

**Document Number: V1.0/C/ALC5**

Note: This document consists of the Annex for the Action line and consolidates the comments received from WSIS Stakeholders for the:

* Proposed zero draft <http://www.itu.int/wsis/review/mpp/pages/phase1-submissions.html>
* Proposed first draft <http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html>

Please note that this document is not for comments it is only for the purpose of information.

Draft WSIS+10 Vision for WSIS Beyond 2015

С5. Building confidence and security in the use of ICTs

**Annex: Zero Draft Stakeholder Contributions**

1. **Engagement of all stakeholders, cooperation:**
2. Recognize that the open nature of the multistakeholder process has proved adept at developing innovative solutions to technical and policy problems. The WSIS process should guide governments to **look beyond solely legislation and government-led solutions**, in order to both harness the existing knowledge and expertise of the multistakeholder organizations, and engage with them to enhance and improve the existing solutions.
3. **Need Multistakeholder cooperation** to foster a global culture of cybersecurity.
4. Appreciate that many confidence and security solutions are developed in **cooperation between different stakeholders including industry, academia and governments**.
5. Recognize that the **technical community and the private sector have critical expertise** that should be better incorporated into cybersecurity related policy-making.
6. Encourage **governments to work with the business sector** **and civil society** on a more regular basis.
7. Stress the **need for national, regional and International multistakeholder cooperation** against cyber attack
8. Encourage multistakeholder **cooperation and sharing of information between the public and the private sectors and on the interregional level** in order to maintain the protection and security of networks and information systems and the protection of national cyberspace, including the application of the security measures, resilience and recovery for local networks and computer systems
9. Pursue greater cooperation toward achieving **cohesive, compatible, cybersecurity frameworks** among all stakeholders, which is in line with international human rights norms,
10. Recognize that while malicious actions can undermine users’ trust and confidence in the network, but **cutting off Internet access is not the solution**. Instead, we need to focus on ensuring the Internet is stable, secure and resilient. To do so, it is important that these **issues be addressed by all stakeholders in a spirit of collaboration and shared responsibility**. It is also important that these issues be addressed in **ways that do not undermine the global architecture of the Internet or curtail internationally recognized human rights**.
11. Ensure that critical infrastructure is managed by professionals in ICT. 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 which will hold them accountable, in this way trust will be assured.
12. **Strengthening enhanced cooperation**, to enable governments, as well as all stakeholders, on an equal footing, to carry out their roles and responsibilities on an equal footing, in international public policy issues pertaining to the Internet. [Delete]
13. **Cooperate with all stakeholders, particularly** manufacturers and operators, to pave the way toward the achievement of the **“security by design”** concept, where devices and products contain standard security features to reduce the exploitation of vulnerabilities
14. Condemning and prohibiting any kind of espionage or gathering private information of any foreign person, company or government without their consent by using ICTs.
15. Promoting cooperation between governments within the United Nations and with all stakeholders at other appropriate forums to enhance user confidence and protect data and network integrity; considering existing and potential threats for ICTs, and addressing other issues of information security and networking.
16. **Frameworks addressing cyber security:**
17. Strengthen and enhance the legal and regulatory frameworks to ensure that private sector and the other stakeholders do necessary measures to protect users against cyber threats.
18. Recognize the **growing importance of pursuing national, regional and international frameworks to mitigate/protect against cyber threats**
19. Through a programme of **multi-stakeholder cooperation**, implement comprehensive cyber-legislation in line with international treaties and conventions (including human rights instruments) at the global and regional level to cover all topics related to cyberspace, in particular those related to cyber-attacks,,; [Delete]
20. Emphasize the need for an **frameworks focused on the elaboration of norms and principles agreed at national, regional and global levels**, specifically in the following areas:  
    - access to the Internet  
     - cybersecurity  
     - protection of fundamental rights  
     - state involvement and  
     - international/regional cooperation
21. Recognize the urgent need for **building frameworks** to address existing and emerging cyber-attacks at national, regional and international levels. [Delete]
22. Encourage stakeholders to **invest in existing fora** that work to build confidence and security in ICTs. While new national, regional, and international frameworks may be appropriate in some cases, there is already an ecosystem of entities and structures that address the issue of cybersecurity.
