en adelante el "evento"), que tendrá lugar en la Sede del OIEA en Viena (Austria) del **19 al 23 de junio de 2023**.

La finalidad del evento es ofrecer un foro para llevar a cabo presentaciones y debates sobre las actividades de seguridad física nuclear realizadas hasta la fecha en la esfera de la seguridad informática, a fin de examinar las nuevas tendencias en seguridad informática y las esferas que es preciso abordar, los posibles objetivos y prioridades de las actividades de seguridad física nuclear en relación con la seguridad informática, y la manera en que el OIEA y otras organizaciones internacionales pueden contribuir a la cooperación internacional dentro de esa esfera en auge.

El evento se celebrará en inglés.

Se invita a los Estados Miembros a difundir entre el público destinatario del evento el anuncio y la invitación a presentar memorias que se adjuntan y a designar a participantes mediante la plataforma InTouch+, conforme se indica en la sección H. Asimismo, se los alienta encarecidamente a seleccionar a mujeres cualificadas para que participen en el evento.

Por lo general, el OIEA no está en condiciones de sufragar los gastos de viaje ni de otra índole de los participantes en el evento. No obstante, dispone de fondos limitados para ayudar a cubrir los gastos de asistencia de determinados participantes. Esa ayuda puede ofrecerse normalmente, previa solicitud expresa, a un participante por país siempre que, en opinión del OIEA, la persona para la que se solicite pueda hacer una contribución importante al evento.

Tanto las solicitudes de asistencia financiera como la presentación de memorias pueden tenerse en cuenta únicamente si se reciben por conducto de InTouch+ dentro del plazo indicado en la sección O del anuncio y la invitación a presentar memorias.

Cabe señalar que el OIEA no paga ninguna indemnización por daños o pérdida de efectos personales. Tampoco proporciona seguro médico a los participantes en eventos. Por lo tanto, se recomienda que estas personas adopten las medidas necesarias para contratar por su cuenta un seguro privado. No obstante, el OIEA cubrirá mediante un seguro los accidentes y las enfermedades claramente relacionados con los servicios prestados al OIEA.

La Secretaría del Organismo Internacional de Energía Atómica aprovecha esta oportunidad para reiterar a los Estados Miembros del OIEA el testimonio de su distinguida consideración.

23 de junio de 2022

Documentación adjunta (en inglés únicamente):

Anuncio e invitación a presentar memorias

CN-313; EVT2102337

IAEA
International Atomic Energy Agency
Atoms for Peace and Development

International Conference on Computer Security in the Nuclear World: Security for Safety

IAEA Headquarters
Vienna, Austria

19–23 June 2023
Organized by the
International Atomic Energy Agency (IAEA)

Announcement and Call for Papers

A. Background

Nuclear material and facilities, other radioactive material and associated facilities, and materials outside of regulatory control all depend upon computer-based systems which play an essential role in all aspects of their safety and security through use, processing, storage, and transport of information. As technology advances, the use of computer-based systems in all areas of operations, including nuclear security and safety, is expected to increase.

Vulnerability to the theft and/or manipulation of sensitive information, including computer systems, to cyber-attack has become a significant issue across the digitally connected world. Incidents of cyber-attack on computer systems across all industries by adversaries with malicious intent, are common occurrence and are reported regularly in the media.

The nuclear industry is not immune and cyber-attacks are identified as means to target computer-based systems to carry out or facilitate malicious acts, whether directly or in combination with more conventional means such as physical access and insiders, potentially leading to theft, trafficking, or unacceptable radiological consequences. Nuclear Security Fundamentals specify the need for Nuclear Security Regimes to provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets such as computer-based systems.

Since the first International Conference on Cyber Security in the Nuclear World in 2015, perceptions and awareness of the growing threat of cyberattacks and their potential impact on nuclear security have evolved and the IAEA has produced Nuclear Security Series Guidance for States and established computer security as an integral element of nuclear security and safety. Considering the evolving nature of computer security, the IAEA is organizing an *International Conference on Computer Security in the Nuclear World: Security for Safety* from 19 to 23 June 2023.

