|  |  |  |
| --- | --- | --- |
| APTlogogreen3 | ASIA-PACIFIC TELECOMMUNITY | **Document No.:** |
| **The 3rd Meeting of the APT Preparatory Group for WTDC-21 (APT WTDC21-3)** | **APT WTDC21-3/**  **OUT-13 (Rev.1)** |
| 5-8 October 2021, Virtual/Online Meeting | 7 February 2022 |

Chair, WG3

**PRELIMINARY APT COMMON PROPOSAL**

**Proposed modification TO WTDC-17 RESOLUTION 69**

**Facilitating creation of national computer incident response teams, particularly for developing countries, and cooperation between them**

|  |
| --- |
| **Priority area:** (Please mark “X” in front of the appropriate item)  \_\_\_ Declaration  \_\_\_ Thematic Priorities, Action Plan, Regional Initiatives and SG Questions  \_\_\_ Working Methods  \_X\_\_ Resolutions and Recommendations  \_\_\_ Other proposals  **Summary:**  This document contains proposed modifications to WTDC-17 Resolution 69 “Facilitating creation of national computer incident response teams, particularly for developing countries, and cooperation between them”. The proposal aims to incorporate references to the relevant work taking place in ITU-T Study Group 17, clarify text on CIRT establishment, and encourage the use of technical measures enabled by emerging technologies where using them improves and enhances conventional CIRT capabilities. The modifications also highlight the importance of engaging in the Pacific on this issue, particularly with Pacific Island Countries, through the addition of references to the Pacific Cyber Security Operational Network (PaCSON).  **Expected results:**  APT Member administrations invite WTDC to examine the proposal and approve the changes to Resolution 69.  **References:**  [WTDC Resolution 69 (Rev. Buenos Aires, 2017)](https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/69BuenosAires.pdf) |

**PROPOSALS**

APT Member administrations propose to modify WTDC Resolution 69, according to the annex below.

**MOD**

RESOLUTION 69 (Rev. Addis Ababa, 2021)

**Facilitating creation of national computer incident response teams, particularly for developing countries[[1]](#footnote-1)1, and   
cooperation between them**

The World Telecommunication Development Conference (Addis Ababa, 2021),

*recalling*

*a)* Resolutions 101, 102 and 130 (Rev. Dubai, 2018) of the Plenipotentiary Conference, which stress the need for collaboration;

*b)* Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly (WTSA), on encouraging the creation of national computer incident response teams (CIRTs), particularly in developing countries;

*c)* Resolution 50 (Rev. Hammamet, 2016) of WTSA, on cybersecurity,

*recognizing*

*a)* the highly satisfactory results obtained by the regional approach adopted within the framework of Resolution 69 (Rev. Addis Ababa, 2021);

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

*c)* the exposure of developing countries to malicious cyber activities targeting ICT networks, and that they could be better prepared for such malicious cyber activities and for the increasing level of fraudulent activity by these means;

*d)* the need to improve coordination and capacity to respond to cybersecurity challenges;

*e)* the results of the work carried out to date under Question 3/2 by Study Group 2 of the ITU Telecommunication Development Sector (ITU‑D) and its reports and coursework on this subject, which include support for the creation of CIRTs and establishing public-private partnerships;

*f)* the work carried out to date by the Telecommunication Development Bureau (BDT), to bring together Member States and other stakeholders to assist countries in building national incident management capabilities, such as CIRTs;

*g)* the importance of having an appropriate level of computer emergency preparedness in all countries, particularly developing countries, by establishing CIRTs on a national basis, and the importance of coordination within and among the regions and of taking advantage of regional and international initiatives in this regard, including ITU cooperation with regional and global projects and organizations, such as the Forum of Incident Response and Security Teams (FIRST), the Organization of American States (OAS), the Asia-Pacific Computer Emergency Response Team (APCERT) and the Pacific Cyber Security Operational Network (PaCSON), among others;

*h)* that emerging technologies are being applied more broadly across industries and applications than ever before, including as part of technical measures against malicious cyber activities;

*i)* the work of Study Group 17 of the ITU Telecommunication Standardization Sector (ITU-T) on cybersecurity information exchange (CYBEX) techniques, especially, but not limited to, Recommendation ITU‑T X.1500 and X.1215, and the work of OASIS (Organization for the Advancement of Structured Information Standards) on Structured Threat Information Expression (STIX),

*noting*

*a)* that there is an improved, but still low, level of computer emergency preparedness within developing countries;

*b)* that the high level of interconnectivity of telecommunication/ICT networks could be affected by malicious cyber activity from networks of less-prepared nations, which are mostly the developing countries;

*c)* *considering g)* in Resolution 130 (Rev. Dubai, 2018), which states that, in order to protect these infrastructures and address these challenges and threats, coordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents, on the part of government authorities, at the national (including the creation of CIRTs) and sub-national levels, the private sector and citizens and users, in addition to international and regional cooperation and coordination, and that ITU has a lead role to play within its mandate and competencies in this field;

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

*e)* that the establishment of CIRTs requires ongoing and appropriate resourcing in order to be successful and sustainable;

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

*g)* the need for the establishment of CIRTs on a national basis as appropriate, including CIRTs responsible for government-to-government cooperation, and the importance of coordination among all relevant organizations;

*h)* the ITU Global Cybersecurity Agenda,

*resolves*

1 to invite Member States and Sector Members with experience in this area:

• to establish national CIRTs, including CIRTs responsible for government-to-government cooperation, where needed or currently lacking, as appropriate;

• to collaborate closely with relevant organizations, and ITU‑T, in this regard, taking into consideration Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly (WTSA);

• to facilitate exchanging best practices among their national CIRTs;

• to encourage the use of technical measures enabled by emerging technologies where using them improves and enhances conventional CIRT capabilities;

2 to instruct the Director of BDT to give the necessary priority to this, by:

• promoting national, regional and international best practices for establishing CIRTs, as identified to date by the relevant ITU study groups, such as ITU‑D Study Group 1 under past Question 22‑1/1 and ITU-T Study Group 17, and by other relevant organizations and experts;

• preparing the training programmes necessary for this purpose and continuing to provide support as required to those developing countries that so wish;

• promoting collaboration between and among national CIRTs, including CIRTs responsible for government-to-government cooperation, industry CIRTs and academia CIRTs, in accordance with national legislation, at the regional and global level, by encouraging the participation of developing countries in regional and global projects and in the work of organizations such as FIRST (Forum of Incident Response and Security Team), OAS (Organization of American States), APCERT (Asia Pacific Computer Emergency Response Team) and PaCSON (Pacific Cyber Security Operational Network), among others;

• working to achieve these goals while avoiding duplication of effort with other organizations;

3 to instruct ITU-D Study Group 2, under Question 3/2, within its mandate, to contribute to the implementation of this resolution, also taking into consideration the work carried out by ITU‑T, especially ITU-T Study Group 17, on this issue.

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

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