CN-342; EVT2501008

IAEA

Atoms for Peace
and Development

International Conference on Computer Security in the Nuclear World: Securing the Future

IAEA Headquarters
Vienna, Austria

11–15 May 2026
Organized by the
International Atomic Energy Agency (IAEA)

Announcement and Call for Papers

A. Background

The safe and secure use of nuclear and other radioactive material, along with the operation of nuclear facilities and management of associated facilities and activities, rely heavily on information and computer systems. Additionally, these systems are crucial for the detection and recovery of materials outside of regulatory control.

The rapid pace of digital innovation and the growing reliance on computer-based systems in all areas of operations, including instrumentation and control systems for nuclear security and safety, highlight the need to discuss vulnerabilities. It is also essential to address the risk of cyber-attacks, theft and/or manipulation of sensitive information and computer-based systems.

The nuclear sector is not immune to cyber-attacks that can 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. These types of blended cyber-attacks can potentially lead to theft, illicit trafficking, or sabotage resulting in radiological consequences for people and the environment.

The IAEA's Nuclear Security Series publications stipulates the need for national nuclear security regimes to establish regulations and requirements to protect the confidentiality of sensitive information and to protect sensitive information assets such as computer-based systems.

Since the first *International Conference on Computer Security in the Nuclear World*, held in 2015, awareness of the growing threat of cyber-attacks and their potential impact on nuclear security has increased. The IAEA has also developed detailed nuclear security guidance to assist countries in their national efforts to establish computer security as an integral element of nuclear security. Considering the evolving nature of computer security, the IAEA organized the second *International Conference on Computer Security in the Nuclear World: Security for Safety* in June 2023 that emphasized the large scope of computer security for nuclear activities, including safety.

To build on the previous two conferences, the IAEA is now organizing the third *International Conference on Computer Security in the Nuclear World: Securing the Future (CyberCon26)* which will be held at the IAEA's Headquarters in Vienna, Austria from 11 to 15 May 2026.

B. Purpose and Objectives

The purpose of the conference is to provide a global forum for competent authorities, operators, system and security integrators, vendors, and other relevant entities engaged in computer security activities related to nuclear security or safety to share experiences, exchange information and foster international cooperation in computer security.

The conference seeks to achieve the following objectives:

- Explore computer security emerging technologies and discuss their potential impact on nuclear security, identifying areas of opportunity and/or risk.

- Identify priorities for computer security in nuclear security, and develop strategies to evolve current approaches to address emerging challenges and stay ahead of threats.
- Foster international cooperation in computer security for nuclear security by leveraging the expertise and resources of the IAEA and other organizations, and identifying opportunities for joint initiatives and capacity-building programmes.

Participants are encouraged not to discuss any sensitive nuclear security information.

C. Themes and Topics

The conference themes, associated topics and proposed technical sessions for each theme are the following:

1. Computer Security's Place in the Nuclear Sector and Beyond

Topics:

- What the nuclear world needs from computer security.
- Cooperation with the wider nuclear and non-nuclear community, e.g. aerospace, transport, medicine.
- Explaining the relevance of computer security to those who don't work in it.
- Achieving better mutual understanding on computer security challenges and solutions across the entire community, including non-technical stakeholders.
- Integrating computer security requirements with physical security, safety and emergency preparedness.
- Effective incident response, including personnel resources, equipment, and budget.
- Integrating computer security into national regulatory frameworks.
- International cooperation on computer security, leveraging partnerships, networks and communities of practice (e.g. IAEA Community of Practice).

Proposed Technical Sessions:

1. Breaking down silos: fostering collaboration and knowledge sharing.
2. Opportunities to adapt experience from non-nuclear sectors.
3. Building computer security into material detection, transport, use of radioactive sources and other activities.
4. Computer security explained to non-cyber nuclear professionals.
5. Effective incident response, and ensuring resource readiness.
6. How are we going to work together on advanced reactors, small modular reactors (SMRs) and microreactors?

