



Response to the UN Secretary-General's Technology Envoy on the Global Digital Compact

Submission by the Internet Governance Forum's Dynamic Coalition (IGF, DC) on Internet Standards, Security and Safety, Coalition (IS3C)

Haarlem The Netherlands, 21 April 2023

This submission is prepared by the Internet Governance Forum's Dynamic Coalition on Internet Standards, Security and Safety Coalition (IS3C), Global Digital Compact (GDC) team. As a world-wide stakeholder membership coalition, IS3C actively works towards, and is committed to, supporting the aims of the GDC in establishing an open, free, trusted and secure digital future for all. In achieving the remits of the coalition's aims and programme of work, IS3C members support the scope of the Compact, in particular, focusing on ensuring the security of digital technologies and applications, and to data protection. Our contribution sets out key proposals, along with practical steps to support the delivery of the commitments to action among the stakeholder groups.

Proposal for an eighth thematic area: Digital Security and Safety

Opinion canvassed from IS3C membership suggests that the Compact should include an additional thematic area focused on addressing world-wide demands for greater security and trust online. Internet and digital technologies would be more secure and safer if the principle of security-by-design was adopted throughout the development, manufacturing and procurement phases. Achieving this goal requires the active support of the technology industry sector, in particular the research community, standards developers, manufacturers to design and manufacture secure-by-design. The private and public sector's supply chain and procurement agencies must demand security-by-design during the procurement of ICTs and digital technology.

(i). Key principle: security-by-design

Security-by-design is proposed as a key principle that would underpin the Compact's critical focus on security and trust. IS3C members believe that adopting the principle of security-by-design would address the needs of individual, corporate and public sector users for online security and safety. The results would lead to more effective, universal and rapid adoption of existing security-related internet standards and ICT best practices, many of which currently have not been actively deployed, in the markets for devices, network services and ICT, often, due to costs, and a lack of awareness.

(ii). Commitments to action

The IS3C membership recommends that the principle of security-by-design should be adopted and implemented through commitments to action by the following stakeholder groups.



1. **Designers and developers** of new and emerging digital technologies, devices and applications, commit to embedding the principle of security-by-design in their activities and projects with the result that their devices and applications deploy the latest relevant security-related standards and best practices.
2. **Manufacturers** of devices and network applications commit to requiring the deployment of the latest relevant security-related standards and best practices in the specifications of their product lines.
3. **Procurement agencies and corporate purchasers** commit to demanding from suppliers secure by design products, services, applications and devices.
4. **Procurement agencies and corporate purchasers** cooperate with **suppliers** in ensuring the maintenance, review and updating of the security requirements and provision of the devices and network applications which they procure in order to ensure their long-term sustainability, without fear of early obsolescence and vulnerability to new means of attack and criminal misuse.
5. **Educational and vocational training establishments** commit to including in their curricula and training modules comprehensive information relating to cybersecurity requirements, including up-to-date information about current security-related technical standards. This would ensure that graduates and new entrants in the cyber industry have the necessary technical skills that the industry requires for the design and development of new devices and applications.
6. **The manufacturing sector** commits to promoting greater transparency about the security specifications of their products and to making available to procurers and users the necessary information so that they are better informed about their security and safety.
7. **Manufacturers and suppliers** commit to ensuring that procurement agencies and supply chain managers are kept up-to-date with the latest updates and data on the deployment of security-related standards in their digital products.

These stakeholder commitments are set out in the table attached to this submission at Annex A: together with a general statement on cooperative actions to increase consumer awareness of the importance of greater security, safety and trust online.

The members of the IGF's IS3C coalition believe that a higher level of trust in the Internet will be achieved through the adoption of the principle of security-by-design along with implementation of the commitments to action, and the cooperation by key stakeholders as listed above. The IS3C proposal includes policies and actions that will ensure a trusted and predictable way ahead for current and emerging digital technologies to contribute to enhancing social and economic welfare. In addition, successful delivery will reduce online risks and threats in all countries and regions that are currently experienced.



As a multi-stakeholder coalition representing our world-wide membership, IS3C is ready to contribute to the delivery of the GDC's actions to successfully implement the Compact, as will be agreed; and, contribute to the successful launch of the GDC at the Summit of the Future in September 2024. Further information about IS3C's aims and programmes of work are available on the Internet Governance Forum's website: <https://www.intgovforum.org/en/content/internet-standards-security-and-safety-coalition-is3c> and the IS3C website: <https://is3coalition.org/>.

Please feel free to contact us for further information.

With best regards,

The IS3C GDC Team:

Dr Allison Wylde (Chair GDC team, IS3C)
Mr Mark Carvell (Senior Policy Advisor, IS3C)
Mr Wout de Natris (Co-ordinator IS3C, contact for correspondence)

Submitted by:

Mr Wout de Natris, Coordinator, IGF Dynamic Coalition on Internet Standards, Security and Safety (IS3C)

E: wout.denatris@is3coalition.org

Annex A



Annex A

Response to the UN Secretary-General’s Technology Envoy on the Global Digital Compact: Submission by the Internet Governance Forum’s Dynamic Coalition (IGF, DC); Internet Standards, Security and Safety, Coalition (IS3C)

Table 1. Commitments to Action and Leading Stakeholders

Commitments to Action	Key Stakeholders
<p>1. Adoption of the principle of security by design regardless of cost throughout the development and manufacturing stages of Internet devices and applications.</p>	<p>Emerging technologies’ researchers, designers and developers of new digital devices and applications; with the support of national and regional governmental bodies and administrations.</p>
<p>2. Adoption and implementation of current security-related standards.</p>	<p>Supply side: Developers, manufacturers and suppliers of digital devices, services, soft and hardware, ICT and network applications.</p> <p>Demand side: Governmental procurement agencies; industry purchasing departments; top management buy-in; consumer advocacy organisations; consumers.</p>
<p>3. Inclusion in educational curricula on cybersecurity and training manuals; comprehensive and up-to-date information and advice on security-related standards.</p>	<p>Educational and vocational training establishments; with the support of national and regional education administrations, representative technology institutions and the standards development organisations (SDOs) including the Internet Engineering Task Force (IETF) , the International Telecommunication Union (ITU), ISO, IEEE, NIST, NSA, ??.</p>
<p>4. Establishment of data governance requirements and mechanisms that build greater trust amongst private, corporate and public sector users.</p>	<p>Private and public sector policymakers, data and information regulators; with the support of digital technology manufacturers and suppliers</p>
<p>5. Increasing consumer awareness on how to ensure greater online security, protection and the safer use of digital devices and applications.</p>	<p>National and regional administrations, consumer protection agencies, consumer advocacy organisations and private sector providers of consumer advice.</p>