B. Purpose and Objectives

The Conference will provide a global forum for competent authorities, operators, system and security integrators and vendors, and other relevant entities engaged in computer security activities related to nuclear security or safety to exchange information and foster international cooperation in computer security as an integral element of nuclear security and safety through:

- Presentations and discussion on nuclear security and safety efforts to date within the area of computer security (including achievements, experience gained, and lessons learned).
- Review of emerging trends in computer security and areas that need to be addressed.
- Consideration of possible objectives and priorities for nuclear security or safety efforts in computer security, and of how current approaches may evolve to address these and meet future challenges.
- Consideration of how the IAEA and other international organizations can contribute to international cooperation in this important area.

C. Themes and Topics

Main themes of the conference will be the following:

- State-level strategy and regulatory approaches for computer security in a nuclear security regime
  - State-level Strategy on evolving threat and legislative framework on Computer Security
  - Computer security regulations and regulatory requirements
  - Graded approach to national regulatory requirements for computer security
  - Harmonizing regulatory approaches on computer security across a nuclear security regime
  - Functions, competencies and effectiveness of competent authorities
  - Approaches to coordination among stakeholders involved in information and computer security
  - Good practices for notification, reporting and exchange of information between stakeholders on capabilities, infrastructures, requirements (e.g., performance-based or compliance-based), emergency preparedness, incident response…
- Computer Security Programme Implementation
  - Identification and management of facility functions and adversarial targets within facilities and activities
  - Characterization of current and emerging threats, hazards and risks related to computer security for nuclear safety and security
  - Practical approaches to risk assessment and to risk management (what is good enough) within a Computer Security program, including risk management framework for nuclear activities and use of Security Operation Centres (SOC)
  - Harmonizing approaches to computer security for nuclear security and safety (including emergency preparedness, incident response and forensics)
  - Detection, analysis, and response to computer security incidents
  - Establishing and maintaining a defensive computer security architecture and/or associated computer security measures, including potential integration of computer security by design
- Computer Security in Supply Chain Management
  - Ensuring computer security throughout the supply chain
  - Managing imbedded digital components/devices security of Original Equipment Manufacturer (OEM)
  - Complex supply chain relationship management (suppliers' supplier)
  - Risk ownership/management between computer security stakeholders
  - System/device/vendor qualifications (performances testing, assessment and certifications, graded approach)
  - Practical approaches of supply chain management, including requirements/assessment for vendors, hardware and software, life cycle management, and dedicated national or industry standards
- Practical implementation of Computer Security Assurance Activities
  - Conducting computer security assessments for nuclear safety and security
  - Preparation, conduct and evaluation of computer security exercises
  - Developing and maintaining a computer security training programme
  - Organizational procedures and practices to ensure computer security effectiveness
  - Measuring computer security compliance and effectiveness: methods and tools for "metrics" of qualitative and quantitative performance measures
- Sustainability of Computer Security
  - Effectiveness of established approaches for regularly evaluating information and computer security
  - Updating regulations to address the changing threat environment

- Safety and computer security interface
- Successes and challenges in digital transition of safety or security related analogue systems
- Lifecycle management of computer security within nuclear facilities and/or functions, including design improvements to mitigate emerging vulnerabilities
- Approaches to measure maturity of computer security programs
- Capability of a nuclear facility or organisation to be risk informed on Computer Security
- Reconciling long term and stable safety process and requirements with evolving digital technologies

- Human resources contribution to computer security
  - Characterising and resolving challenges in human resources development and retention, including appropriate balance between nuclear and computer security knowledge
  - Practical governance of computer security competencies and capabilities in nuclear activities, including team approaches that promote interdisciplinary collaboration and in recognition of intersecting IT/OT disciplines
  - Leadership on developing appropriate integration of computer security in the culture of nuclear industry, specifically through education and training
  - Assessment and mitigation of insider threat for computer security, including behavioural observation