2. Regulatory Frameworks

Topics:

- Aligning national regulatory frameworks with international standards and guidance.
- Enhancing computer security using inspections.

- Sharing experience and lessons learned to improve national regulatory frameworks.
- Writing regulation that anticipates innovations and new technologies e.g., artificial intelligence (AI), SMRs.
- How to address nuclear-specific and general supply chain risks in regulation.
- Creating adaptable and resilient security policies for emerging threats.

Proposed Technical Sessions:

1. Practical use of international standards and guidance to enhance computer security
2. Regulatory frameworks – lessons learned including from outside the nuclear sector.
3. Inspections – how to reduce risk and gain assurance.
4. How regulatory frameworks can help reduce supply chain risk.
5. How regulatory frameworks are written to anticipate emerging threats and new technologies and evolve as necessary.

3. Capacity & Competency Management for Computer Security and Sustainability

Topics:

- Addressing nuclear computer security competency and gaps through training, workforce development and enhancing knowledge management.
- Modelling the size and nature of the workforce needed for computer security.
- Attracting and retaining computer security talent in a competitive market.
- Improving incident response through computer security exercises and training.
- Building partnerships between government, industry and academia through communities of practice.
- Creating a security culture in the workforce across all nuclear disciplines.

Proposed Technical Sessions:

1. Attracting and retaining skilled computer security staff – the skill shortage.
2. Continuing professional development and education in computer security.
3. Working together to solve the shortage: academia, industry, and government.
4. Embedding a culture of security – and that includes everyone!
5. Enhancing computer security through exercises and drills.

4. Threats and Risks

Topics:

- Using continuous risk management to identify, assess, and mitigate computer security risks.
- Developing practical indicators to detect cyber-attacks, using forensics to investigate and respond to security incidents.
- Creating and using national threat statements and DBTs (Design Basis Threat) – what does "beyond DBT" mean for computer security.
- Collaborating and information-sharing to improve collective computer security.
  - Using threat intelligence and predictive analytics to prepare for cyber-attacks.
  - Protecting against malware, etc., being delivered via the supply chain.
  - Employing computer security to identify and address the insider.

- Defending against cyber-enabled sabotage and theft.

Proposed Technical Sessions:

1. Practical risk management strategies, the role of the DBT.
2. Detect, respond and recover: lessons learned from when "protect" fails.
3. Threat intelligence in action: informing risk management decisions.
4. Managing risks and mitigating vulnerabilities in the supply chain.
5. Insider threats and cyber-enabled sabotage: balancing human and computer security.

5. Computer Security by Design

Topics:

- Addressing computer security at every stage in the system lifecycle and facility lifetime.
- Addressing the impact of advanced reactor designs on computer security.
- Implementing security-by-design, to avoid computer security being an add-on.
- Designing and implementing defensive security architectures that defend functions.
- Implementing zero-trust architectures – practical examples in nuclear systems.
- Creating and assuring secure software, hardware and systems.
- Creating secure supply chains, both domestically and internationally.
- Addressing the human elements in computer security, including human error.
- Designing architectures to detect and respond to computer security incidents.
- Integrating computer security with physical security, safety and emergency preparedness.

Proposed Technical Sessions:

1. Secure-by-design in practice – integrating computer security.
2. Building a fortress: effective controls, security architecture, and defensive strategies.
3. Using complex technology, e.g. software-based systems, Field-Programmable Gate Arrays.
4. Mitigating risks of human error and social engineering.
5. Safety/Security interface – practical steps for safety/security to work together.

6. Computer Security Impact of New Digital Technologies

Topics:

- Using new digital technologies in the nuclear sector, such as wireless, drones, next-generation encryption and post-quantum cryptography, AI, machine learning, automation and robots, while mitigating risks.
- Learning from non-nuclear industries that have successfully used new digital technologies and applying these lessons to the nuclear sector.
- The value of frameworks for the use of technology.
- Using innovative digital technologies to enhance security and safety.
- Breaking the security boundary by implementing secure remote operation, remote maintenance, and cloud computing in nuclear environments.
- Practical examples of managing the trade-offs between innovation and security in the digital transformation of nuclear infrastructure.

