

UN Internet Governance Forum  
Dynamic Coalition on Internet Standards, Security & Safety (DC-ISSS)  
*Making the Internet more secure and safer*

**Working Group 3: Procurement and Supply Chain Management**

***Including security-related technical standards in public procurement contracts and supply chain management***

**Mission Statement**

This multi-stakeholder working group of the Dynamic Coalition on Internet Standards, Security and Safety (DC-ISSS) aims to improve the security and safety of the global Internet for all by developing recommendations and guidance for policymakers and decision takers so that requirements for security-related technical standards are included in public sector procurement contracts and supply chain management of digital technologies.

*1. Background*

Since 2006 the Internet Governance Forum (IGF) provides a non-binding, multi-stakeholder space for policy dialogue on Internet governance issues under the auspices of the United Nations. Governments, the private sector, civil society, the technical community and academia tackle current issues through open and inclusive processes.

One such process of the IGF is that of the Dynamic Coalition (DC). DCs are long-term intersessional groups dedicated to an Internet governance issue or set of issues. Their working mechanisms are transparent, their participants representative of a variety of stakeholder categories, and their work progress accountable through annual reports to the IGF secretariat and larger community.

The IGF's Dynamic Coalition on Internet Standards, Security and Safety (DC-ISSS) brings together key stakeholders from the technical community, civil society, policymakers, parliamentarians, regulators, academics, corporate implementers and individuals, with the shared goal of making the Internet and online activity more secure

and safer. The first two years' work of the DC-ISSS focuses on three collaborative areas in order to achieve this goal:

1. Security by design;
2. Education and skills; and
3. Procurement and supply chain business models.

### *2. Achieving change in procurement and supply chain management practice as a driver of security-related standards deployment*

The DC-ISSS Working Group 3 aims to develop actionable and practicable policy recommendations and guidance which will ensure public sector procurement and private sector supply chain best practice and related professional training takes into account Internet security and safety requirements. It is expected that the adoption of WG3's recommendations and guidance by government procurement agencies, trade and industry bodies, enterprises in the tech sector and standards bodies will make a significant contribution to the realisation of the DC-ISSS goal to make the Internet more secure and safer.

### *3. The Work Plan*

WG3's work plan below consists of three of phases of activities:

- i) issue mapping;
- ii) development of recommendations and guidance for policymakers and decision takers;
- ii) outreach and strategic engagement of relevant experts and stakeholders in order to advocate adoption of WG3 recommendations and guidance

The detailed actions planned in these three phases are summarised in Table 1 below.

#### Phase I: Issue mapping

In the first phase during most of 2021, WG3's will research the question "[what guidance exists?](#)" The aims of this work are to inform the second phase of developing policy recommendations and guidance and to review and amplify existing positive initiatives and processes which will be documented in a report to be published on the IGF website. Crucially this research will aim to identify common problems and gaps. The matrix criteria to be applied in the research will include breakdowns by region, institution and sector, as well as by specific products and services. In this way, the data collated on existing and previous initiatives will help to identify:

- a) common elements of best practice;

- b) shared problem barriers;
- c) challenges especially for Global South applicability;
- d) gaps for future research with the aim of identifying solutions.

### Phase II: Development of policy recommendations and guidance

In line with the outcomes of the research and policy and practice gaps identified in Phase I, the work plan will proceed in Phase II to identify solutions and develop proposals for adoption by policymakers and decision takers, including potentially

- Guidelines
- Policy Toolkits
- Checklists.

### Phase III: Outreach and participation

In the third phase of the work plan, the key contacts for policymakers and decision takers in all geographical regions and in relevant sectors will be identified in order to promote awareness, dissemination and adoption of the working group’s policy recommendations and guidance. Consideration will be given to holding webinars with the aim of promoting awareness in particular amongst stakeholders in the national, regional and global IGF networks and members of the DC-ISSS.

Table 1. *WG3 Work Plan actions*

<b>Outcome</b>		
Meeting global Internet security standards is a ubiquitous baseline requirement in any public or private sector procurement and supply chain management policy.		
<b>Objectives</b>		
1. Full scope of security standards and procurement challenges and opportunities.	2. Relevant and actionable guidance to require security standards in procurement.	3. Guidance influences public and private sector procurement and supply chain management.
<b>Activities</b>		
1.1 Conduct basic desk research to answer “What has been done by others to achieve [this project’s outcome]”? 1.2 Develop a decision matrix to narrow in on global	2.1 Circulate a short survey to procurement decision makers on challenges and opportunities in shifting policies. 2.2 Identify areas for improvement in existing	3.1 Circle back to decision makers with guidance. 3.2 Promote the DC-ISSS and its future work to decision makers. 3.3 Follow up to document outcomes, if any.

institutions within the UN IGF's sphere of influence and impact. 1.3 Collect and document existing procurement and supply chain policies of those institutions, and contacts list. 1.4 Adjust the work plan based on findings.	procurement and supply chain management policies for internet security standards. 2.3 Develop a guidance document (checklist, issue paper, etc), or suite of materials, fit for purpose. 2.4 Determine areas of future work and adjust the work plan.	
<b>Outputs</b>		
Issue paper (2021)	Guidance documents (2022)	Working group growth (ongoing)

**4. Contacts**

To learn more about the DC-ISSS Working Group 3 on procurement of digital technologies and supply chain management, the principal contacts are the WG3 Chair Mallory Knodel [mknodel@cdt.org](mailto:mknodel@cdt.org) and the Vice-chair Gustavo Ortega [gustavo@ortega.cr](mailto:gustavo@ortega.cr)

The DC-ISSS is led by the Coordinator, Wout de Natris [denatrisconsult@hotmail.nl](mailto:denatrisconsult@hotmail.nl) supported by Mark Carvell, Senior Policy Advisor [markhbcarvell@gmail.com](mailto:markhbcarvell@gmail.com). To subscribe to the DC-ISSS mailing including all three working groups, register [here](#).

=====  
Date: 22 June 2021