23. Encourage that all **frameworks must be subject to "evidence-based policy-making**" involving all stakeholders and the necessary expertise.
24. Recognize that **cloud computing delivers economic and societal benefits and may which may raise jurisdictional questions** and needs careful examination.
25. Note that more than ten year implementation of the Cybercrime Convention has brought forth a range of **measures and partnerships against cybercrime. They have to be enriched further on a global and regional level**.
26. Develop appropriate **national legal and regulatory framework for privacy protection, e-transactions and Cybersecurity** [Delete]
27. Encourage **enhanced cooperation to develop solid frameworks and operational processes** to address cybersecurity, cyber-attacks, spam and related abuses at the national, regional and international levels
28. Highlight that any emerging international framework focused on the **elaboration of norms and principles in the area of access to the Internet** will need to address public access if we are to ensure that needs of everyone in the information society are met.
29. Establish special regional structures in order to build confidence in using ICT within the region.
30. Recognize the need for an **international framework to cooperate on cybersecurity matters** and to avoid unilateral assertions of national laws and to avoid extra-territorial actions. All countries should consider the principles posted at "necessaryandproportionate.org", both when developing or revising national legislations, and as a possible new Resolution or Statement. [Delete]
31. Recognize the need for **international agreement to cooperate on security matters** and to avoid unilateral assertions of national laws and to avoid extra-territorial actions. In this context, states shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in a manner that respects and upholds their human rights obligations, and they should consider best practices regarding human rights, in particular those put forward by civil society organizations.
32. Need framework for the **protection of personal data at cross-border level.**
33. Establishment of international framework to address cyber conflicts and wars among countries
34. Respecting to the laws of each jurisdiction by all of the stakeholders and recognizing the nation-state’s legitimate right to prosecute any breach of its law which lead to harm to its ICT infrastructures and services as well as its citizens in/through cyber space.
35. Preventing, detecting, and responding to cyber-crime and misuse of ICTs by establishing legislation that allows for effective investigation and prosecution of misuse; promoting effective efforts of mutual assistance; strengthening institutional support at the international level for the prevention, detection and recovery of these incidents, and encouraging education and awareness.
36. **Technical and procedural measures:**
37. Recognize the **importance of the concept of “security by design”, especially amongst the business sector** when providing products and services.
38. Outline standards and adopt novel and innovative methodologies on how to develop **safe and reliable e-services and applications resilient to external risks and threats**, including necessary mechanisms to maintain the privacy and confidentiality of personal information and the development of multilingual tools in particular
39. Develop and integrate technology, protocols and standards improvements that introduce **native capability for network** security while maintaining stability and interoperability.
40. Develop an **effective and efficient equipment certification process** and ensure adherence to global standards benefits both the industry and users, as it protects the integrity of the telecom networks, guarantees that consumers get standard equipment that works and prevents frequency spectrum interferences.
41. Facilitate the **introduction and expansion of electronic transactions** over the Internet and the development of efficient security systems in this regard.
42. Recognize the **urgent need to introduce cyber risk analysis and risk management** and Develop a **better understanding and analysis of the threats and actors involved**; this would allow for more tailored and proportionate policy responses.
43. Encourage and support the increasing importance of **proactively identifying vulnerabilities** in critical resources, infrastructures and key priorities relying as part of a cyber security plan involving all stakeholders
44. Promote World Standards Cooperation
45. Focus on security in **mobile devices and the Cloud**, security of **critical infrastructures**., computer security for **national defense**
46. **Organizational Structures**
47. Realize the need to establish strategies and capabilities at the national level to ensure protection of national critical infrastructures, while enabling prevention and prompt responses to cyberthreats. Also the **establishment of Computer Incident Response Teams (CERTs) with national responsibilities** and national cybersecurity frameworks are key elements towards the achievement of cybserecurity.
48. Encourage with appreciation the growing deployment of national Computer Incident Response Teams.
