CEN/CENELEC/ETSI

Cyber Security Coordination Group (CSCG)

White Paper No. 01

Recommendations for a Strategy on European Cyber Security Standardisation

---

Version: 01.08

Contents

1 Executive Summary

The Cyber Security Coordination Group (CSCG) of CEN, CENELEC and ETSI is the only joint group of the three officially recognised European Standardisation Organisations with a mandate for coordinating Cyber Security standards within their organisations. The CSCG was created in late 2011 to provide strategic advice on standardisation in the field of IT security, Network and Information Security (NIS) and Cyber Security (CS).

This White Paper is the CSCG's response to the European Union's Cyber Security Strategy, which was jointly issued by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy on 7th February 2013. The CSCG's Recommendations listed below underline the importance of Cyber Security standardisation for the completion of the European internal market (i.e. unlocking business potential by the use of harmonised Cyber Security standards) as well as for increasing the level of Cyber Security in Europe in general. Both objectives need to be addressed through seamless and interoperable Cyber Security mechanisms, embedded into a coherent governance framework.

To this end the CSCG has formulated the following nine Recommendations:

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.
4. The EC should mandate CEN/CENELEC/ETSI to **establish an** initiative to produce standardised mechanisms for a strong, interoperable, trustworthy and transparent **European Public Key Infrastructure and strong cryptographic capabilities** for all participants in the European Digital Single Market.

5. The EC should authorise the CSCG to coordinate the standardisation work for a **high-level European Cyber Security Label** for information and communication technologies (ICT) to protect the European consumer (objective 4 of the EU Cyber Security Strategy).
6. The EC should mandate CEN/CENELEC/ETSI, with the CSCG coordinating appropriate harmonisation with the European regulatory bodies, to **extend existing European Cyber Security requirements and evaluation frameworks** to ensure adequate Cyber Security throughout the full ICT value chain and to establish an initiative for risk-based standardisation.
7. The EC should authorise the CSCG to **create a high-level interface between the CSCG and the European research community** to ensure alignment between standardisation and research including industrial research.
8. The EC, with the support of the CSCG, should **engage in an industrial forum** to harmonise Cyber Security Standards with key international players and stakeholders according to European requirements.
9. The EC, with the support of the CSCG, should **launch a targeted global initiative** to promote standards appropriate to European requirements for the development of trustworthy ICT products and services as well as Cyber Security solutions.

The individual Recommendations above target three areas of Cyber Security standardisation in the European Union:

- Governance (Recommendations 1, 2 and 3),
- Harmonisation (Recommendations 4, 5, 6 and 7) and
- Global Dimension (Recommendations 8 and 9)

of Cyber Security standardisation in the European Union (see section 3 below).

Through these Recommendations the CSCG encourages the European institutions to establish a global lead in Cyber Security standardisation, in line with the core values of the European Union (EU), and to take the necessary next steps to make the European online environment the safest in the world, as demanded by the EU's recently published Cyber Security Strategy.

2 The Cyber Security Coordination Group (CSCG)

2.1 Background to the CSCG

In 2011 the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI) – the three officially recognised European Standards Organisations (ESOs) – established the joint Cyber Security Coordination Group (CSCG). Its aim is to provide strategic advice on standardisation in the field of IT security, Network and Information Security (NIS) and Cyber Security (CS).

International standards promote worldwide trade, encouraging rationalisation, quality assurance and environmental protection, as well as improving security and communication. Standards have a greater impact on economic growth than patents or licences. Thus standardisation is an important strategic instrument for economic success.

International and European standardisation activities in the field of IT security and Cyber Security, as well as the prevention and detection of cybercrime, take place in many different standards committees and working groups. Standardisation also increases the opportunities for closer international cooperation in law enforcement agencies in their fight against cybercrime. Harmonisation and coordination between CEN, CENELEC and ETSI could positively influence the progress and the results of these standardisation efforts at the European and international levels.

Coordinated standardisation for products and services related to security is aimed at:

1. the avoidance of duplication,
2. improved interoperability,
3. trusted evaluation for a consistent level of security.

The objective is to help individuals to protect their autonomy and retain control over personal information, irrespective of their IT activities.

