INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2025-2028

SG17-LS75
STUDY GROUP 17
Original: English

Question(s):	2/17	Geneva, 3-11 December 2025

Ref.: SG17-TD298R1/GEN

Source:	ITU-T Study Group 17
Title:	LS on initiation of a new work item related to coordination of networking and computing

LIAISON STATEMENT

For action to:	-
For information to:	ITU-T SG13, 3GPP SA3 and NIST
Approval:	**ITU-T Study Group 17 meeting (Geneva, 11 December 2025)**
Deadline:	N/A

Contact:	Arnaud Taddei Chair, SG17	E-mail: arnaud.taddei@broadcom.com
Contact:	Heung-Ryong Oh Co-Rapporteur, Q2/17	Email: hroh@tta.or.kr
Contact:	Takamasa ISOHARA Co-Rapporteur, Q2/17	Email: ta-isohara@kddi.com
Contact:	Ke WANG Associate Rapporteur, Q2/17	Email: wangkeyj@chinamobile.com

Abstract: This liaison statement informs ITU-T SG13, 3GPP SA3 and NIST that SG17 initiates a new work item related to coordination of networking and computing (Geneva, 3-11 December 2025).

ITU-T Study Group 17 (SG17) would like to inform ITU-T Study Group 13 (SG13), 3GPP SA3 and NIST about our initiation of a new work items related to coordination of networking and computing, draft new Recommendation ITU-T X.5Gsec-CNC "Security requirements and guidelines for Coordination of networking and computing in IMT-2020 networks and beyond" (SG17-TD117/WP2).

Summary and scope of this new work item are provided in Annex.

ITU-T SG17 would like to continuously collaborate with you and to exchange information on CNC security related activities.

Annex:1

- Scope and summary for draft new Recommendation ITU-T X.5Gsec-CNC

Annex

Scope and summary for draft new Recommendation ITU-T X.5Gsec-CNC : “Security requirements and guidelines for Coordination of networking and computing in IMT-2020 networks and beyond”

Summary

Coordination of Networking and Computing (CNC) in IMT-2020 networks and beyond is a core technology for integrating multi-level computing power, networking, and storage resources to support the digital economy. It enables optimal resource allocation for vertical industries such as industrial internet, internet of vehicles, and smart healthcare—fields that rely on the ubiquitous connection and intelligent scheduling of cloud-edge-terminal resources.

However, CNC’s multi-layer architecture and distributed resource characteristics introduce unique security risks throughout resource layer, control layer, management and orchestration layer, and operation and service layer. Additionally, data security risks permeate all layers, threatening service availability and data integrity.

This Recommendation systematically addresses these challenges by: 1) Analyzing security threats and vulnerabilities across CNC’s four core layers and data security throughout the lifecycle; 2) Defining security requirements aligned with ITU-T Y.3400 (CNC requirements) and Y.3401 (CNC capability framework); 3) Providing targeted security guidelines, including the infrastructure layer, the control layer, the management layer, the service layer and the data layer. By complementing existing standards that lack CNC-specific security guidance.

This document aims to ensure the secure deployment of CNC in IMT-2020 networks and beyond, safeguard the stability of digital economy applications.

Scope

Draft new Recommendation ITU-T X.5Gsec-CNC aims to identify the security threats and challenges of CNC in IMT-2020 networks and beyond, and provides security guidelines for for its four-layer architecture including resource layer, control layer, management and orchestration layer, and operation and service layer. Additionally, it proposes corresponding security guidelines for cross-layer data security.

Note: Application security is out of scope of this recommendation.