49. Encourage and **support Security and Emergency Response Team at the Government and Business level**.
50. Establish ISMS (**Information Security Management system**) in each organization
51. Create **alert centers** in those countries that do not have one
    1. Enhance alert centers in those countries that have one
    2. Promote the interconnection of the alert centers
52. Establish the **NISC (National Information Security Center) within the government to promote measures relating to information security**. The NISC establishes basic strategies on information security, promotes and assists measures on security for the government.
53. **Capacity Building**
54. Recognize that prevention represents an important stage in the fight against attacks in cyberspace. It is a broad category encompassing the elaboration of standards as well as practical steps such as: constant provision of information about the opportunities and the risks of the Internet; formation of special skills and behaviour of users and especially of young people; distribution of sufficient materials; organization of campaigns; promotion of good models and practices, etc.
55. Emphasize the importance of accounting for the “**human element” as priority**. 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, make a commitment to a code of ethics and professional conduct and have regard to the society which they serve which will hold them accountable, in this way trustworthiness will be assured.
56. Recognize the **urgency to build human capacity**, to improve the skills and expertise of security professionals and increase the awareness of the general public
57. Build **national and regional capabilities** in the field of Cyber-Security. There is a need to continue building national and regional Computer Incident Response Teams.
58. Promote **Education for safety and security** of Internet usage. Raise **public awareness in regards to online safety** at large for all segments of users with various aims.
59. Encourage **campaigns by the governments and other stakeholders** to promote people’s awareness about the importance of confidence, safety and security in cyberspace and empower them to protect themselves against the threats.
60. Promote **dialogue on confidence and security issues between all stakeholders**. The security of the individual must be further prioritized.
61. Contribute to the **building of a “national culture of cyber security”** through proper awareness and education campaigns regarding online risks particularly those affecting children
62. Enhance ICT literacy that includes **knowledge on information morals and information security**
63. Encourage the education and training institutes to develop related programs on cyber security to ensure the **availability of qualified human resources**.
64. Provide **assistance to countries needing help** in setting up national cybersecurity strategies and the creation of national Computer Incident Response Teams (CERTs). This could be provided in a number of ways **including by bilateral assistance from those countries that have already set up national strategies and CERTs**.
65. Aim to **educate government officials on non-legislative solutions available to them**, and facilitate bringing together technical experts - from the business community and civil society - and policy makers in developing countries. As the issues faced by the stakeholders engaged with Internet security develop rapidly it is difficult for legislation to keep up with the pace of technological change. Engaging with, and benefiting from, international best-practices and policies developed by the multistakeholder organizations can be a more effective way to enhance security for all stakeholders.
66. Develop an **effective assessment mechanism on the ISP’s security capability**; Encourage **industry self-discipline on content management**; Awareness-raising for Internet users
67. **Privacy, Data protection, Intellectual property**
68. **Protect the privacy and personal data** in the various processes of information processing in the public and private sectors
69. **Protect intellectual property and copyright frameworks that are in line with universal human rights to freedom of expression and access to information.**
70. Raise the **awareness on the IPR and related rights.**
71. Promote **respect for privacy in the digital age**. Business, civil society and government should work together in developing practices aimed at ensuring protection for personal data in a manner that not only provides effective protection of personal data and privacy, but also enables the data flows that are needed by new technologies and business models to foster both economic growth and societal benefits.
72. Promotion of **personal data utilization and circulation considering privacy protections** etc.
73. Clarify rules regarding utilization of personal data that considers the **balance between free circulation of information and protection of privacy**
74. Enhance utilization and circulation of information that contains personal datum that crosses over borders through network
75. Recognize the **contradictions between surveillance and security**, with one undermining the other.