- International cooperation in computer security for a nuclear security regime
  - Legally binding and non-legally binding international instruments on information and computer security
  - Example of computer security guidance and standards relevant in nuclear safety and security (e.g. International Atomic Energy Agency (IAEA), International Organizations for Standardization (ISO), International Electrotechnical Commission (IEC))
  - Raising awareness among international organizations, industry, civil society, and other stakeholders about computer security
  - International cooperation and assistance to enhance computer security

- Computer security of emerging digital technologies for nuclear activities
  - Impact and/or application of smart devices, automation tools, digital twins modelling, Artificial Intelligence (AI)/Machine Learning (ML), Information Technology (IT)/Operation Technology (OT) convergence, cloud computing, Internet of Thing (IoT), Block Chain, Quantum computing, etc.
  - Computer security considerations for new reactors designs (Small Modular Reactors, Micro Reactors, etc.)
  - Computer Security modelling and simulation activities
  - Effect of new working environment (e.g. Mobility) for employees/contractors on computer security

D. Structure

The conference will include:

- The opening plenary session, for all participants and invited speakers, with a key note speech and introduction to conference structure and demonstrations that will be performed during the entire week in parallel with the thematic sessions.

- Main sessions, dedicated to one of the conference themes, including keynote presentations. Each main session may conclude with a panel discussion.

- 6 simultaneous scientific and technical sessions following a high-level session, with topical presentations in order to stimulate discussion among conference participants.
- Poster sessions or interactive sessions, for exhibitors, or demonstrations of specific points. Sufficient time will be dedicated for discussion and interaction with participants.
- Vendor exhibit area to showcase computer security technologies and security activities.
- The Final Plenary Session on the last day of the conference, dedicated to the President's Report.

E. Expected Outcomes

The conference will significantly contribute to raising awareness of the threat of cyber-attacks, and their potential impact on nuclear security and safety, and mitigation techniques to protect computer-based systems and facilities. It will foster international cooperation as well as bring together experts and policy-makers to promote the exchange of information and experiences in protecting against cyber-attacks. Furthermore, it will help to improve and guide future IAEA activities in the area of information and computer security consistent with the Nuclear Security Plan 2022 – 2025.

Therefore, demonstrations performed during the conference will be, to the extent practical, designed for future viewing by States for further awareness raising purposes.

F. Target Audience

Similar to the 2015 International Conference on Computer Security which attracted over 700 participants from 92 Member States, the intended audience of CyberCon23 is expected to meet or exceed the previous conference, and include the following types of participants:

- National authorities of Member States (e.g. regulatory, research, security, law enforcement, and other involved in cyber security for nuclear safety and security within their State)
- Nuclear operators including facilities operators, transport operators, and owners of nuclear materials or other radioactive materials
- International and regional organizations and initiatives
- Relevant industry or technology organizations, institutes and companies

G. Call for Papers

Contributions on the topics listed in Section C are welcome as oral or poster presentations. All submissions, apart from invited papers, must present original work, which has not been published elsewhere.

G.1. Submission of Abstracts

Abstracts (approximately 150 to 200 words on one printed A4 page, may contain any charts, graphs, figures and references) should give enough information on the content of the proposed paper to enable the Programme Committee to evaluate it. Anyone wishing to present at the conference must submit an abstract in electronic format using the conference's file submission system (IAEA-INDICO), which is accessible from the conference web page (see Section Q). The abstract can be submitted through this system until **15 September 2022**. Specifications for the layout will be available on IAEA-INDICO. The system for electronic submission of abstracts, IAEA-INDICO, is the sole mechanism for submission of contributed abstracts. Authors are encouraged to submit abstracts as early as possible. The IAEA will not accept submissions via email.

In addition, authors must register online using the InTouch+ platform (see Section H). The online registration together with the auto-generated Participation Form (Form A) and Form for Submission of a Paper (Form B) must reach the IAEA no later than **15 October 2022**.

