REPORT BY THE LEADERSHIP TEAM OF THE IGF DYNAMIC COALITION ON INTERNET STANDARDS, SECURITY AND SAFETY (DC-ISSS) ON WORK UNDERTAKEN DURING 2020

DC-ISSS - Making the Internet more secure and safer

Launch of the DC-ISSS at IGF 2020

The Dynamic Coalition on Internet Standards, Security and Safety (DC-ISSS) was launched at the IGF on 6 November 2020. It brings together expert stakeholders from the technical community, civil society, governments and regulatory authorities, and corporate and individual adopters, with the shared goal of making online activity more secure and safer. Its objective is to make policy recommendations and guidelines that will promote more rapid and widespread deployment of security-related Internet standards and best practices.

Background

Internet and ICT security is an issue that is high on the agenda of governments, industry and individuals alike. The COVID-19 pandemic has brought into sharp focus the rapid increase in society's dependency on the Internet, communications technologies and networks, interconnectivity of devices, and the vast array of online services, networks and applications that permeate all social and economic sectors, and every aspect of daily life, including our health and financial welfare.

It is also widely recognised that many existing and future Internet-related products and services will be vulnerable to security threats and the spread of online harms and criminal misuse, if relevant standards are not effectively deployed worldwide to reduce and prevent these risks. A concern that adds to this conclusion, is that current education curricula do not match the level of expertise needed where Internet security, governance and architecture are concerned.

DC-ISSS Objectives

Consultations were held prior to IGF2020 with a range of stakeholders who had expressed support for the establishment of a follow-up process to the IGF Pilot Project on Internet Standards conducted in 2018-19. Accordingly, the primary purpose of the DC-ISSS will be to make recommendations and provide guidance for decision-takers, with the following objectives:

1. Solutions are identified for addressing barriers to the global deployment of security-based Internet standards.
2. Public sector procurement and supply chain management best practice takes into account Internet security and safety requirements.
3. Security awareness and skills gaps are addressed through the inclusion in educational curricula, vocational training and induction programmes, detailed coverage of cybersecurity, Internet standards, Internet architecture and best practices such as producing secure coding guidelines, designing more secure IoT devices, and developing more secure website applications.

4. The knowledge gaps between the technical community, Internet policy advisers and users of standards is addressed through creating a voluntary global network of expert liaisons and commitments to develop a repository of best practice.

First phase of work since the launch of the DC-ISSS in November 2020

A stakeholder survey of priorities was conducted at the time of IGF 2020 which confirmed support for establishing three thematic working groups in the first phase of the DC-ISSS work plan for 2020-21, on the following themes:

WG 1: Security by design – Sub group 1: Internet of Things;

WG 2: Education and skills;

WG 3: Procurement, supply chain management and creation of the business case.

These working groups held their first meetings in November 2020 and all three agreed as a first step to collate and analyse recent and current initiatives, and best practice (with second meetings held in January 2021 to review progress in receiving inputs and submissions).

Stakeholders are invited to subscribe to the DC-ISSS mail list for updates on the progress of the coaltion and for details of upcoming meetings of the working groups at http://intgovforum.org/mailman/listinfo/dc-isss_intgovforum.org

During the period since the launch of the coalition, the DC-ISSS leadership team has continued its programme of outreach in the form of virtual meetings with potentially interested stakeholders in governments, parliamentary groups, IGOs, the business community and technical sectors, civil society rights and consumer protection groups. These meetings had three aims:

i. to increase the membership of the working groups and enhance their sectoral and geographical diversity, and to ensure gender balance;
ii. to secure financial donations that will cover the secretariat and general administrative costs of the coalition;
iii. to invite nominations for chairs of the working groups.

This outreach programme continues in 2021. The Leadership team has also been considering how to involve young people and parliamentarians in the work of the coalition. Consultations on this are also continuing in 2021.

Planning for the second phase of work beyond IGF 2021

The three working groups are due to report the outcomes of their work, including draft recommendations and guidance, during the DC-ISSS session during IGF 2021. It is intended that these reports will be published as IGF outcomes. The Leadership team has started planning for a possible second phase of work for the coalition in

2021-22. The decision on whether to launch this would follow a review of the outcomes of the first phase and would be taken in consultation with the working group chairs and members at IGF 2021.

In particular, DC-ISSS members will be asked to consider if the establishment of new working groups, or sub-groups of the three current ones, would be necessary to examine specific questions and issues that do not fall within the remits of the current three working groups. These could potentially relate to consumer protection, testing of devices and other products, and other regulatory or self-regulatory incentives, which were all issues identified by the IGF Pilot Project in its report Setting the Standard for a more Secure and Trustworthy Internet .

31 January 2021

DC-ISSS Leadership Team:

Wout de Natris – Executive Coordinator   E: denatrisconsult@hotmail.nl

Mark Carvell - Senior Policy Adviser   E: markhbcarvell@gmail.com

Marten Porte – Policy Adviser   E: martenporte@hotmail.com