The CSCG is committed to coordinating Cyber Security standardisation effectively while CEN, CENELEC and ETSI foster the active engagement of European experts in international standardisation work and promote greater coherence between the international and European standards portfolios through a strengthened relationship with ISO and IEC. The

CSCG recognises that Cyber Security standardisation is an important economic stimulus for the completion of the European internal market.

The CSCG has set itself the following main tasks within the overall area of the standardisation of IT security, NIS and CS:

- Provide strategic advice on Cyber Security to the technical steering committees of CEN/CENELEC and ETSI,
- Analyse current and future European and international standards for Cyber Security,
- Define joint European requirements for European and international standards for Cyber Security,
- Suggest a European roadmap on the standardisation of Cyber Security, taking into account European Commission mandates as appropriate,
- Act as a contact point for questions from European institutions relating to the standardisation of Cyber Security,
- Coordinate and implement a joint European awareness programme for top management within the area of Information Security, to ensure managers have the right skills and knowledge to make the most appropriate decisions,
- Cooperate with US Standards Developing Organisations (SDOs) as well as SDOs in other countries working in the same field of standardisation,
- Suggest a joint US and European, as well as a multilateral, strategy for the establishment of a framework of international standards on Cyber Security,
- Coordinate European activities in international standards committees with the aim of implementing such a joint transatlantic strategy.

Drawing on their joint expertise, the members of the CSCG present this White Paper as strategic advice with recommendations to the European institutions. The White Paper is the result of the collaborative efforts of all CSCG Member Bodies[1].

[1] See Annex A for a complete list of the CSCG Member Bodies.

2.2 The CSCG's Claim

The CSCG claims the following position:

- The CSCG is the single point of contact for pan-European interchange on Cyber Security standardisation.
- The CSCG provides recommendations and advice to the European Commission and EU Member States in the area of Cyber Security standardisation.
- The CSCG coordinates Cyber Security standardisation efforts and initiatives and liaises actively with the Multi-Stakeholder Platform on ICT standardisation.
- The CSCG is the point of contact at a strategic level for extra-European organisations regarding Cyber Security standardisation.

3 The CSCG Recommendations

There are already many different technical standardisation groups working on Cyber Security, and the CSCG will not replicate their valuable work.

The CSCG's efforts towards the harmonisation of Cyber Security 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.

In particular, the CSCG has noted the trend that more and more suppliers of information and communication technologies (ICT) to the European market now come from outside the EU.

The recent proposal for a European Cyber Security Strategy is considered a first step, but it needs to be followed by a dedicated and sustainable effort towards the standardisation and harmonisation of Cyber Security across Europe in several different dimensions. These dimensions include a strong governance framework under which technical standards can be implemented efficiently and the need to protect the European consumer (objective 4 of the EU Cyber Security Strategy).

The CSCG considers *the re-establishment of trust* a key issue for the completion of the European Digital Single Market, and that Cyber Security standardisation is a crucial facilitator for the establishment of trust: mutual trust is based on agreed and transparent security standards, implemented in an interoperable way and available to all participants in the European Digital Single Market. Although there are many different technical security standards available, the interoperability between them is generally low, and fragmented segments of the European Digital Single Market remain isolated from each other. A *strategic* and EU-wide approach towards Cyber Security harmonisation is therefore essential. Such an approach will not only help to complete European internal Cyber Security, but also strengthen the whole European Digital Single Market by creating the required trust across national borders within the EU. In contrast to national *regulation*, where EU Member States often add national flavours to an agreed European baseline, *standardisation* addresses both sides of trust: the agreed baseline (creating trust) and the need for interoperability (spreading trust).

This White Paper derives its Recommendations from a strategic and structured top-down approach, considering:

- The opportunity for supporting the completion of the Digital Single Market by defining standardised and harmonised Cyber Security requirements.
- The opportunity to unlock business potential by the provision of strong, standardised and harmonised Cyber Security.
- The need to reduce cybercrime within the EU, which is becoming increasingly dependent on non-EU suppliers of ICT.
- The need to protect the privacy and security of the European citizen as a user of ICT products and services often produced or provided outside the EU.
- The unique position of the EU as a diversified union with strong fundamental rights and common core values, which apply as much in the digital as in the physical world.