IMPORTANT: The Programme Committee will consider uploaded abstracts only if these two forms have been received by the IAEA through the established official channels (see Section H).

G.2. Acceptance of Abstracts

The Secretariat reserves the right to exclude abstracts that do not comply with its technical or scientific quality standards and that do not apply to one of the topics listed in Section C.

Authors will be informed by **18 November 2022** as to whether their submission has been accepted, either orally or as a poster, for presentation at the conference. Accepted abstracts will also be reproduced in an unedited electronic compilation of Abstracts which will be made available to all registered participants of the conference.

G.3 Submission of Full Papers

Authors of accepted abstracts will be requested to submit a full paper in Word format, of about **5 to 6** pages in length. A compilation of full papers (in electronic format) will be made available to participants at registration.

Full papers must also be submitted through the IAEA-INDICO file submission system in Word format. Submitting the paper in the indicated electronic format is mandatory. Specifications for the layout and electronic format of the contributed papers and for the preparation of posters will be made available on IAEA-INDICO.

The IAEA reserves the right to exclude papers that do not comply with its quality standards and those that do not apply to one of the topics outlined in Section C above and those that do not meet the expectations based on the information in the abstract.

The deadline for electronic submission of the full papers as Word files is **1 March 2023**. The IAEA will not accept papers submitted after the deadline.

The IAEA will notify authors of its completed review process of the full papers by **28 April 2023**. The deadline for revised papers to be submitted through IAEA-INDICO is **15 May 2023**.

IMPORTANT: The system for electronic submission of papers, IAEA-INDICO, is the sole mechanism for submission of contributed papers. Authors are encouraged to submit papers as early as possible. The IAEA will not accept submissions via email.

G.4 Proceedings

Following the conference, the IAEA will publish a summary report. The proceedings will be made available to read online.

H. Participation and Registration

All persons wishing to participate in the event must be designated by an IAEA Member State or should be member of an organization that has been invited to attend. The list of IAEA Member States and invited organizations is available on the event web page (see Section Q).

Registration through the InTouch+ platform:

1. Access the InTouch+ platform (https://intouchplus.iaea.org):

- Persons with an existing NUCLEUS account can **sign in here** with their username and password;
- Persons without an existing NUCLEUS account can **register here**.

2. Once signed in, prospective participants can use the InTouch+ platform to:

- Complete or update their personal details under 'Basic Profile' (if no financial support is requested) or under 'Complete Profile' (if financial support is requested) and upload the relevant supporting documents;
- Search for the relevant event (**EVT2102337**) under the 'My Eligible Events' tab;
- Select the Member State or invited organization they want to represent from the drop-down menu entitled 'Designating authority' (if an invited organization is not listed, please contact Conference.Contact-Point@iaea.org);
- If applicable, indicate whether a paper is being submitted and complete the relevant information;
- If applicable, indicate whether financial support is requested and complete the relevant information (this is not applicable to participants from invited organizations);
- Based on the data input, the InTouch+ platform will automatically generate Participation Form (Form A), Form for Submission of a Paper (Form B) and/or Grant Application Form (Form C);
- Submit their application.

Once submitted through the InTouch+ platform, the application together with the auto-generated form(s) will be transmitted automatically to the required authority for approval. If approved, the application together with the form(s) will automatically be sent to the IAEA through the online platform.

NOTE: Should prospective participants wish to submit a paper or request financial support, the application needs to be submitted by the specified deadlines (see section O).

For additional information on how to apply for an event, please refer to the InTouch+ Help page. Any other issues or queries related to InTouch+ can be sent to InTouchPlus.Contact-Point@iaea.org.

If it is not possible to submit the application through the InTouch+ platform, prospective participants are requested to contact the IAEA's Conference Services Section via email: Conference.Contact-Point@iaea.org.

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.

I. 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 conference. The IAEA has, however, limited funds at its disposal to help cover 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 conference.

