KEY DEADLINES

30 January 2015	Submission of the synopses (*including Form B*)
30 January 2015	Submission of Grant Application Form (*Form C*)
27 February 2015	Notification of acceptance of synopses
02 May 2015	Submission of full paper (*only upon request by the IAEA*)

Any prospective participant not intending to present a paper should submit the Participation Form (*Form A*) through the appropriate authority as soon as possible.

SUBMISSION OF PAPERS

Extended synopses and full papers must be submitted through the IAEA-INDICO file submission system. Instructions will be available as of September 2014 at:

www-pub.iaea.org/iaeameetings/46530/CompSec2015

REGISTRATION

No registration fee.

LANGUAGE

English.

IAEA CONTACT PERSONS

Scientific Secretary
Mr Donald D. Dudenhoeffer
Division of Nuclear Security
Department of Nuclear Safety and Security
Tel.: +43 1 2600 26424
Fax: +43 1 2600 7
Email: CompSec2015@iaea.org

Participation, grant application and administrative matters:
Ms Julie Zellinger
Division of Conference and Document Services
Department of Management
Tel.: +43 1 2600 21321
Fax: +43 1 2600 7
Email: J.Zellinger@iaea.org

CONFERENCE WEBSITE

http://www-pub.iaea.org/iaeameetings/46530/
International-Conference-on-Computer-Security-in-a-
Nuclear-World-Expert-Discussion-and-Exchange

Please include reference number IAEA-CN-228 in all communications.

Organized by the

IAEA
International Atomic Energy Agency

in cooperation with

Interpol — International Telecommunication Union — unicri United Nations Interregional Crime and Justice Research Institute — IEC International Electrotechnical Commission

International Conference on
Computer Security in a Nuclear World:
Expert Discussion and Exchange

1–5 June 2015
Vienna, Austria

Organized by the

IAEA
International Atomic Energy Agency

15-00371

CN-228

BACKGROUND

Computer security involves the protection of digital data and the defence of systems and networks against malicious acts. Computer systems and networks that support nuclear facility operations include non-standard information technology systems that affect architecture, configuration and performance requirements. These systems can include specialized industrial control systems, access control systems, alarm and tracking systems and information systems pertaining to safety and security and emergency response.

The Stuxnet computer security incident demonstrated that nuclear facilities can be susceptible to cyberattack. This and other events have significantly raised global concerns over potential vulnerabilities and the possibility of a cyberattack or a joint cyber–physical attack that could impact nuclear security. The increasing use of computers and other digital electronic equipment presents an ever more likely target for cyberattack that may affect physical protection systems at nuclear facilities as well as facility safety systems, instrumentation, information processing and communications. In addition, computer security for facilities handling nuclear and other radioactive material, and associated activities such as transport, present a unique set of challenges.

This conference has been organized to foster international cooperation in computer security as an essential element of nuclear security.

PURPOSE AND OBJECTIVES

- Review the international community's experience, achievements and lessons learned for strengthening computer security within the framework of nuclear security

- Enhance understanding of current approaches for computer security worldwide within nuclear regimes

- Review emerging trends in computer security and identify areas that need to be addressed

- Provide a global forum for competent authorities, operators and other entities engaged in computer security activities relevant to nuclear security

- Discuss possible objectives and priorities for nuclear security efforts in computer security and how current approaches may evolve to address current and future challenges.

- Discuss ways the IAEA and other international organizations can contribute to international cooperation in this growing area

TOPICS

- Cyberthreats in Nuclear Security

- Computer Security and System Design for Systems at Nuclear Facilities

- Coordination for Ensuring Computer Security in a Nuclear Security Regime

- Nuclear Security Regulatory Approaches to Information and Computer Security

- Computer Security Programmes at Licensed Facilities

- Computer Security Management in Nuclear Security

- Computer Security Culture and Capacity Building for Nuclear Security International and Legal Considerations in Relation to Computer Security at Nuclear Facilities

AUDIENCE

The conference is intended for technical experts, nuclear security professionals and others with responsibilities in the field of computer security with nuclear security considerations.

This includes practitioners, senior officials and policy makers responsible for developing and implementing computer security programmes for nuclear and other radioactive material facilities.

The conference is also aimed at representatives from specialist organizations, law enforcement agencies, industries, and other entities engaged in computer security efforts for nuclear facilities and activities.