The CSCG Recommendations are distributed over three different areas, addressing:

- the Governance of Cyber Security standardisation (see 3.1 below),
- the Harmonisation of Cyber Security standardisation (see 3.2 below),
- the Global Dimension of Cyber Security standardisation (see 3.3 below).

3.1 Governance

Technical standards can only be efficient if they are embedded into a strong governance framework, supporting their seamless implementation and assuring the required political support. Without such a framework at the European level, there might be only a partial exploitation of the benefits of Cyber Security standardisation.

3.1.1 Governance Framework

CSCG Recommendation # 1:

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

The CSCG recommends that the European Commission should consult the CSCG on all harmonisation and standardisation issues related to Cyber Security. Within the European Cyber Security initiative, the CSCG shall be the relevant point of contact for a cooperative network for the exchange of best practices, assisting its members in building coordinated capacity and steering the organisation of harmonised standardisation projects.

The CSCG also recommends that the European Commission should establish a legal framework throughout the EU, enabling the complete and seamless implementation of harmonised and mature Cyber Security standards.

3.1.2 Common Understanding of "Cyber Security"

CSCG Recommendation # 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.

To establish clear understanding, the CSCG recommends that the European Commission should harmonise its usage of the key terms "Cyber Security", "NIS" and "cybercrime" across the EU on the basis of existing definitions. Official communications currently use all three terms without distinguishing between them, which risks them being interpreted differently in different EU Member States (or languages).

The CSCG recommends that the European Commission should not limit its clarification to definitions but should also establish an agreed understanding of the interdependencies and relationships between the three areas in question. The CSCG also recommends that the Commission should establish and enforce a suitable governance model for the three areas, with special emphasis on avoiding working in silos on topics that are inherently intertwined.

3.1.3 Trust in the European Digital Environment

CSCG Recommendation # 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.

The average European citizen finds it difficult to determine which services on the Internet are trustworthy and which are less so. US-based providers dominate many market areas and there are different methods governing secure transactions in different EU Member States. It is thus not always easy to assess respective risks and to make the right choices to ensure security.

The CSCG recognises both identity management and privacy technologies as key elements for the protection of the European citizen, including but not limited to data protection. For many organisations, the proper management of identity information is crucial to maintain security of the organisational processes. Mature security solutions for identity management need to sufficiently address both anonymity and pseudonymity aspects to meet European privacy requirements. For the individual European citizen, strong and trustworthy identity management is important to protect privacy. An appropriate level of privacy is a prerequisite in re-establishing trust and creating confidence in European Cyber Security.

Any initiative for re-establishing trust should be well organised and managed on the basis of a reasonable assessment for continuity purposes.

Activities to improve the business environment for small and medium-sized enterprises (SMEs) should consider raising awareness of Cyber Security standardisation in the field, including how standards are developed and maintained and any special mechanisms used in the development of information technology standards. The CSCG therefore recommends an initiative for harmonised education about Cyber Security and cyber risk across Europe and the start of a European awareness campaign to bring Cyber Security to the attention of the European citizen as a personal concern rather than a technical menace. In addition, the CSCG

recommends an initiative to encourage European SMEs to take a more active role in Cyber Security standardisation activities to enable them to realise their full potential in today's global economy and to encourage them to help re-establish trust in the European digital environment

3.2 Harmonisation

Harmonisation of Cyber Security throughout the EU is essential to make the European digital environment the safest in the world, which is one of the expressed objectives of the EU's Cyber Security Strategy. Apart from infrastructure protection – which is already addressed in the EU's strategy – the European citizen, as the end user of ICT, must also be supported. This is especially important when the ICT in question is of non-European origin.

3.2.1 European PKI and Cryptographic Capabilities

CSCG Recommendation # 4:

The EC should mandate CEN/CENELEC/ETSI to **establish an** initiative to produce standardised mechanisms for a strong, interoperable, trustworthy and transparent **European Public Key Infrastructure and strong cryptographic capabilities** for all participants in the European Digital Single Market.