If participants wish to apply for a grant, they should submit applications to the IAEA using the InTouch+ platform through their competent national authority (see Section H). Participants should ensure that applications for grants are:

1. Submitted by **15 October 2022**;
2. Accompanied by Grant Application Form (Form C); and
3. Accompanied by Participation Form (Form A).

Applications that do not comply with the above conditions cannot be considered.

Approved grants will be issued in the form of a lump sum payment that usually covers **only part of the cost of attendance**.

J. Distribution of Documents

A preliminary and final programme will be made available on the conference web page (see Section Q) prior to the start of the conference. The electronic compilation of abstracts will be accessible free of charge to participants registered for the conference.

K. Exhibitions

A limited amount of space will be available for commercial vendors' displays/exhibits during the conference. Interested parties should contact the Scientific Secretariat by email CyberCon23@iaea.org by **15 December 2022**.

L. Working Language

The working language of the conference will be English. All communications must be sent to the IAEA in English.

M. Venue and Accommodation

The conference will be held at the Vienna International Centre (VIC), where the IAEA's Headquarters are located. Participants are advised to arrive at Checkpoint 1/Gate 1 of the VIC one hour before the start

of the event on the first day in order to allow for timely registration. Participants will need to present an official photo identification document in order to be admitted to the VIC premises.

Participants must make their own travel and accommodation arrangements. Hotels offering a reduced rate for participants are listed on https://www.iaea.org/events. Please note that the IAEA is not in a position to assist participants with hotel bookings, nor can the IAEA assume responsibility for paying fees for cancellations, re-bookings and no-shows.

N. Visas

Participants who require a visa to enter Austria should submit the necessary application to the nearest diplomatic or consular representative of Austria as early as three months but not later than four weeks before they travel to Austria. Since Austria is a Schengen State, persons requiring a visa will have to apply for a Schengen visa. In States where Austria has no diplomatic mission, visas can be obtained from the consular authority of a Schengen Partner State representing Austria in the country in question.

For more information, please see the Austria Visa Information document available on https://www.iaea.org/events.

O. Key Deadlines and Dates

Submission of abstracts through IAEA-INDICO	**15 September 2022**
Submission of Form B (together with Form A) through the InTouch+ platform	**15 October 2022**
Submission of Form C (together with Form A) through the InTouch+ platform	**15 October 2022**
Notification of acceptance of abstracts for oral or poster presentation	**18 November 2022**
Electronic submission of full papers through IAEA-INDICO	**1 March 2023**
Notification of review of full papers	**28 April 2023**
Deadline for submission of revised full papers submitted through IAEA-INDICO	**15 May 2023**
Submission of Form A only (no paper submission, no grant request) through the InTouch+ platform	**No deadline**

P. Conference Secretariat

General Postal Address and Contact Details of the IAEA:

International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 VIENNA
AUSTRIA
Tel.: +43 1 2600
Fax: +43 1 2600 2007
Email: Official.Mail@iaea.org

Scientific Secretaries of the Conference:

Mr. Trent NELSON
Nuclear Safety and Security
Information Management
Tel.: +43 1 2600 / 26424
Fax: +43 1 26007
Email: CyberCon23@iaea.org

Mr. Christophe PILLEUX
Nuclear Safety and Security
Information Management
Tel.: +43 1 2600 / 26734
Fax: +43 1 26007
Email: CyberCon23@iaea.org

Administration and Organization:

Mr. Sanjai PADMANABHAN
Conference Services Section
Division of Conference and Document Services
Department of Management
IAEA-CN-313; EVT2102337
Tel.: +43 1 2600 / 24838
Email: Conference.Contact-Point@iaea.org

Subsequent correspondence on scientific matters should be sent to the Scientific Secretaries and correspondence on administrative matters to the IAEA's Conference Services Section.

Q. Conference Web Page

Please visit the IAEA conference https://www.iaea.org/events/cybercon23 regularly for new information regarding this conference.