CEN – European Committee for Standardization
CENELEC – European Committee for Electrotechnical Standardization

CEN Identification number in the EC register: 63623305522-13
CENELEC Identification number in the EC register: 58258552517-56

CEN and CENELEC response to the EC Public Consultation on the contractual public-private partnership and possible accompanying measures

March 2016

Executive Summary

CEN and CENELEC welcome the opportunity to respond to the EC consultation on the contractual public-private partnership on cybersecurity and possible accompanying measures.

European Standardization is a powerful tool to help achieve the EU objectives, and the **European Standardization System** provides an adequate framework to set the best conditions to enable the creation of cybersecurity standards for Europe.

Voluntary European standards are **innovation-friendly**, **market-driven** tools – the output of a **coherent**, **inclusive**, **results-driven**, **dynamic** system built on **partnerships** with all industry and societal stakeholders.

CEN and CENELEC **links with ISO and IEC** are key strengths in international markets and full advantage should be taken of using international standards within Europe, where supported by stakeholders.

Through 33 national members active in ICT standardization for over 20 years, CEN and CENELEC have a strong European network with **global outreach** through ISO and IEC that can provide the framework for Europe to capture global market opportunities.

CEN-CENELEC Management Centre, Avenue Marnix 17, 1000 Brussels, Belgium
T: +32 2 550 0811 – F: +32 2 550 0819 – info@cencenelec.eu – www.cencenelec.eu

Standardization for cybersecurity requires cohesive and committed approach from all stakeholders to embrace the diverse and growing spectrum of technologies and applications.

The European Standardization System is a unique asset for Europe that **with the support and engagement of the Commission and the EU institutions will develop the needed cybersecurity standards.**

CEN and CENELEC are active members of the Multi-Stakeholder Platform on ICT Standardisation (MSP). This platform has identified Cybersecurity as one of the priorities in its advice to the Commission on the Priority Plan on ICT Standardization. This advice was endorsed by CEN and CENELEC.

Our societies are increasingly being confronted with various kinds of security threats, including man-made threats such as terrorism and organized crime, natural disasters, pandemics and major technical accidents.

The ability of the responsible public authorities and emergency services to respond to such threats depends on having common terminology and procedures, compatible equipment and communication systems. Standardization can contribute to overcoming fragmentation in this field by increasing interoperability and compatibility of systems and products.

The security of information and communication systems (or 'cybersecurity') is an area of increasing concern, both for public authorities (from local governments to international organizations) and for private companies (from micro-enterprises to large multinationals). A CEN/CENELEC/ETSI Cybersecurity Coordination Group (CSCG) was set up in 2011 to handle political and strategic matters related to cybersecurity standardization.

The Cybersecurity Coordination Group (CSCG) acts as a single point of contact for pan-European interchange on Cyber Security standardization and will provide a set of recommendations and advice to the European Commission (DG CONNECT and DG ENTR) and EU Member States in the area of Cyber Security standardization. Additionally, the Coordination Group liaises actively with the European Union Agency for Network and Information Security (ENISA) and the Multi-Stakeholders Platform on ICT standardization.

Most important, the CSCG's efforts towards the harmonization of Cybersecurity in Europe are targeted at the high level, aiming to strengthen strategically the European digital economy and to provide a solid security platform for continued growth in Europe's Digital Single Market.

The Group has focused on the definition of a European roadmap on cyber security standardization and supports global initiatives on cybersecurity standards that are compliant with EU requirements in view of development of trustworthy ICT products, systems and services.

The CSCG developed a document (White Paper) with proposals addressed to the European Commission. The CSCG White Paper 'Recommendations for a Strategy on European Cybersecurity Standardization' was presented to Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, on 2 April 2014.

In 2016, the Coordination Group will change its status into a Focus Group (always named 'CSCG') to better support its parent organizations in exploring ways and means for supporting the implementation of the trustworthy Digital Single Market in terms of cybersecurity aspects and data protection.