There is currently no well-functioning, pan-European, trustworthy and transparent Cyber Security capability available to European citizens. Most citizens are not protected when communicating (e.g. when sending e-mail) across European internal borders and are unable to digitally sign or authenticate by standard means that are acknowledged in all EU Member States and across all segments of the European Digital Single Market. Europe must not become dependent on non-EU technology manufacturers, which could cause trust issues or lead to commercial disadvantages.

A European Public Key Infrastructure and strong encryption capability are key elements required both by individual citizens and in the public sector, not only domestically, but especially for cross-border activities within Europe. Further elements (e.g. a central European antivirus capability or a trustworthy European security scan capability for citizens' ICT devices) could be considered at a later stage.

3.2.2 European Cyber Security Label

CSCG Recommendation # 5:

The EC should authorise the CSCG to coordinate the standardisation work for a **high-level European Cyber Security Label** for information and communication technologies (ICT) to protect the European consumer (objective 4 of the EU Cyber Security Strategy).

To become sufficiently visible, European Cyber Security regulatory efforts need to be complemented by a European Cyber Security Label for ICT products and services. The idea of a European Security Label was officially formulated in the final report of the European Security Research and Innovation Forum (ESRIF), but has not yet materialised. For the specific area of Cyber Security, a label would be beneficial for consumer protection and as an incentive for manufacturers to provide solid security solutions.

Ideally, the European Cyber Security label should harmonise with the EU's Cyber Security requirements and the evaluation framework of CSCG Recommendation # 6. The standardisation work should reflect a risk-based approach to conformity assessment, applicable to the issue of a European Declaration of Conformity, including but not limited to the manufacturer's / supplier's self-declaration (see 3.2.3 below).

The CSCG recognizes the high value of the "Common Criteria" (i.e. ISO/IEC 15408) as a basis for high level evaluation but for basic protection a simplified scheme can be used. The basic label could be implemented via self-certification although there may be a need for accredited evaluation for higher security requirements. The European Cyber Security Label would not have to be a static label but could be a dynamic online label, for example being downgraded to reflect poor review results or upgraded after security issues have been found and fixed.

For a European Security Label to be successful, transparency and evaluation will be necessary to establish a trustworthy environment and to inspire confidence in the system.

3.2.3 European Cyber Security Requirements

CSCG Recommendation # 6:

The EC should mandate CEN/CENELEC/ETSI, with the CSCG coordinating appropriate harmonisation with the European regulatory bodies, to **extend existing European Cyber Security requirements and evaluation frameworks** to ensure adequate Cyber Security throughout the full ICT value chain and to establish an initiative for risk-based standardisation.

To implement its Cyber Security requirements in a market of 500 million citizens and particularly to justify the need for such action to manufacturers, Europe needs to develop a level playing field. Standardised requirements are the key to interoperability and to avoiding national requirements being added to an EU baseline, thus complicating the situation. Manufacturers will have to respect EU requirements aimed at making the European digital environment the safest in the world, particularly to make sure European fundamental rights and core values are not violated. By aligning European Cyber Security requirements with the European Cyber Security Label of CSCG Recommendation # 5, an adequate level of Cyber Security for all ICT products and services in the European market should be ensured (see 3.2.2 above).

A potential future European regulatory framework for security should be built on the model of the New Approach / New Legislative Framework, with harmonised standards underpinning essential (regulatory) requirements. This includes the use of a risk-based approach to conformity assessment, based on the issue of a European Declaration of Conformity, with the manufacturer's / supplier's self-declaration being accepted as indicating the application of and compliance with the relevant harmonised standards.

The CSCG recommends that harmonised European Cyber Security requirements should be created, with a strong emphasis on the need to respect European fundamental rights and core values, including but not limited to privacy, freedom of speech and the free flow of information.

3.2.4 European Cyber Security Research

CSCG Recommendation # 7:

The EC should authorise the CSCG to **create a high-level interface between the CSCG and the European research community** to ensure alignment between standardisation and research including industrial research.