Proposed Technical Sessions:

1. Balancing innovation and security: trade-offs in digital transformation.
2. Secure use of smart sensors, cloud, remote operations and maintenance, and autonomous operations.
3. Applying non-nuclear industry innovations to nuclear computer security.
4. Harnessing the benefits of AI while mitigating cyber risks.

D. Structure

The conference is designed to cover the three pillars of nuclear security – prevention of, detection of and response to – through:

- A cyber-threat scenario with system level vulnerabilities, including investigation and analysis activities to identify security gaps and mitigation techniques for the establishment of computer security programmes and controls to protect against current and emerging threats.
- Presentations and engaging discussion on computer security prevention, detection and response capabilities against cyber-attacks (including achievements, experience gained, and lessons learned) through the conference themes.

The conference will include:

- The opening plenary session, for all participants and invited speakers, with a keynote speech and introduction to conference structure and demonstrations that will address the three key pillars on prevention, detection and response.
- The conference themes will flow throughout the conference including keynote speakers and panel sessions in support of computer security for nuclear security.
- Scientific and technical sessions with topical presentations in order to stimulate discussion among conference participants.
- Technical posters will be presented through flash presentation sessions.
- Side events on specific topics.
- Vendor exhibit area where computer security technologies, products, and security activities will be showcased.
- 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 and improve understanding on building, developing and improving computer security capabilities in order to prevent, detect and respond to cyber-attacks, considering their potential impact on nuclear security and safety. 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 IAEA's Nuclear Security Plan, as applicable.

F. Target Audience

The conference is open to a broad range of experts and organizations from Member States, encompassing regulators, research institutions, security, law enforcement, and other entities involved in computer security for nuclear security within their respective countries. Additionally, nuclear operators, including facilities operators, transport operators, and owners of nuclear material and other radioactive material, are also invited to participate. The conference welcomes international, regional, and non-governmental organizations, as well as relevant industry or technology organizations, institutes, and companies. Furthermore, individuals and organizations from countries embarking on nuclear power are also encouraged to attend. The IAEA particularly encourages the participation of women, early career professionals, and individuals from developing countries to ensure a diverse and inclusive representation.

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 from **10th June 2025** until **30th September 2025**. 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 **15th October 2025**.

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 **17th November 2025** 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 **1st March 2026**. 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 **27th March 2026**. The deadline for revised papers to be submitted through IAEA-INDICO is **17th April 2026**.

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):

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

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

1. 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;
2. Search for the relevant event (**EVT2501008**) under the 'My Eligible Events' tab;
3. 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);
4. If applicable, indicate whether a paper is being submitted and complete the relevant information;
5. If applicable, indicate whether financial support is requested and complete the relevant information (this is not applicable to participants from invited organizations);
6. 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);
7. 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 **15th October 2025**;
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 CyberCon26@iaea.org by **15 December 2025**.

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	**30 September 2025**
Submission of Form B (together with Form A) through the InTouch+ platform	**15 October 2025**
Submission of Form C (together with Form A) through the InTouch+ platform	**15 October 2025**
Notification of acceptance of abstracts for oral or poster presentation	**17 November 2025**
Electronic submission of full papers through IAEA-INDICO	**1st March 2026**
Notification of review of full papers	**27 March 2026**
Deadline for submission of revised full papers submitted through IAEA-INDICO	**17 April 2026**
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 Secretary of the Conference:

Mr. Trent Nelson
Division of Nuclear Security
Department of Nuclear Safety and Security
Tel.: +43 1 2600 26424
Fax: +43 1 26007
Email: CyberCon26@iaea.org

Administration and Organization:

Mr. Sanjai PADMANABHAN
Conference Services Section
Division of Conference and Document Services
Department of Management
IAEA-CN-342; EVT2501008
Tel.: +43 1 2600 24838
Email: Conference.Contact-Point@iaea.org

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

Q. Conference Web Page

Please visit the IAEA conference website regularly for new information regarding this conference.