In responding to this public consultation, CEN and CENELEC recall their response to the public consultation on the development of the Priority ICT Standards Plan: "Standards in the Digital Single Market: setting priorities and ensuring delivery", in December 2015. In that response, which was based on input from the national members, CEN and CENELEC indicated that standardization of cybersecurity is their number one priority.

This CEN and CENELEC response incorporates input provided by the CSCG.

CEN and CENELEC believe it is essential to stop differentiating between standardization policies for ICT and non-ICT applications.

CEN and CENELEC wish to engage with the PPP on cybersecurity and contribute actively to the development of the accompanying measures.

CEN and CENELEC await with keen interest the overall conclusions of the Consultation that will shape the focus and activities of the PPP on cybersecurity.

Detailed Replies

I. Identification of your priorities in cybersecurity

2.2. Applied Cybersecurity -> Application areas with demand in cybersecurity products/services

- ○ Critical infrastructures in general
- ⊙ Energy
- ⊙ Transport
- ⊙ Health
- ○ Finance and Banking
- ○ Public Administration
- ⊙ Smart Cities
- ⊙ Digital Service Providers
- ○ Protection of individual users
- ○ Protection of SMEs
- ○ Other

Please specify

CEN and CENELEC believe that all sectors will be affected by cyber risks and will need solutions underpinned by standards. Currently, products and services are not very well known. There are insufficient EU protocols available based on European standards.

2.3. Applied Cybersecurity -> Specific IT technology areas with cybersecurity as a functional requirement

- ⊙ Internet of Things
- ⊙ Embedded Systems
- ⊙ Cloud Computing
- ○ 5G
- ⊙ Big Data
- ○ Smartphones
- ○ Software Engineering

- ○ Hardware Engineering
- ○ Other

II. Assessment of cybersecurity risks and threats

2. Preparedness

*

2.1. Are the necessary products/services available on the European market to ensure security of the whole value chain.

- ○ Yes
- ◉ No
- ○ I don't know

It is our belief that a complete and coherent set of products and services relevant for European stakeholders is not yet available and that a coordinated and appropriate framework in which these products and services can be developed and delivered, underpinned by European standardization, is required.

4. Cybersecurity challenges by 2020

4.1. What will be the 3 main cybersecurity challenges by 2020? (Please explain)

The challenges relevant to recommendations of the CEN CENELEC ETSI Cybersecurity Coordination Group White Paper 2013 'Recommendations for a Strategy on European Cybersecurity Standardization':

1. The European Commission (EC) should mandate the CSCG to create a ***governance framework*** for the coordination of Cyber Security standardisation within Europe

2. The EC should establish a clear and common understanding of the ***scope of Cyber Security***, based on an initiative the CSCG plans to launch to clarify the ***key terms and definitions*** used in the standardisation of and communication related to Cyber Security within the European Union.

3. The EC should mandate CEN/CENELEC/ETSI to launch an initiative to re-establish the trust of the European citizen in the European digital environment, coordinated by the CSCG and aimed at producing standards to create the most trustworthy environment in the world; this should include privacy and harmonised objectives for education and awareness.

III. Cybersecurity Market Conditions

1. To what extent are markets in cybersecurity products/services competitive in Europe? Please provide your assessment of the overall situation in Europe and your views on the particular sectors of your expertise

Europe is a fragmented market, solutions in one Member State do not work in another.

4. How does European competitiveness compare to other countries/regions? In particular what are the strengths and weaknesses of European cybersecurity solution providers (self-assessment if you are a supplier)?

Good skills available but the market in Europe is fragmented.

5. Which level of ambition do you think the EU should set itself for cybersecurity market development?

	Retain global lead	Strive for global leadership	Make EU more competitive
Identity and access management	⊙	○	○
Data security	○	⊙	○
Applications security	○	⊙	○
Infrastructure (network) security	○	○	○

Hardware (device) security	○	○	⊙
IT security audit, planning and advisory services	○	⊙	○
IT security management and operation services	⊙	○	○
IT security training	⊙	○	○

6. How does legislation (currently in force or soon to be adopted) influence the European cybersecurity

Among other through the NIS Directive, EU Data Protection. There is the need to harmonize the different approaches.

