|  |  |  |
| --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16)Hammamet, 25 October - 3 November 2016 | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| PLENARY MEETING | Addendum 15 toDocument 48-E |
|  | 8 October 2016 |
|  | Original: English |
|  |
| United States of America |
| VIEWS ON ASPECTS OF ITU-T STUDY GROUP 20 FUTURE WORK |
|  |

|  |  |
| --- | --- |
| **Abstract:** | By this contribution, the United States offers its views regarding certain aspects of Study Group 20’s terms of reference and work items. We offer these views primarily in response to document WTSA-16/ 22, Report of ITU-T SG20 to the World Telecommunication Standardization Assembly (WTSA-16), Part II: Questions Proposed For Study During The Next Study During (2017-2020). We also offer minor edits to document WTSA-16/ 21, Report of ITU-T SG20 to the WTSA-16, Part I, (General), particularly in Section 4 “Observations concerning future work.” |

**Discussion:**

Study Group 20 (SG20) was created by the Telecommunication Standardization Advisory Group (TSAG), between WTSAs. Its current Terms of Reference (ToR) can be found at [TD322Rev3](http://www.itu.int/md/T13-TSAG-150602-TD-GEN-0322/en). For the past year, the United States has participated constructively in discussions at both TSAG and at SG20 about the scope of SG20’s authority and appropriate work items. The United States has consistently raised questions and concerns, some of which we have sought to address in our other contributions to this assembly. In reviewing Document 21 (particularly Section 4 on “Observations for future work”) and Document 22, the United States identified several areas that are still of concern.

This contribution addresses two of our concerns related to privacy and infrastructure, on which we seek clarification from WTSA. Additionally, because this is the first opportunity WTSA has had to consider the matter, it is important that SG20’s ToR and future work items be considered and updated.

*Privacy*

The United States believes further clarity is needed to ensure a clear separation between international technical standards work and national policies governing privacy and data protection. “Privacy” has different meanings in different contexts and is legally protected in different ways around the world. Privacy is a matter for national administrations to manage through legislation and/or regulation. Internationally, administrations work together to negotiate agreements that reflect extensive legal analysis and a desire for cooperation.

The United States recognizes that other Standards Development Organizaitons (SDOs) are labelling their standards development work “security and privacy” but it is important to note that such work is limited to the *technical* elements of privacy. As an organization of member states, ITU-T must take particular care to avoid both actual and perceived efforts to go beyond its mandate for technical standards for international public telecommunication networks and to address issues defined by national laws, regulations or policies of ITU Member States. The Union also must avoid any appearance of endorsing specific national approaches. It would, for instance, be inappropriate for ITU-T to develop recommendations that endorse a specific national or regional privacy policy.

Because of the difficulties in maintaining appropriate separation between the technical elements of privacy and its legal ramifications, the United States recommends that the ITU-T avoid references to “privacy” in work items and Recommendations, and emphasize instead the specific technical mechanisms ITU-T experts seek to standardize.

To that end, and in order to align with Resolution 130 (rev. Busan 2014), we recommend replacing the term “privacy” with “confidence” in Documents 21, 22, and in the Terms of Reference for Study Group 20. The United States understands the term “security”, where used in either C21 or C22, refers to the work allocated to SG20 by the Ad Hoc Group (TSAG TD614Rev2) approved at the July 2016 TSAG meeting.

*Infrastructure*

Questions E/20 and F/20 center on issues about the use of IoT techniques in Smart Cities and Communities. It is our understanding that the physical infrastructure in Questions E/20 and F/20 do not include critical infrastructure protection, as it is a matter of *national*, not international, policy to determine categorizations of *critical* infrastructure. We further note that any security aspects of SC&C Infrastructure in Questions E/20 and F/20 should abide by the allocations identified in TSAG TD 614R2.

The United States recognizes the potential value of IoT applications and services in managing urban systems and infrastructure such as electrical grids, and we acknowledge the potential value of technical standards to facilitate such work. We note, however, that many such systems are operated in ways that preclude international standardization, due to the degree of physical and national specificity in how such infrastructure is built and regulated. We propose adding text to clarify these important distinctions.

**Proposal**

1. The United States proposes to modify the ToR for SG20 found in TSAG-15 [TD322Rev3](http://www.itu.int/md/T13-TSAG-150602-TD-GEN-0322/en) by replacing the word “privacy” with “confidence”.
2. The United States proposes to replace the word “privacy” and/or “privacy and trust” with “confidence and security”, wherever these words appear in documents WTSA-16/ 22 and WTSA-16/Doc. 21 (Section 4) – Observations concerning future work.
3. The United States proposes to add text to Question E/20 and F/20 to clarify the important distinction between technical standards that pertain to IoT techniques for sensing and control of physical infrastructure (electrical grids, water, transportation) and the rights of individual nations to determine designations and policies regarding critical infrastructure and its protection.