|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 10 toDocument 35-E |
|  | 13 September 2024 |
|  | Original: English |
|  |
| African Telecommunication Union Administrations |
| PROPOSED MODIFICATIONS TO RESOLUTION 58 |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This contribution proposes to update WTSA Resolution 58 in order to ask Member States to support CIRTs in enhancing information sharing and collaboration for cybersecurity incident response particularly in developing countries globally. Member States to develop and implement programmes on awareness campaigns on the importance of CIRTs. |
| **Contact:** | Isaac BoatengAfrican Telecommunication Union | E-mail: i.boateng@atuuat.africa |

Introduction

To support Computer Incident Response Teams (CIRTs) in enhancing information sharing and collaboration for cybersecurity incident response, particularly in developing countries. This will lead to improved cybersecurity emergency preparedness and a stronger, more resilient cybersecurity posture particularly in developing countries.

MOD ATU/35A10/1

RESOLUTION 58 (Rev. New Delhi, 2024)

Encouraging the creation of national computer incident response teams, particularly for developing countries

(Johannesburg, 2008; Dubai, 2012; Geneva, 2022; new Delhi, 2024)

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

considering

that Resolution 123 (Rev. Bucharest, 2022) of the Plenipotentiary Conference instructs the Secretary-General and the Directors of the three Bureaux to work closely with each other in pursuing initiatives that assist in bridging the standardization gap between developing and developed countries,

considering further

that Recommendation ITU-T X.1060 provides a framework for the creation and operation of a cyber defence centre,

recognizing

*a)* the highly satisfactory results obtained by the regional approach within the framework of Resolution 54 (Rev. Hammamet, 2016) of the World Telecommunication Standardization Assembly;

*b)* the increasing level of computer use and computer dependency in information and communication technologies (ICTs) within developing countries;

*c)* the increasing attacks and threat on ICT networks through computers;

*d)* the work carried out by the ITU Telecommunication Development Sector (ITU‑D) under former Question 22/1 of ITU‑D Study Group 1 and current Question 3/2 of ITU-D Study Group 2 on this subject,

noting

*a)* that there is still a low level of computer emergency preparedness within many countries, particularly developing countries;

*b)* that the high level of interconnectivity of ICT networks could be affected by the launch of an attack from networks of the less-prepared nations, which are mostly the developing countries;

*c)* the importance of having an appropriate level of computer emergency preparedness in all countries;

*d)* the need for establishment of computer incident response teams (CIRTs) on a national basis and the importance of coordination within and among the regions;

*e)* the work of Study Group 17 of the ITU Telecommunication Standardization Sector (ITU-T) in the area of national CIRTs, particularly for developing countries, and cooperation between them, as contained in the outputs of the study group;

*f)* the increasing complexity of managing cyber defence infrastructure, tools, personnel, and security services due to the growing sophistication of cyber attacks on ICT networks in all countries,

bearing in mind

that well‑functioning CIRTs in developing countries will serve to improve the level of developing countries' participation in world computer emergency response activities and contribute to achieving an effective global ICT infrastructure and cybersecurity expertise,

resolves

1 to support the creation of national CIRTs in Member States where CIRTs are needed and are currently absent;

2 to support CIRTs in enhancing information sharing and collaboration for cybersecurity incident response, aiming to elevate the level of cybersecurity emergency preparedness, particularly in developing countries globally;

3 to engage ITU regional offices in the implementation of this Resolution and raise awareness on the importance of CIRTs to Member States about the ITU-T activities on this,

instructs the Director of the Telecommunication Standardization Bureau

to inform TSAG annually on the implementation of this Resolution,

instructs the Director of the Telecommunication Standardization Bureau, in collaboration with the Director of the Telecommunication Development Bureau

1 to identify best practices to establish CIRTs in line with the ITU toolkit;

2 to identify where national CIRTs are needed, particularly in developing countries, and encourage their establishment;

3 to collaborate with international experts and bodies to establish national CIRTs;

4 to provide support, as appropriate, within existing budgetary resources;

5 to facilitate collaboration between national CIRTs, such as capacity building and exchange of information, within an appropriate framework;

6 to take necessary action to progress implementation of this resolution;

7 to develop programmes on awareness campaigns on the importance of CIRTs to elevating the level of cybersecurity posture,

invites the Member States

1 to consider the creation of a national CIRT as a high priority;

2 to collaborate with other Member States and with Sector Members;

3 to encourage collaboration networks and participating in international organizations like FIRST (Forum of Incident Response and Security Teams) for enhancing global cybersecurity capabilities and incident response collaboration,

invites Member States and Sector Members

to cooperate closely with ITU-T, ITU‑D and Regional ITU offices in this regard.