|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 10 toDocument 37-E |
|  | 22 September 2024 |
|  | Original: English |
|  |
| Asia-Pacific Telecommunity Member Administrations |
| PROPOSED MODIFICATION TO RESOLUTION 50 |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This document contains the proposal for modification of WTSA Resolution 50 “Cybersecurity”. |
| **Contact:** | Mr. Masanori Kondo Secretary GeneralAsia-Pacific Telecommunity | E-mail: aptwtsa@apt.int  |

Introduction

Security is becoming more and more important for today’s telecommunication/ICT infrastructure. ITU-T has a role to play in developing key technical Recommendations in supporting building confidence, trust and security in the use of ICTs. Providing security by ICTs and ensuring security for ICTs are both major study areas.

Security should be considered throughout the entire lifecycle of a system/network/application, otherwise it will result in the system/network/application full of security vulnerabilities requiring a lot of patchwork.

Considering that security standardization activities contribute to prevention of damage resulted from malicious cyber activities, the security work should be continued. In addition, study groups in ITU-T, especially SG17, should address emerging security technologies which were identified, such as AI security, metaverse security, zero trust security, software supply chain security, etc**.**

The main aim of this modification is to clarify and strengthen the role of SG17 as the lead study group for Security.

Proposal

Based on the background above, APT Member Administrations propose to WTSA-24 to consider revising the WTSA Resolution 50 “Cybersecurity”.

MOD APT/37A10/1

RESOLUTION 50 (Rev. New Delhi, 2024)

Cybersecurity

(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022; New Delhi, 2024)

The World Telecommunication Standardization Assembly (New Delhi, 2024),

recalling

*a)* Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

*b)* Resolution 174 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on ITU's role with regard to international public policy issues relating to the risk of illicit use of ICTs;

*c)* Resolution 179 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on ITU's role in child online protection;

*d)* Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference, on definitions and terminology relating to building confidence and security in the use of ICTs;

*e)* Resolutions 55/63 and 56/121 of the United Nations General Assembly (UNGA), which established the legal framework on countering the criminal misuse of information technologies;

*f)* UNGA Resolution 57/239, on the creation of a global culture of cybersecurity;

*g)* UNGA Resolution 58/199, on the creation of a global culture of cybersecurity and the protection of essential information infrastructures;

*h)* UNGA Resolution 68/167, on the right to privacy in the digital age, affirms, *inter alia*, "that the same rights that people have offline must also be protected online, including the right to privacy";

*i)* UNGA Resolution 41/65, on principles relating to remote sensing of the Earth from outer space;

*j*) UNGA Resolution 70/125, on the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society (WSIS);

*k)* Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;

*l)* Resolution 52 (Rev. Hammamet, 2016) of the World Telecommunication Standardization Assembly, on countering and combating spam;

*m)* Resolution 58 (Rev. Geneva, 2022) of this assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[1]](#footnote-1)1;

*n)* that ITU is the lead facilitator for WSIS Action Line C5 in the Tunis Agenda for the Information Society (Building confidence and security in the use of ICTs);

*o)* the cybersecurity-related provisions of the WSIS outcomes,

considering

*a)* the crucial importance of telecommunication/ICT infrastructure and its application to practically all forms of social and economic activity;

*b)* that the legacy public switched telephone network has a level of inherent security properties because of its hierarchical structure and built-in management systems;

*c)* that Internet Protocol (IP) networks provide reduced separation between user components and network components if adequate care is not taken in the security design and management;

*d)* that the converged legacy networks and IP networks are therefore potentially more vulnerable to intrusion if adequate care is not taken in the security design and management of such networks;

*e)* that cybersecurity is a cross-cutting issue, and the cybersecurity landscape is complex and dispersed, with many different stakeholders at the national, regional and global levels with responsibility for identifying, examining and responding to issues related to building confidence, trust and security in the use of ICTs;

*f)* that the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybersecurity alarm all developed and developing nations of the world without exception;

*g)* that the fact, *inter alia*, that critical telecommunication/ICT infrastructures are interconnected at the global level means that inadequate infrastructure security in one country could result in greater vulnerability and risks in others and, therefore, cooperation is important;