The EC should authorise the CSCG to create a high-level interface between the CSCG and the European research community to ensure alignment between standardisation and research, including industrial research. Regardless of any current definition, the term "Cyber Security" and its meaning will probably undergo changes, especially when more stakeholders become involved in Cyber Security problems or solutions. In addition, with many unanswered questions about Cyber Security remaining, deeper analysis is needed. The connection between Cyber Security research and Cyber Security standardisation is therefore important, especially given the rapid development in cyberspace (and in ICT in general). This linkage is important as research often lacks reference to standardisation and especially standardisation institutions, procedures and indeed the whole standardisation landscape.

Significant relevant forthcoming activities include:

- The CSCG will cooperate with the Horizon 2020 research planning and related endeavours, e.g. the European Defence Agency (EDA), the WG 3 "Secure ICT Research and Innovation" of the European Commission NIS Public-Private Platform. The CSCG should also liaise with existing security groups within the EC/Council and European Parliament.
- Synchronisation between research and standardisation should be a two-way process, especially when concerning the exchange of results.
    - Fast-tracking mature research results and trialled solutions into standards:
      A process should be established that allows research results to be standardised sufficiently quickly so that industry can apply the results and maintain or gain a competitive edge. To re-establish the necessary trust in the European digital environment (cf. Recommendation # 3, see 3.1.3 above) this process, while

being fast, should also consider alignment with European values including the protection of citizens and their privacy.

- General support to transfer research results into standards:
  The standardisation process often lasts longer than the support period of a research project. As a result, the transfer of research results into standardisation may be interrupted if the project ends before the standard has been completed. This issue should be addressed.
- Bring well-established standards into research programmes:
  - The landscape of standardisation committees and efforts needs to be explained in a much more efficient way. This needs to include EU resources for developing tutorial material with information on the background of published standards, examples and the modus operandi, and roadmaps of related projects and committees.
  - The standards themselves need to be made accessible to researchers in an easy, straightforward, and affordable way, e.g. via EU budgeted bulk subscriptions for (EU) research projects.

Synchronisation should include international standards (e.g. ISO, IEC and ISO/IEC) where they address European values, such as the recent frameworks and architectures on privacy and identity management.

- NIS education and awareness raising for the general public and basic NIS education should relate to the major fields for improved activities on Cyber Security in the EU as listed under Recommendation # 3 (see 3.1.3 above). In addition, tying NIS education in with general education and skills certification programmes, such as the European Computer Driving Licence (ECDL, www.ecdl.org), would be useful.

Such activities should ensure that European research results are incorporated into European standards to support innovation in European industry, but in this way they will also support European researchers by using international standardisation as a platform for the discussion and promotion of their ideas and results. The global perspective is important, as many international framework standards in security and privacy have a major impact on the European Union. However, special support should be given to initiatives which align with European values and strengths.

3.3 Global Dimension

At present, Cyber Security is a national issue but it is clearly desirable for it to be accepted as a regional issue to ensure a harmonised European approach. ICT in general and the Internet in particular have contributed significantly to the globalisation of markets, and Cyber Security is an issue everywhere. In its Cyber Security strategy, the EU has identified this global dimension. The CSCG shares the view that all European efforts on Cyber Security need to be embedded into a suitable international (i.e. global) initiative.

3.3.1 EU Industrial Forum on Cyber Security Standards

CSCG Recommendation # 8:

The EC, with the support of the CSCG, should **engage in an industrial forum** to harmonise Cyber Security Standards with key international players and stakeholders according to European requirements.

The CSCG has the goal to consolidate all stakeholder views including all relevant views expressed by the European industry in the area of Cyber Security Standardisation. However, we have to recognise that within International Standards, for example in ICT, initiatives are not always taken within Europe. Other key players and industrial stakeholders also lead on this standards development.

For this reason the CSCG proposes to engage and work closely with the key international players and stakeholders, and will establish a forum, or will make use of an existing forum as appropriate, where it can engage such key international players and stakeholders.

This will ensure that we do not duplicate activities or try to lead in areas where we do not have the leadership, but work together harmoniously. The CSCG will continue to be the European focus for Cyber Security Standardisation through its engagement in an appropriate industrial forum to coordinate European activities with key international players and stakeholders.

