|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 1 June 2023 |
| **Ref:**  | **TSB Circular 106**TSB Events/XY | **To:**- Administrations of Member States of the Union;- ITU-T Sector Members;- ITU-T Associates;- ITU Academia**Copy to:**- The Chairmen and Vice-Chairmen of Study Groups;- The Director of the Telecommunication Development Bureau;- The Director of the Radiocommunication Bureau;- The Director of the ITU Regional Office for Asia and the Pacific |
| **Contact:** | **Xiaoya Yang** |
| **Tel:** | +41 22 730 6206 |
| **Fax:** | +41 22 730 5853 |
| **E-mail:** | tsbsg17@itu.int tsbevents@itu.int |
| **Subject:** | **ITU Workshop on “Zero Trust and Software Supply Chain Security”****(Goyang, Republic of Korea, 28 August 2023)** |

Dear Sir/Madam,

1 I am pleased to inform you that the International Telecommunication Union (ITU) is organizing a workshop on **“Zero trust and software supply chain security”** at the Korea International Exhibition Center (KINTEX), Goyang, Republic of Korea on 28 August 2023.

The workshop is kindly hosted by the Ministry of Science and ICT of the Republic of Korea and will precede the meeting of [ITU-T Study Group 17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) (29 August to 8 September 2023) taking place at the same venue. Remote participation will be provided for the workshop. The workshop will be held in English only.

2 In today's interconnected and rapidly evolving digital landscape, cyber threats have become increasingly sophisticated, with attackers targeting vulnerabilities in software supply chains to compromise systems and steal sensitive data. Zero Trust is a new strategic cybersecurity approach that secures an enterprise through removing implicit trust and continuously evaluating every stage of digital interactions. Software supply chain security focuses on the risk management during the lifecycle of the software for all related stakeholders including software vendors and users. By integrating Zero Trust principles into software supply chain security, organizations can establish a resilient defence against cyber threats.

3 The objectives of this workshop include, but are not limited to:

* providing an overview of Zero Trust and software supply chain security with insights into the new and emerging threats in these areas;
* identifying technical countermeasures and organizational controls to effectively mitigate the identified threats;
* showcasing on-going activities among relevant ITU-T study groups and other organizations in these areas; and
* identifying a way forward and providing suggestions to ITU-T Study Group 17 on potential topics of study in the future related to Zero Trust and software supply chain security.

5 Participation in the workshop is open to ITU Member States, Sector Members, Associates and Academic Institutions and to any individual from a country that is a member of ITU who wishes to contribute to the work. Participation is free of charge and open to all. No fellowships will be granted for the workshop.

5 All relevant Information pertaining to the workshop including the draft programme will be made available on the event website here: <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0828/Pages/default.aspx>.

The event webpage will be updated regularly as more information becomes available. Participants are encouraged to check the webpage periodically for updates.

6 General information for participants, including hotel accommodation, transportation and visa requirements is available on the ITU website mentioned above.

Registration is mandatory for all participants planning to attend the workshop. You are invited to complete the online registration form at: <https://www.itu.int/net4/CRM/xreg/web/registration.aspx?Event=C-00012439> as soon as possible.

**Early registration is encouraged for onsite attendance** and, to enable TSB to make the necessary arrangements concerning the organization of the workshop, **registration for on-site attendance** is requested to be completed by **21 August 2023 at the latest**.Please note that pre-registration of participants for our events is carried out exclusively online.

7 I would remind you that citizens of some countries are required to obtain a visa in order to enter and spend any time in the Republic of Korea. The visa must be obtained from the office (embassy or consulate) representing the Republic of Korea in your country or, if there is no such office in your country, from the one that is closest to the country of departure. Visa processing and approval may take some time, it is therefore suggested to check directly with the appropriate representation and apply early.

Additional information on visa requirements is available on the event webpage under the section “[Practical Information](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Documents/Practical-information-SG17-Korea_28_Aug-_8_Sep-2023.pdf)”.

Yours faithfully,

Seizo Onoe
Director of the Telecommunication
Standardization Bureau