|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 15 toDocument 39-E |
|  | 13 September 2024 |
|  | Original: English |
|  |
| Member States of the Inter-American Telecommunication Commission (CITEL) |
| Proposed modifications to Resolution 50 |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | CITEL proposes modifications to WTSA Resolution 50 to ensure its compatibility with modifications introduced in PP-22 Resolution 130 and WTDC-22 Resolution 45. This effort to align and harmonize the resolutions aims to enhance the advancement of a security-centric approach, where security is seamlessly integrated into products right from their inception and persistently upheld throughout their existence. Furthermore, a set of editorial refinements is suggested to enhance overall clarity. |
| **Contact:** | Maria Celeste Fuenmayor Inter-American Telecommunication Commission | E-mail: mfuenmayor@oas.org  |

MOD IAP/39A15/1

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 the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

*b)* Resolution 174 (Rev. Bucharest, 2022) 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 64/211, on the creation of a global culture of cybersecurity and the protection of essential information infrastructures;

*h)* UNGA Resolutions 77/211 and 68/167, on the right to privacy in the digital age;

*i)* UNGA Resolution 76/19, on developments in the field of information and telecommunications in the context of international security;

*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. Kigali, 2022) 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 and security in the use of ICTs;

*f)* that the growth in cyberthreats and cyberattacks has caused considerable and increasing losses for users of telecommunication/ICT systems , alarming all 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), smart cities and communities, and other emerging telecommunication/ICT services and technologies;

*j*) that mitigating human-induced risks is a key element of cybersecurity;

*k)* 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;*l*) 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, and under the Kigali Action Plan adopted by the last WTDC (Kigali, 2022);

*m)* 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;

*b)* that Recommendation ITU‑T X.805 provides a systematic framework for identifying security vulnerabilities, 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 and Recommendation ITU-T X.509 provides the Public-key and attribute certificate frameworks;

*c)* 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 development entities such as the World Wide Web consortium (W3C), the Organization for the Advancement of Structured Information Standards (OASIS), the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), 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;

*d)* the importance of promoting a culture in which security is seen as a continuous and iterative process, built into products from the beginning and continuing throughout their lifetime,

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 will focus on achieving accessible, affordable, high-quality, interoperable, and secure telecommunication/ICT infrastructure, services and applications;

*c)* that standards are a key component of Pillar 2 – Technical and Procedural Measures of the ITU Global Cybersecurity Agenda (GCA) which 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,

recognizing further

*a)* that a range and diversity of cyberattacks such as phishing, pharming, scan/intrusion, distributed denials of service, web-defacements, and unauthorized access, have emerged and have 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;

*e)* that securing data is a key component of cybersecurity as data are often the target in cyberattacks;

*f)* that cybersecurity is one of the elements for building confidence and security in the use of telecommunications/ICTs;

*g)* that the rise of new AI-driven applications and technologies has the potential to significantly impact cybersecurity, introducing new threats and new defence strategies,

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 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;

*c)* 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 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, with respect to their robustness of design and potential for exploitation by malicious parties, and take into account new services and emerging applications 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), according to their mandates in Resolution 2 (Rev. Geneva, 2022) of this assembly;

3 that ITU‑T continue to raise awareness, within its mandate and competencies, about the importance of strengthening and safeguarding information and telecommunication systems against cyberthreats and malicious cyberactivity, 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 standards frameworks;

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 telecommunication/ICT services and technologies, according to their mandates, in order to develop Recommendations, supplements and technical reports that help to overcome challenges related to security;

7 that ITU‑T continue work on the development and improvement of terms and definitions related to building confidence and security in the use of telecommunications/ICTs, including the term cybersecurity;

8 that consistent and interoperable processes for sharing information related to incident response should be promoted at the national, regional, and international level;

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 and security in the use of ICTs;

10 that security aspects should be considered throughout the ITU‑T standards-development process;

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

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

instructs Study Group 17

1 to promote studies on cybersecurity, including security for new and emerging telecommunications/ICT services and technologies, to be supported by the global telecommunication/ICT infrastructure;

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, and share this with relevant groups of the ITU Radiocommunication Sector (ITU-R) and ITU-D as the mission of the lead ITU-T study group for security;

3 to promote joint coordination activities on security among all relevant study groups and focus groups in ITU and other standards-development organizations;

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 counter security vulnerabilities, and continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group;

5 to define a general/common set of security capabilities throughout every stage of the development cycle (requirements, design, implementation, verification, release and maintenance) of information system/network/application/service products, so that security capabilities and features can be integrated at all phases of product’s lifecycle from day one;

6 to design one or more security architecture reference frameworks with security functional components 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;

7 to develop cooperative security analysis and incident management frameworks,

8 to continue considering human-induced risks in cybersecurity,

instructs the Director of the Telecommunication Standardization Bureau

1 to continue to maintain, in building upon the information base associated with the ICT Security Standards Roadmap and Security Compendium 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 ICTs, as specified in Resolution 130 (Rev. Bucharest, 2022);

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

4 to continue to recognize the role played by other organizations with experience and expertise in the area of security 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 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 and security in the use of ICTs;

9 to disseminate information to all stakeholders related to cybersecurity through the organization of training programmes, forums, workshops, seminars, etc., for policy-makers, regulators, operators and other stakeholders, especially from developing countries, to raise awareness and identify needs in collaboration with the Director of BDT;

10 to continue to support initiatives to encourage active participation of women in ITU-T cybersecurity related activities and leadership roles, including the Network of Women (NoW) in ITU-T,

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 ICTs, in order to mitigate risks and 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 and security in the use of ICTs;

4 to utilize relevant ITU‑T Recommendations and supplements;

5 to continue to contribute to Study Group 17 work on cybersecurity, including risk-management approaches;

6 to continue to engage in initiatives to encourage active participation of women in ITU-T cybersecurity related activities and leadership roles, including NoW in ITU-T.

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