*h)* that the number and methods of cyberthreats and cyberattacks are growing, as is dependence on the Internet and other networks that are essential for accessing services and information;

*i)* that standards can support the security aspects of Internet of things (IoT) and smart cities and communities including security aspects for new and emerging technologies;

*j)* that in order to protect global telecommunication/ICT infrastructures from the threats and challenges of the evolving cybersecurity landscape, coordinated national, regional and international action is required for prevention, preparation, response and recovery in respect of cybersecurity incidents;

*k)* the work undertaken and ongoing in ITU, including in ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17 and ITU Telecommunication Development Sector (ITU‑D) Study Group 2, including the final report of ITU‑D Study Group 1 Question 22/1-1, and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);

*l)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *considering j)*,

considering further

*a)* that Recommendation ITU‑T X.1205 provides a definition, a description of technologies, and network protection principles for cybersecurity;

*b)* that Recommendation ITU‑T X.805 provides a systematic framework for identifying security vulnerabilities and Recommendation ITU T X.509 provides the Public-key and attribute certificate frameworks, and Recommendation ITU‑T X.1500 provides the cybersecurity information exchange (CYBEX) model and discusses techniques that could be used to facilitate the exchange of cybersecurity information;

*c)* that Recommendation ITU-T X.1060 provides a framework for organizations to build and manage a cyber defence centre (CDC) that enable the security of an organization, evaluate its effectiveness in implementing security services and address its cybersecurity risks;

*d)* that ITU‑T and the Joint Technical Committee for information technology (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), as well as several consortia and standards entities such as the World Wide Web consortium (W3C), the Organization for Advancement of Structured Information Standards (OASIS), the Fast IDentity Online (FIDO) alliance, the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE), among others, already have a significant body of published materials and ongoing work that is directly relevant to this topic, which needs to be considered;

*e)* the importance of ongoing work on security reference architecture for lifecycle management of e‑commerce business data,

recognizing

*a)* the operative paragraph of Resolution 130 (Rev. Bucharest, 2022) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups;

*b)* that Resolution 71 (Rev, Bucharest, 2022) of the Plenipotentiary Conference adopted the strategic plan for 2024-2027, including Strategic Goal 1 (Universal Connectivity: Enable and foster universal access to affordable, high-quality and secure telecommunications/ICTs), under which the Union is to achieve universally accessible, affordable, high-quality, interoperable and secure telecommunication/information and communication technology (ICT) infrastructure, services and applications;

*c)* that the ITU Global Cybersecurity Agenda (GCA) promotes international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of ICTs, considering security aspects throughout the whole lifecycle of the standards-development process;

*d)* the challenges that States, particularly in developing nations, face in building confidence and security in the use of ICTs, and that Resolution 44 (Rev. Geneva, 2022) of the WTSA on bridging the standardization gap between developing and developed countries;

e) the challenges that Member States, particularly in developing nations, face in building trusted and secure Telecommunications/ICT infrastructure and applications for technical and operational aspects of protection of data and personally identifiable information (PII),

recognizing further

*a)* that cyberattacks such as phishing, spam, pharming, scan/intrusion, distributed denials of service, advanced persistent threat, web-defacements, unauthorized access, malware, data poisoning, spoofing, etc., are emerging and having serious impacts;

*b)* that botnets are being used to distribute bot-malware and carry out cyberattacks;

*c)* that sources of attacks are sometimes difficult to identify;

*d)* that critical cybersecurity threats in software and hardware may require timely vulnerability management and timely hardware and software updates and appropriate access rights assignment to prevent end devices attacks;

*e)* that ransomware attacks continue to grow;

*f)* that the application of new technologies along with the constantly evolving global telecommunications/ICT infrastructure brings new challenges and requires higher requirements to telecommunications/ICT security and technical and operational aspects of protection of data and PII, which may affect network security architecture;

*g)* the advancement of technologies in managing cybersecurity threats and protecting telecommunications/ICTs;

*h)* that the needs of security capability development including personnel capability development in managing security risks and technologies;

*i)* that securing data and big data infrastructure are key components in cybersecurity as data are often the target of cyberattacks while the wide application of big data technology makes this target ubiquitous in today's network behaviours;