3.3.2 EU Global Initiative on Cyber Security Standards

CSCG Recommendation # 9:

The EC, with the support of the CSCG, should **launch a targeted global initiative** to promote standards appropriate to European requirements for the development of trustworthy ICT products and services as well as Cyber Security solutions.

Global interconnectivity and Cyber Security are essential for the future economic success of almost all sectors of European markets, not only the European Digital Single Market. International standards are the baseline for global business, and cannot be ignored. The European Commission should underline its expressed objective to ensure concerted international action in the field of Cyber Security.

Based on the unique positioning of the EU as a consensus-oriented Union with strong core values and fundamental rights, the time has come to establish a European lead on Cyber Security standardisation. This could be accomplished by launching an international initiative under EU leadership.

The CSCG recommends that the EU should establish a global initiative to ban untrustworthy ICT, with the final objective of eradicating untrustworthy ICT products and services. This initiative should be based on the European Commission's effort to complete the European Digital Single Market and should be carried out globally in close collaboration between the European Commission and the EU External Action Service.

4 Conclusions

The Cyber Security issue (i.e. the information security issue) has been a matter of concern for more than 25 years and, in spite of many different initiatives, has only become increasingly fragmented and difficult to handle with time. The CSCG therefore appreciates the efforts of the European Commission and of the High Representative for Foreign Affairs and Security Policy to adopt an EU-wide approach to Cyber Security.

The EU Cyber Security Strategy communicated in February 2013 is a first step, but it needs to be complemented by a dedicated and strategic European effort on Cyber Security standardisation. Such an effort should take into account both the perspective of the infrastructure operators and the need to protect European citizens as end users of modern ICT, which originates increasingly from non-EU producers.

The EU is well placed to make such an effort now: a European market of more than 500 million consumers represents a very significant power and an attractive target for manufactures. Strong European fundamental rights and core values can provide the required trust for pan-European solutions.

The CSCG recommends that the EU should take the opportunity to establish a global lead in Cyber Security standardisation, fulfilling its documented objective to make the European digital environment the safest in the world.

(This page intentionally left blank.)

Annex A The CSCG Member Bodies

The CSCG Member Bodies (MBs), i.e. the CEN/CENELEC Management Centre (CCMC), the European Telecommunications Standards Institute (ETSI), the National Standardisation Bodies and/or the appropriate National Committees of a number of EU Member States as well as the European Network and Information Security Agency (ENISA) and the EU's Joint Research Centre (JRC) work in close collaboration within the CSCG.

In December 2013 there were fourteen EU Member States participating actively in the work of the CSCG, in addition to CCMC, ETSI, ENISA and JRC. All the CSCG experts were nominated to the Group by the institutions indicated below.

No.	Abbreviation	Description of the Institution of the respective CSCG Member Body	MB[1]
1.	AENOR	Asociación Española de Normalización y Certificación	ES
2.	AFNOR	Association française de normalisation	FR
3.	ASI	Austrian Standards Institute	AT
4.	ASRO	Asociatia de Standardizare din România	RO
5.	BSI	British Standards Institution	UK
6.	CCMC	CEN-CENELEC Management Centre	
7.	CYS	Cyprus Organization for Standardization	CY
8.	DIN	Deutsches Institut für Normung e.V.	DE
9.	ENISA	European Union Agency for Network and Information Security	
10.	ETSI	European Telecommunications Standards Institute	
11.	JRC	Joint Research Centre of the European Commission	
12.	NEN	Netherlands Standardization Institute	NL
13.	PKN	Polish Committee for Standardization	PL
14.	SIS	Swedish Standards Institute	SE
15.	SN	Standards Norway	NO
16.	SUTN	Slovak Standards Institute	SK
17.	UNI	Ente Nazionale Italiano di Unificazione	IT
18.	UNMZ	Czech Office for Standards, Metrology and Testing	CZ

The CSCG Secretariat is located at DIN in Berlin, Germany.

[1] The EU Member States are indicated by the appropriate ISO 3166 two-letter country code. Please note the above list is ordered sequentially by abbreviation of the nominating institutions only, thus the Member Bodies and/or EU Member States are presented without any sequential priorities.

