

**Document Number : WSIS+10/3/49**

**Submission by: ISOC, Civil Society**

***Please note that this is a submission for the Third Physical meeting of the WSIS +10 MPP to be held on the 17th and 18th of February.***

**Document Number: V2/C/ALC5**

Note: This document is the **result of the first reading of the document number V1.1/C/ALC5**

and reflects the changes and comments received at the second physical meeting of the WSIS+10 MPP.

This document is available at: <http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html>

This document has been developed keeping in mind the [Principles](http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html).

Please note that the Geneva Declaration and the Geneva Plan of Action still remain valid until further decisions by the General Assembly.

Draft WSIS+10 Vision for WSIS Beyond 2015

С5. Building confidence and security in the use of ICTs

**1. Vision**

[Confidence, safety, trust and security in the use of ICTs are among the main pillars and prerequisites for building the information society. We should all collectively strive to create trusted and safe ICTs environments, where all stakeholders can fully enjoy the benefits from new technologies in full confidence .

**2. Pillars**

1. Encourage greater cooperation at the national, regional and international levels among all stakeholders in building confidence and security in the use of ICTs.
2. Promote frameworks that reinforce greater safety and confidence in the use of ICTs. Assist developing and least developed countries to participate in the development of these frameworks.
3. Encourage and strengthen support for the establishment of [authorized]national and regional Computer Incident Response Teams (CIRTs) for incident management and regional and international coordination among them, for real-time handling and response of incidents, especially for national critical infrastructures, including information infrastructure. [Also, promote collaboration among CIRTs at the regional and global level by encouraging their participation in regional and global projects and organizations.]
4. Continue to encourage the building of a “culture of cybersecurity” marked by shared responsibility and collective action at the national, regional and international levels through [public-private partnerships], awareness raising and training, especially for the general public - providing assistance to developing and least developed countries in this regard.
5. Promote, through international [multistakeholder] [frameworks/ approach] [legal and /or multistakeholder] [if needed], respect for privacy rights, data and consumer protection, [in particular for applications and services hosted on cloud-based platforms].
6. Ensure special emphasis for protection and empowerment of the vulnerable people, especially children, online. In this regard, governments and other stakeholders, [especially civil society], should work together to help all to enjoy the benefits of ICTs in a safe and secure environment.
7. Recognize the importance of the concept of “security by design”,[ especially amongst the business sector] when providing products and services.
8. [Ensure that critical infrastructure is managed by professionals in ICT so that trust can be assured. ICT professionalism means operating at a higher standard of ICT practice than that which may be in place today. This will mean that ICT professionals will undertake ongoing continuing professional development, commitment to a code of ethics and professional conduct and have regard to the society which they serve and which will hold them accountable, in this way trust will be assured.]
9. Promote the development of assessment criteria to measure and monitor the, confidence and security aspects in the use of ICTs.
10. [Recognizing the national cyber sovereignty of countries and respecting the national cyber security of countries by all of the stakeholders.]

k bis) [State sovereignity and international norms and principles that flow from sovereignty applied to state conduct of ICT related activities and to their jurisdiction over ICT infrastructure within their territory ].

l) S]

m) [Promote confidence and trust in electronic environments/[cyberspace] globally by encouraging secure cross border flows of information, including electronic documents.]

**3. Targets**

ISOC: We would suggest removing these targets; their criteria and measurability are both unclear and too specific.

1. [Overall readiness in the field of confidence and security in the use of ICTs in all countries should be improved by 40% by 2020 – with specific focus on developing countries, including least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. The assessment of readiness in the field of confidence and security in the use of ICTs should take into account the current level of penetration of ICTs.
2. Building transborder space of confidence and security in the Internet at the international and regional levels by 2020.
3. Ensuring [maximum] level of child on-line protection by 2020.]