76. Note that **Public confidence in the privacy of personal data has been shaken** by a) the increasing use of personal data by commercial enterprises to maximise business revenues, with **limited control available to individual users over their own information**; and b) recent revelations concerning the extent of mass surveillance of personal data and communications, including internet use, by government agencies. These two factors threaten public confidence in ICTs and especially the internet, and could in particular inhibit the use of cloud computing. They also raise the risk of data becoming available to criminals and so increase the vulnerability of electronic commerce.
77. Concern about the **importance of data privacy and data protection**, resulting from changes in the capabilities of technology, the depth and intrusiveness of analysis of data now undertaken by commercial businesses, and recent revelations concerning surveillance by governments. These are likely to be **exacerbated by the spread of cloud computing and the advent of the internet of things**. Public confidence in ICTs and the internet depends on data privacy and data protection, which should be given greater emphasis in this Action Line.
78. A new concept of **data protection under the conditions of cloud computing to be formulated** and **cross-border instruments for investigation** be elaborated.
79. **Human Rights, Freedom of Expression**
80. Recognize that **Freedom of expression and the media can be crucial tools** for attaining all enlisted goals and the media can be a valuable partner in the fight against cyber-attacks and other cyber offences and risks. Freedom of expression on the one hand can boost positive attitude and on the other help in exchanging relevant information and good practice.
81. **Concern for the catch-all approach to the issue of cybersecurity and the use of invasive and disproportionate policy responses** that can imperil human rights and economic development
82. When addressing cybersecurity it needs to be done holisticallytaking into account **the protection of individual citizens** **as well as ICTs and internet access and services for society as a whole.**
83. **Protection of the vulnerable**
84. Emphasize the urgency to **ensure that the child online safety element is imbedded in the work stream of Action Line C5**
85. Need **special protection against harmful and inappropriate behavior on the net**. With regard to this **children and the most vulnerable have to be particularly protected** **and educated** how to communicate in the new information environment.
86. Emphasize that it is **critical to provide parents and children with the information they need** to navigate cyberspace in order **to create a trusted environment** that will encourage children to go online.
87. Encourage **broad cooperation between national authorities and social partners** (including the owners of the servers and Internet portals, foundations, etc.) in order to protect children from the illicit content.
88. Encourage **Governments, educators, civil society and industry together to help parents and children** understand how to maximize the benefits and minimize the risks of being online.
89. Develop responsible practices, clear information, robust education and coordinated law enforcement efforts that can greatly improve the level of safety children experience online.
90. Emphasize that **special protection should be offered against cyberbullying, online harrasment and cyberattacks.**
91. Prioritize **Digital literacy among girls and women** .
92. All stakeholders should commit to provide a safer ICT services particularly internet for child and family to fulfill their obligations based on the UN Convention on the Rights of Child and its optional protocols.
93. Encourage all stakeholders to work to establish Child Online Protection (COP) frameworks to promote and harmonize the necessary activities to provide safer internet for child at regional and national level.
94. Develop **policies to guide child online protection**.
95. Emphasize the **need to protect children from accessing undesirable content, including child pornography**.
96. Highlight **violence against women online** which presents a serious threat and inhibitor for women’s use of ICTs; privacy issues.
97. Insisting and reaffirming the Tunis agenda as a separate point which says “incorporating regulatory, self-regulatory, and other effective policies and frameworks to protect children and young people from abuse and exploitation through ICTs into national plans of action and e-strategies”(par.90.q.)
98. Adding Child Online Protection as a main component to the ICT regulatory framework and related laws to to support the victims of cyber crimes.
99. Insisting on helpline and hotline establishment at national, regional and international levels and providing fund and the other technical assistance for less developed countries by the UN or developed countries to implement their commitment to the Tunis Agenda which insists on Helpline“We encourage countries, and all other interested parties, to make available child helplines, taking into account the need for mobilization of appropriate resources. For this purpose, easy-to-remember numbers, accessible from all phones and free of charge, should be made available.”(par. 92.)
100. Developing and Promoting positive contents for child and family should be included in the government's strategical road map to .
101. **Spam**
102. **Promote measures against spam mail to prevent the propagation of spam and minimize its impact on international telecommunication services.**