*j)* that cybersecurity is a key element for building confidence, trust and security in the use of telecommunications/ICTs;

*k)* that security occupies an important position throughout the lifecycle of systems, networks, applications, and data;

*l)* that security architecture and framework are important and could be considered as the basis of security architecture design for various systems, networks, applications, and data,

noting

*a)* the vigorous activity and interest in the development of telecommunication/ICT security standards and Recommendations in Study Group 17, the lead ITU‑T study group on security and identity management, and in other standardization bodies, including the Global Standards Collaboration (GSC) group;

*b)* that interoperability and security aspects of evolving network infrastructure and rapid innovation in development of open network infrastructure should be evaluated;

*c)* that in addition to other cyber threats, technical and operational aspects of protection of data and PII have emerged as a big issue for the Member States;

*d)* that there is a need for national, regional and international strategies and initiatives to be harmonized to the extent possible, in order to avoid duplication and to optimize the use of resources;

*e)* the significant and collaborative efforts by and among governments, the private sector, civil society, the technical community and academia, within their respective roles and responsibilities, to build confidence, trust and security in the use of ICTs,

resolves

1 to continue to give this work high priority within ITU‑T, in accordance with its competencies and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national, regional and international level;

2 that all ITU‑T study groups continue to evaluate existing and evolving new Recommendations, according to their mandates in Resolution 2 (Rev. Geneva, 2022) of this assembly, with considering security issues throughout the entire process of developing ITU-T standards, with respect to their robustness of design and operation, and potential for exploitation by malicious parties, and take into account new and emerging telecommunication/ICT services and technologies to be supported by the global telecommunication/ICT infrastructure (including, but not limited to, for example, cloud computing and IoT, which are based on telecommunication/ICT networks);

3 that ITU‑T continue to raise global awareness regarding security in ICTs, through the development of Recommendations and technical reports which support cybersecurity procedures, technical policies and frameworks, within its mandate and competencies, of the need to harden and defend information and telecommunication systems from cyberthreats and malicious cyberactivity, to enhance the personnel capability development for security, and continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical information in the field of information and telecommunication network security;

4 that ITU-T should raise global awareness regarding security in ICTs through the development of Recommendations and technical reports which support cybersecurity procedures, technical policies and frameworks, with the objectives to better manage cybersecurity risks and protect their information and telecommunication networks;

5 that ITU‑T should work with ITU‑D, particularly in the context of ITU-D Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity);

6 that relevant ITU-T study groups should keep pace with the development of the new and emerging technologies, according to their mandates, in order to alert SG17 to areas that may require new Recommendations, supplements and technical reports to address challenges related to security and technical and operational aspects for the protection of data and PII;

7 that ITU‑T continue work on the development and improvement of terms and definitions related to building confidence, trust (including through protection of data and Personally Identifiable Information) and security in the use of telecommunications/ICTs, including cybersecurity;

8 that global, consistent and interoperable processes for sharing information related to incident response should be promoted;

9 that ITU‑T study groups continue to liaise with standards organizations and other bodies active in this field and encourage the engagement of experts in ITU's activities in the area of building confidence, trust and security in the use of ICTs;

10 that secure, trusted and resilient telecommunication/ICT networks and services should be developed and maintained to enhance confidence and trust in the use of Telecommunications/ICT;

11 that Study Group 17 needs to develop cooperative cybersecurity analysis and incident management frameworks;

12 that the resilience of ICT networks and systems should be considered as a priority in telecommunication/ICT network infrastructure and applications development,

instructs Study Group 17

1 to promote studies on cybersecurity, including security and technical and operational aspects of data and PII for new and emerging services and technologies to counter the vulnerabilities in the use of the global telecommunication/ICT infrastructure, by developing Recommendations, supplements and technical reports, as appropriate;

2 to support the Director of TSB to maintain the ICT Security Standards Roadmap, which should include work items to progress standardization work related to security, technical and operational aspects of protection of data and PII, and security compendium which should include the list of Recommendations and terms and definition and share those with relevant groups of the ITU Radiocommunication Sector (ITU-R) and ITU-D as the mission of the lead group for security;