Annex B Abbreviations

The CSCG White Paper makes use of several abbreviations as comprised below.

Abbreviation[2]	Description of the abbreviated term (and URL where applicable)
AENOR	Spanish Association for Standardisation and Certification *Asociación Española de Normalización y Certificación* http://www.aenor.es
AFNOR	Association française de normalisation http://www.afnor.org
ASI	Austrian Standards Institute *Österreichisches Normungsinstitut* https://www.austrian-standards.at
ASRO	Asociatia de Standardizare din România http://www.asro.ro
AT	Austria
BSI	British Standards Institution http://www.bsigroup.com
CCMC	CEN-CENELEC Management Centre http://www.cencenelec.eu/aboutus/MgtCentre
CEN	European Committee for Standardisation http://www.cen.eu
CENELEC	European Committee for Electrotechnical Standardisation http://www.cenelec.eu
CS	Cyber Security
CSCG	CEN/CENELEC/ETSI Cyber Security Coordination Group http://www.cscg.focusict.de
CY	Cyprus
CYS	Cyprus Organization for Standardization http://www.cys.org.cy
CZ	Czech Republic
DE	Germany
DIN	German Institute for Standardization *Deutsches Institut für Normung e.V.* http://www.din.de
EC	European Commission http://ec.europa.eu
ES	Spain
ECDL	European Computer Driving Licence http://www.ecdl.org
EDA	European Defence Agency http://eda.europa.eu

[2] Annex A uses the appropriate ISO 3166 two-letter country code (listed here in *italics* as abbreviation) for these CSCG members which represent EU Member States. Please refer to the list of CSCG Member Bodies on page 21.

Abbreviation[2]	Description of the abbreviated term (and URL where applicable)
ENISA	European Union Agency for Network and Information Security http://www.enisa.europa.eu
ESO	European Standards Organisation
ESRIF	European Security Research and Innovation Forum http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf
ETSI	European Telecommunications Standards Institute http://www.etsi.org
EU	European Union http://europa.eu
FR	France
ICT	information and communication technology
IEC	International Electrotechnical Commission http://www.iec.ch
ISO	International Organization for Standardization http://www.iso.org
ISO/IEC	ISO and IEC joint activities and joint international standards http://www.standardsinfo.net
IT	information technology
IT	Italy
JRC	Joint Research Centre of the European Commission http://ec.europa.eu/dgs/jrc/
JTC 1	ISO/IEC Joint Technical Committee No. 1 – Information Technology http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm
MB	Member Body
NEN	Netherlands Standardization Institute *Nederlands Normalisatieinstituut* http://www.nen.nl
NIS	Network and Information Security
NL	Netherlands
NO	Norway
NSO	National Standards Organisation
PKI	Public Key Infrastructure
PKN	Polish Committee for Standardization *Polski Komitet Normalizacyjny* http://pkn.pl
PL	Poland
SDO	Standards Developing Organisation
SE	Sweden
SIS	Swedish Standards Institute http://www.sis.se
SK	Slovakia
SME	small and medium-sized enterprise
SN	Standards Norway *Standard Norge* http://www.standard.no

Abbreviation[2]	Description of the abbreviated term (and URL where applicable)
SUTN	Slovak Standards Institute *Slovenského ústav technickej normalizácie* http://www.sutn.sk
UK	United Kingdom
UNI	Ente Nazionale Italiano di Unificazione http://www.uni.com
UNMZ	Czech Office for Standards, Metrology and Testing *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* http://www.unmz.cz
URL	uniform resource locator a.k.a. web address
US	United States of America
WG	working group

Contact and Copyright

Point of Contact: Deutsches Institut für Normung e.V.

CEN/CENELEC/ETSI CSCG Secretariat

Burggrafenstraße 6

10787 Berlin

Germany

Tel.: +49 (0) 30 2601-0

Fax: +49 (0) 30 2601-1231

http://www.cscg.focusict.de

Contact Person: Volker Jacumeit

Tel.: +49 (0) 30 2601-2186

<volker.jacumeit@din.de>

Copyright Notice