|  |  |  |
| --- | --- | --- |
| Title: ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATION STANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | TSAG-TD558 |
| TSAG |
| **Original: English** |
| **Question(s):** | N/A | Geneva, 29 July - 2 August 2024 |
| **TD(Ref.:** [SG17-LS109](http://handle.itu.int/11.1002/ls/sp17-sg17-oLS-00109.docx)**)** |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS/i on sharing the results of the ITU workshop on "Generative AI: Challenges and Opportunities for security and privacy" and the establishment of the Correspondence Group on AI security (CG-AISEC) [from ITU-T SG17] |
| **LIAISON STATEMENT** |
| **For action to:** | TSAG |
| **For information to:** | ETSI, IEEE, ISO/IEC JTC1/SC27/WG5, ISO/IEC JTC1/SC27/WG4, OECD, ISO/IEC JTC1/SC42, ITU-T SG2, SG3, SG5, SG9, SG11, SG12, SG13, SG15, SG16 |
| **Approval:** | ITU-T Study Group 17 meeting (Geneva, 1 March 2024) |
| **Deadline:** | 31 July 2024 |
| **Contact:** | Heung Youl YoumSoonchunhyang UniversityKorea (Republic of) | E-mail: hyyoum@sch.ac.kr  |
| **Contact:** | Zhiyuan HUvivo Mobile CommunicationChina | E-mail: huzhiyuan@vivo.com  |

A new liaison statement has been received from SG17.

This liaison statement follows and the original file can be downloaded from the ITU ftp server at <http://handle.itu.int/11.1002/ls/sp17-sg17-oLS-00109.docx>.

|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | **SG17-LS109** |
| **STUDY GROUP 17** |
| **Original: English** |
| **Question(s):** | All/17 | Geneva, 20 February - 1 March 2024 |
| **(Ref.:** [**SG17-TD1848R1**](https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1848)**)** |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on sharing the results of the ITU workshop on "Generative AI: Challenges and Opportunities for security and privacy" and the establishment of the Correspondence Group on AI security (CG-AISEC)  |
| **LIAISON STATEMENT** |
| **For action to:** | TSAG |
| **For information to:** | ITU-T SGs, ETSI SAI, OECD, IEEE AIS Trust and Agency Committee, ISO/IEC JTC 1/SC 27/WG 4 & WG 5, and ISO/IEC JTC 1/SC 42/WG 3 |
| **Approval:** | ITU-T Study Group 17 meeting (Geneva, 1 March 2024) |
| **Deadline:** | 31 July 2024 |
| **Contact:** | Heung Youl YoumSoonchunhyang UniversityKorea (Republic of) | E-mail: hyyoum@sch.ac.kr  |
| **Contact:** | Zhiyuan HUvivo Mobile CommunicationChina | E-mail: huzhiyuan@vivo.com |

ITU-T Study Group 17 (SG17) is pleased to inform you that we had an ITU workshop on “Generative AI: Challenges and Opportunities for security and privacy” held on 19 February 2024 in Geneva. More information on the structure of the workshop and the content of the presentations/panels can be found at the following URL.

[ITU Workshop on "Generative AI: Challenges and Opportunities for security and privacy"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2024/0219/Pages/default.aspx)

As a result of this workshop, ITU-T SG17 gained the following findings regarding SDOs for potential collaboration on AI security:

• ISO/IEC JTC 1/SC 27/WG 4 for AI security and WG 5 for data protection of AI.

• ISO/IEC JTC 1/SC 42/WG 3 for AI Trustworthiness.

• ITU-T Study Groups for AI and its applications.

• IEEE AIS Trust and Agency Committee for Trust and Agency of AI.

• OECD for AI trustworthy.

• ETSI SAI for AI security.

The following is a published Technical Report and an existing new work item related to AI security in ITU-T SG17:

• [XSTR.sec-ai](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18031): Guidelines for security management of using artificial intelligence technology, which was published in May 2022.

• [X.sr-ai](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19051): Security requirements for AI systems, which is under development in ITU-T Q15/17.

The following is a list of potential topics for future works on AI security captured by the workshop:

• Security, PII protection and trustworthiness for generative AI.

• Controls to mitigate the negative consequence of generative AI.

• Common terms for generative AI ethics.

• Data governance for generative AI.

In addition, ITU-T SG17 had established a new Correspondence Group on AI security (CG-AISEC) at the ITU-T SG17 meeting in Geneva, 20 February - 1 March 2024, see Annex A for the Terms of Reference. ITU-T SG17 invites you to consider participation in the activities of the Correspondence Group whose first meeting will take place virtually on 16 May 2024, 09:00-10:00 Geneva time. More information will be shared through the CG-AISCEC mailing list: cg-aisec@lists.itu.int.

In proceeding with the above studies, it is essential to strengthen coordination and cooperation among ITU-T SG17 and other groups and external organizations, which are invited to liaise with SG17 regarding work in AI security and join in the activities of the CG-AISEC. Therefore, ITU-T SG17 shares the results of this workshop to provide a good opportunity for potential coordination and cooperation in future SG17 work on AI security, and will keep you informed of the progress of the CG-AISEC.

## Annex ATerms of reference for correspondence group on AI security(CG-AISEC)

1. The ITU-T correspondence group on AI security will report to Study Group 17 and will identify a SG17 general and generative AI security strategy considering to:
2. cover both aspects of "Security for AI" and "Security by AI" in general and generative AI security.
3. identify general and generative AI security domain:
	* 1. scope the current state and the future trends of general and generative AI security, including requirements from regulations,
		2. identify market and market status for general and generative AI security,
		3. identify what potential areas of standardization,
4. qualify on which foundation can SG17 establish legitimacy and relevance:
	* 1. determine and qualify the current strength, weaknesses, opportunities, and threats of SG17 vs general and generative AI security,
		2. e.g., as general and generative AI rely on massive data and models, SG17 has a solid foundation on Big Data, operational and technical data protection, etc.,
5. delineate general and generative AI’s collaboration within ITU and with other SDOs,
6. provide high level guidelines to SG17 for responsible and accountable use general and generative AI security and which relevant call for contributions could be made.

will take actions, if appropriate, to provide SG17 with draft of

1. LS out with its results to TSAG,
2. LS out with its results and request for input to other groups,
3. the ToR of this CG,

as well as issue a call to experts for contributions.

1. The correspondence group will submit a report of its activities one month before every SG17 meeting.
2. The correspondence group will use the email list cg-aisec@lists.itu.int. The CG interactions may include email exchange via the email list and virtual meetings.
3. The duration of the CG will last in this study period (2022-2024).
4. The correspondence group convener will be Mr. Xiongwei Jia, Q6/20 Co-Rapporteur, and the vice-conveners will be Ms. Zhiyuan HU, WP2/17 Vice-Chair & Q2/17 Co-Rapporteur, and Mr. Jabu Mtsweni.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_