In particular, with reference to the NIS Directive, CEN and CENELEC invites the European Commission to provide some clarification on how standards could support it. This could be done through the mean of a Standardization Request.

7. How does public procurement impact the European cybersecurity market? :

⊙ It is a driver behind cybersecurity market development and an opportunity for companies to increase market share,

○ It is a barrier to market access

○ I don't know

Please explain

EU Interoperability Framework; too many activities related to the situation at EU Member State level.

V. Specific Industrial Measures

1. How would you evaluate the current role of standardisation in the domain of cybersecurity?

1.2. In what areas is there a need/gap in this respect?

See the CEN CENELEC ETSI Cybersecurity Coordination Group White Paper 2013 'Recommendations for a Strategy on European Cybersecurity Standardization' (freely available from the CEN-CENELEC website)

1.3. Would you consider standardisation as a mean to support innovation and the digital single market in cybersecurity?

- (●) Yes
- ( ) No
- ( ) I don't know

Please explain your view

Voluntary **European standards are** innovation-friendly**,** market-driven **tools – the output of a** coherent**,** inclusive**,** results-driven**,** dynamic **system built on** partnerships **with all industry and societal stakeholders.**

It is widely accepted that economic growth relies on research, innovation and successful transformation of business. Digital technologies are transforming every area of economic life, so new sources of growth will come undoubtedly also from the exploitation of **transformative technologies** such as big data across industries and sectors.

CEN and CENELEC have been active in ICT standardization for more than 20 years. Their strong network cover a wide range of sectors, some of them ICT related, and others that might use or are using ICT. They have also developed a close partnership with the **European research and innovation community**, thereby creating the framework for innovation and research results to be smoothly channeled to the market.

1.4. Should standardisation in cybersecurity be addressed generically or should it focus on specific sectors (e.g. transport, energy, finance) and areas of application (e.g. connected vehicles,

smart-grids, electronic payments)? (Please specify your choice)

CEN and CENELEC believe it is essential to stop differentiating between standardization policies for ICT and non-ICT applications.

1.5. What areas should future cybersecurity standardisation efforts focus on? (Please specify).

The CEN – CENELEC Focus Group on Cybersecurity in 2016 will begin work to:

- Analyse strategic developments and issues in cyberspace, especially future challenges relating to the development of new and advanced technologies including overlaps with other sectors that may transcend the digital sector
- Systematically assess how standards can support regulations and policies related to the cybersecurity and provide regular inputs to the CEN, CENELEC and ETSI representatives to the ICT Multi-stakeholders Platform to ensure a coherent relationship between standardization and regulations/policies
- Examine the possibility for a common terminology and the building blocks for strengthening the cybersecurity capacities in Europe as a first step toward greater EU cooperation in the cyber domain
- Prepare an overview on suitable standards already publicly available (from the International Standards Organizations ISO, IEC and ITU or other sources) to meet specific needs for IT products, systems and services
- Identify and give due consideration to innovation/research projects impacting the cybersecurity domain

The result will be to identify cybersecurity standardization needs.

About CEN and CENELEC

CEN (European Committee for Standardization) and **CENELEC (European Committee for Electrotechnical Standardization)** are recognized by the European Union (EU) and by the European Free Trade Association (EFTA) as European Standardization Organizations responsible for developing and defining standards at European level. These standards set out specifications and procedures in relation to a wide range of products and services.

The members of CEN and CENELEC are the National Standards Bodies and National Electrotechnical Committees of 33 European countries including all of the EU member states plus Iceland, Norway, Switzerland, Turkey and the former Yugoslav Republic of Macedonia.

European Standards (ENs) are developed through a process of collaboration among technical experts nominated by business and societal stakeholders. Once adopted, these standards are implemented and published in all of the 33 countries covered by CEN and CENELEC.

CEN and CENELEC also promote the international harmonization of standards in the framework of technical cooperation agreements with ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). For more information, please see: www.cencenelec.eu