SBS position on the Commission's proposal for the creation of a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

January 2019

➢ BACKGROUND

Building on the 2017 strategy to set up a wide-ranging set of measures to build strong cybersecurity in the EU, the European Commission launched a proposal for a new regulation to create a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

This initiative should help to **create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem, generating a stimulating environment for digital SMEs**. Small Business Standards (SBS) expects this to be done building on the existing standardisation ecosystem, aiming to create the best conditions for European cyber SME champions to compete on global cybersecurity markets.

The proposal defines the level of interaction of **three main entities** that, together with the European Union Agency for Network and Information Security (ENISA) will set the cybersecurity scene at European level. (i) The **European Cybersecurity Competence Centre** will facilitate and coordinate the work of (ii.) the **European Cybersecurity Competence Network**, made of 27 National Coordination Centres, and nurture (iii.) the **Cybersecurity Competence Community**, i.e. a large, open, and diverse group of actors involved in cybersecurity technology, including research entities, supply/demand-side industries and the public sector.

Furthermore, the proposal aims at placing the Union "in a position to autonomously secure its digital assets and to compete on global cybersecurity market". European digital SMEs play an important role in achieving such objective. **Cybersecurity technology is changing rapidly and only**

Small Business Standards aisbl • Rue Jacques de Lalaing 4 • 1040 Brussels, Belgium
info@sbs-sme.eu • T +32 (0)2 230 75 99
Transparency Reg 653009713663-08

the SMEs, due to their agility, can provide the cutting-edge solutions needed to remain competitive.

This position paper provides an overview of standardisation-related measures that, if adopted and well implemented, would contribute to the effective functioning of the new European cybersecurity ecosystem.

➢ Suggested key principles:

I. Ensure that investments are coordinated at European level to the benefit of SMEs

The European Commission has placed cybersecurity high on the agenda in its proposals for the next long-term European Union's budget for the period 2021-2027 and the proposed instrument intends to establish a body dedicated to implementing cybersecurity actions under Digital Europe Programme and Horizon Europe Programme. This should allow an efficient management of funds to allow pooling resources at the Member States' level and/or develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure).

To achieve this objective, the proposal to invest 2 billion euros under the new Digital Europe Programme to boost European Union's (EU) cybersecurity industry and finance state-of-the-art cybersecurity equipment and infrastructure must first look at European SMEs and be complementary with the efforts of the Digital Innovation Hubs initiative in supporting SMEs to improve their competitiveness. However, SBS regrets that the proposal does not foresee to provide financial support and technical assistance for SMEs in general and only for SMEs active in the cybersecurity industry. In addition, it has to be highlighted that the draft text of the Regulation on the Digital Europe Programme so far does not contain a legal basis to do specific actions towards SMEs.

The contribution of standardisation to innovation and research project under the Horizon 2020 framework has already proved impactful market results. Thus, it will be necessary to build on such successful integration of standardisation activities in research and innovation projects also in the framework of the Horizon Europe Programme (whose budget remains to be defined) so to ensure that European and international standardisation work will continue contributing to the uptake of breakthrough technologies in the field of cybersecurity.

It goes without saying that coherence in distribution of funds for research, capacity acquisition through tenders and pooling of resources must be achieved, both in terms operations (i.e. interaction between ENISA, European Cybersecurity Competence Centre and Standards Development Organisation) and timing. With this regard, it has to be noted that the negotiations on this European Commission proposal will end in mid-2019. In the meantime, a call for Horizon 2020 projects related to the implementation of cyber competence centres has been launched and 3 projects have been funded up to 50M€. Despite the short timeframe, it would be highly beneficial

to take into considerations the outcomes of these projects in order to fine-tune the organisation and functioning of the European Cybersecurity Competence Centre and European Cybersecurity Competence Network as currently conceived.

Build on the successful experience of the European Cyber Security Organisation (ECSO)

Some of the tasks that, in the proposal, are assigned to the European Cybersecurity Competence Centre, such as stimulating and supporting the cooperation and coordination of the activities of the cybersecurity community, are currently run by the European Cyber Security Organisation (ECSO).

The first European Public-Private Partnership ('cPPP') on cybersecurity achieved significant results in bringing together the efforts made by the research, industry and public sector communities in Europe. Now the proposal looks at the European Cybersecurity Competence Centre to handle this complex task.

In the last years, the role of ECSO has been decisive to connect buyers and vendors of cybersecurity products and solutions, including SMEs, in critical sectors (e.g. transport, health, energy, financial). Furthermore, **ECSO plays an important role in contributing to standardisation issues** such as standards for interoperability and EU cybersecurity labelling in strict collaboration with the European Commission, ENISA and European standardisation bodies.

Considering the above, we recommend that the European Cybersecurity Competence Centre builds on the experience of ECSO, to keep increasing the level of cybersecurity through standardisation while creating market opportunities and solutions for the growing needs of SMEs in all sectors.

Facilitate and accelerate standardisation and certification processes

The EC proposal refers to the need to facilitate and accelerate standardisation and certification processes, in particular those related to cybersecurity certification schemes as intended in the previously proposed Cybersecurity Act. Again, as these processes are mostly industry-driven and require the involvement of Standards Development Organisations.

SBS advocates a fruitful collaboration between the European Cyber Competence Centre and European Standardisation Organisations and SBS and, at national level, between the National Competence Centre, the SME organisations and the National Standardisation Organisations so to ensure the uptake of existing standards to whose development the SME community is contributing also through the involvement of SBS experts.

Small Business Standards aisbl • Rue Jacques de Lalaing 4 • 1040 Brussels, Belgium
info@sbs-sme.eu • T +32 (0)2 230 75 99
Transparency Reg 653009713663-08