3 to promote joint coordination activities on confidence, trust and security among all relevant study groups and focus groups in ITU and other standards-development organizations, including Joint Coordination Activity on Child Online Protection and its gap analysis;

4 to collaborate closely with all other ITU-T study groups, establish an action plan for assessing existing, evolving and new ITU-T Recommendations to address constantly evolving security, threats and vulnerabilities, to ensure resilience of ICT networks from cyberattacks and continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group;

5 to continue to define a general/common set of security capabilities for each phase of information system/network/application lifecycles, including personnel capability development for security so that consequently security by design (security capabilities and features available by design) could be achieved for systems/networks/applications from day one;

6 to continue to design one or more security frameworks or reference architectures with security functional components including considering security collaboration among different type of systems which could be considered as the basis of security architecture design for various systems/networks/applications in order to improve the quality of Recommendations on security, and provide security design references for potential applications of emerging technologies in global telecommunication/ICT infrastructure;

7 to consider the continuous changes in ICT technology and business, regularly review the network security Recommendations and revise existing Recommendations to adapt to new security requirements and respond to new network security threats;

8 to provide the best practices for evaluating and improving security and technical and operational aspects of protection of data and PII in evolving telecommunication/ICT infrastructure,

instructs the Director of the Telecommunication Standardization Bureau

1 to continue to maintain, in building upon the information base associated with the Telecommunications/ICT Security Standards Roadmap and ITU‑D efforts on cybersecurity, and with the assistance of other relevant organizations, an inventory of national, regional and international initiatives and activities to promote, to the maximum extent possible, the worldwide harmonization of strategies and approaches in this critically important area, including the development of common approaches in the field of cybersecurity;

2 to contribute to annual reports to the ITU Council on building confidence and security in the use of Telecommunications/ICTs, as specified in Resolution 130 (Rev. Bucharest, 2022);

3 to report to the Council on the progress of activities on the Telecommunications/ICT Security Standards Roadmap;

4 to continue to recognize the role played by other organizations with experience and expertise in the area of security, data protection, PII standards, and coordinate with those organizations as appropriate;

5 to continue the implementation and follow-up of relevant WSIS activities on building confidence and security in the use of Telecommunications/ICTs, in collaboration with the other ITU Sectors and in cooperation with relevant stakeholders, as a way to share information and best practices on national, regional and international non-discriminatory cybersecurity-related initiatives globally;

6 to cooperate with the Secretary-General's GCA and other global or regional cybersecurity projects, as appropriate, in promoting capacity building and developing relationships and partnerships with various regional and international cybersecurity-related organizations and initiatives, as appropriate, and to invite all Member States, particularly developing countries, to take part in these activities and to coordinate and cooperate with these different activities;

7 to support the Director of the Telecommunication Development Bureau (BDT) in assisting Member States in the establishment of an appropriate framework among developing countries allowing rapid response to major incidents, and to propose an action plan to increase their protection, taking into account mechanisms and partnerships, as appropriate;

8 to support relevant ITU‑T study group activities related to strengthening and building confidence, trust and security in the use of ICTs;

9 to disseminate information to all stakeholders and increase stakeholder’s understanding related to cybersecurity through the organization of training programmes, forums, workshops, seminars, etc., as appropriate, on ITU-T Recommendations and implementation guidelines for policy-makers, regulators, operators and other stakeholders, especially from developing countries;

10 to consider, whenever possible, to raise awareness by holding workshops concurrently with the meetings of respective regional groups of ITU-T study groups, or events in coordination and collaboration with the Director of BDT and ITU regional offices alongside these meetings,

invites Member States, Sector Members, Associates and Academia, as appropriate

1 to collaborate closely in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Bucharest, 2022), with a view to enhancing confidence and security in the use of Telecommunications/ICTs, in order to mitigate risks and to address threats;

2 to cooperate and participate actively in the implementation of this resolution and the associated actions;

3 to participate in relevant ITU‑T study group activities to develop cybersecurity standards and guidelines in order to build confidence, trust and security in the use of ICTs;

4 to utilize relevant ITU‑T Recommendations, technical reports, and Supplements;

5 to continue to contribute to Study Group 17 work on cybersecurity risk and cyber defence management approaches.

1. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-1)