EUROPEAN COMMISSION
ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Space, Security and GMES
Security Research and Development

Brussels, 17th February 2011
M/487 EN

PROGRAMMING MANDATE ADDRESSED TO CEN, CENELEC AND ETSI TO ESTABLISH SECURITY STANDARDS

1. SCOPE

This Mandate concerns the development of a work programme for the definition of European Standards and other standardisation deliverables in the area of SECURITY[1]. The programme will take note of all aspects linked to the different specific products, systems, procedures and protocols that should be covered by standards to assist the EU to ensure that security is better and consistently addressed in different security landscapes. This Mandate has an exclusively civil application focus.

Therefore, this Mandate concerns the analysis of the current security standards landscape in Europe taking account of the legislative background and the drawing of a security standardisation map. In order to do this, the analysis should cover the most relevant National Standards, *the full range of available EU standards, as well as ISO and IEC. It should as well* comprise the full range of standards-types needed (some standards may cover several of these classes) to ensure protection and security of the citizen, namely:

- **INTEROPERABILITY STANDARDS**

  - **Technical interoperability standards**: Standards aimed at achieving interoperability, mainly when there is a need to share information between security systems, equipments or applications.

  - **Syntax standards:** Those related to data formats and syntax and encoding of data messages.

  - **Semantic standards:** Those that imply a common human understanding of the information being exchanged.

[1] ‘The security concept here includes, among others, protection against threats by terrorism, severe and organised crime, natural disasters, pandemics and major technical accidents. It excludes defence and also space technology, for which a programming Mandate has already been issued by the Commission (Mandate M/415 ‘Programming Mandate addressed to CEN, CENELEC and ETSI to establish Space Industry Standards’)

- **Organisational interoperability standards**: Protocols, procedures and guidelines to harmonise the functioning and operational work of public and private security related organisations.

- **PERFORMANCE STANDARDS**

  - **Performance Standards:** Standards establishing a set of minimum requirements to be fulfilled by **systems, equipments or procedures, for any use related to security**.

The work programme will have to take into account security measures in line with the security levels determined by public authorities and their underlying risk assessments, identifying security needs and secure interoperability schemes between the various nodes and centres for civil security in Europe dealing with law enforcement and crisis management. It should include, as well, similar needs from private perspectives.

The analysis should cover existing formal European and international standards, and the European Standardisation Organisations (ESOs) should then draw up a work programme to provide any missing standards or amend existing standards to meet current and future foreseen requirements, suggesting priorities and timescales.

A list of areas for analysis, taken as an example and not exhaustive, is:

Security of the Citizens

- Organised Crime
- Counter Terrorism
- Explosives
- CBRN
- Fire hazard

Security of infrastructures and utilities

- Building design
- Energy/Transport communication grids
- Surveillance
- Supply Chains

Border Security

- Land border / Check Points
- Sea Border
- Air Border

Restoring security and safety in case of crisis

- Preparedness and planning
- Response
- Recovery

Human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness are relevant to all the topic areas listed above and should be duly taken into account, not forgetting transversal areas neither.

With the exception of Cryptography, as it is considered a key technology for any security application, the Information and Communications Technologies (ICT) are not covered by this mandate. However, specificities which rise from their adaptation to the field of security should be included in it.

2. JUSTIFICATION

2.1 Rationale

The main rationale for the development of a standardisation map in the security area is that, for the time being, not enough appropriate security standards are available to ensure an effective cross-border security within the European Union. Moreover, new EU security "missions" are appearing, and these need a new pan-European approach. For such cases, security standards should fit any existing and foreseeable EU internal market requirements.

Specific standards frameworks related to the different security areas are required in order to meet the Commission policy objectives, avoiding a proliferation of various overlapping and heterogeneous security standards, to arrive at EU-wide standards for the benefit of the internal market. It is essential that these standards are drawn up impartially, objectively and with the involvement of the different stakeholders and operators, particularly end users and SMEs, instead of reflecting only the views of specific parties or industries. The ESOs, together with their international counterparts, provide the platforms for such standards activities.

CEN/CENELEC/ETSI deliverables could also identify minimum performance levels for the different security areas and facilitate companies to be competitive in the different security sectors. In order to achieve this, standards can also play a major role as providing criteria for certification of products and services.

Furthermore, European standards that take into account the relevant policy issues as well as economic interests should create the link between R&D activities and a clear procurement and validation strategy. This should promote the creation of a more consolidated European security market and better cooperation among security stakeholders at national and European levels.

Usually, a bottom-up approach has been followed in the different aspects related to security standardisation, specific working groups being formed to cover specific areas where standards are needed. However, the time seems right to promote a top-down approach, at least in programming terms, as several topics in the area of Security are not being covered with the existing initiatives and an overall picture would give a better way to approach this issue, increasing the level of awareness of the Member States and related stakeholders.

2.2 Relevant political context

The background on the specific role of the standardisation activities related to security can be found in the following sources:

a) ESRIF Report.[2] The ESRIF report highlighted the importance of an integrated approach to security in order to embrace, among others, interoperability, standardisation, certification, validation and the exchange of best practices.

[2] http://www.esrif.eu/documents/esrif_final_report.pdf

“Security research should be grounded in an industrial policy that frames a systematic approach to capability development which, in turn, promotes interoperability among the 27 EU nations and establishes common standards. Ultimately this effort must increase societal security in a globalised world, while fostering trust between European citizens, governments and national and European institutions.”

“Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards.”

“The early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place.”

b) Communication on reaction to ESRIF[3]. The Communication COM (2009) 691 "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations" remarked that in order to harvest innovation and growth tomorrow it is required to invest now in an ambitious industrial policy for the security sector.

"Based on the requirements of the end-users and the results of research, new technologies and solutions need not only to be validated; they should also be certified and where appropriate standardised, so they can become part of an effective response to security threats. R&D activities should be linked to a clear validation and procurement strategy that takes into account the relevant policy issues as well as economic interests. This should promote the creation of a European security market and better cooperation among security stakeholders at national and European levels.

ESRIF recommends that the Commission should evaluate the applicability and efficacy of a "European Security Label". CEN and ETSI have started working on standardisation in the area of security. CEN is initially concentrating on a number of issues for which it has received standardisation Mandates (notably on supply chain security, critical infrastructure protection, and proofing products against crime). As standards can be an effective means for transferring research findings into innovative products, it is expected that work carried out in the 7th Framework Programme will lead to further standardisation. This work needs to be accelerated."

c) Study on Competitiveness of the EU Security Industry[4]. In the study delivered by ECORYS (2009) on the Competitiveness of the European Security Industry, recommendations were made about the development of new European and common international standards for security as a mean to reduce the Security market fragmentation, which is leading to a lack of competitiveness of the Security European Industry.

In their recommendations it is affirmed *"Greater EU-level cooperation on development and adoption of common security standards and approvals/certification systems. Eventually leading to adoption of EU-based standards international markets to the advantage of EU suppliers."*

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0691:FIN:EN:PDF

[4] http://ec.europa.eu/enterprise/newsroom/cf/itemshortdetail.cfm?item_id=3931

d) **Communication Towards an increased contribution from standardisation to innovation in Europe**[5]**.** The Communication COM (2008) 133 underlines the contribution that standards could and should make to innovation (policy). This is judged important for further strengthening the European economy as well as directly in competition in standard setting from emerging powers, who consider standardisation an important strategic asset.

It is stated *"Standardisation complements market-based competition, typically in order to achieve objectives such as the interoperability of complementary products/services, and to agree on test methods and on requirements for safety, health, organisational and environmental performance. Standardisation also has a dimension of public interest, in particular whenever issues of safety, health, security and of the environment are at stake. In addition the standard-setting process needs to be in line with European competition provisions."*

"Public procurement: the appropriate use of standards in public procurement may foster innovation, while providing administrations with the tools needed to fulfil their tasks. Instead of prescribing particular technical solutions, the use of technology-neutral standards allows contracting authorities to call for advanced performance and functional requirements (e.g. relating to environmental aspects or to accessibility for all), thus stimulating the search for innovative technologies that provide best value for money in the long term, while ensuring safety and interoperability."

"The European identity and the visibility of European standardisation, both inside Europe and in the world, need to be reinforced"

e) The **Stockholm Programme**[6], which was adopted by the European Council in December 2009, invites the Council and Commission to develop the **internal security strategy**, *"ensuring that its priorities are tailored to the real needs of users and focus on improving interoperability."*

Further to that, the Communication[7] "*The Internal Security Strategy in Action: Five steps towards a more secure Europe*", sets out coherent goals in five priority areas (serious and organised crime, terrorism, cybercrime, border security and disaster management). Security research plays a crucial role in achieving those goals.

f) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

"In order to facilitate improvements in the protection of ECIs, common methodologies may be developed for the identification and classification of risks, threats and vulnerabilities to infrastructure assets."

"The Commission shall support, through the relevant Member State authority, the owners / operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection."

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0133:FIN:EN:PDF

[6] The Stockholm Programme: An Open and Secure Europe Serving and Protecting the Citizens (Council Document 17024/09); Delivering an area of freedom, security and justice: Action plan implementing the Stockholm Programme (COM 2010 (171)). The Stockholm Programme is the EU's programme for justice and home affairs during the period 2010-14.

[7] COM(2010) 673 final.

3. DESCRIPTION OF THE MANDATED WORK

The overall objectives are:

- To increase the harmonisation of the European security market and reduce fragmentation with the establishment of a set of comprehensive European standards.
- To enhance secure interoperable communications and data management between the various security control centres, operators, public authorities and first responders.
- To develop common technical specifications (taking into account the already existing) concerning interoperability, quality or safety levels, including test methods and certification requirements.
- To provide interoperability and comparability of different solutions, which in turn facilitate competition and innovation.
- To develop methods for security vulnerability assessment by security system operators
- To allow companies the opportunity to develop tailor-made and cost beneficial security measures in agreement with a global EU security strategy.

The preparatory study and subsequent work programmes should include the following:

- Identification of user requirements related to possible standards.
- Analysis and comparison of the existing formal (European and international) security standards implemented in Europe.
- Definition of the areas where CEN/CENELEC/ETSI standards in security should be established.
- Development of a checklist on whether a standard could make business and operational sense.
- Analysis whether a specific rather than generic risk approach for SMEs will be necessary. The ESOs will fully take into account the guidelines included on CEN-CLC Guide 17 on SME needs.
- Analysis whether CEN/CENELEC/ETSI standards can reflect the nature of security threats which could be country specific rather than EU-wide and whether they do not constrain or contradict any national legislation.
- Analysis of any provision related to the classification of sensitive information that could be involved in the standardisation process.
- Analysis whether a standard would reduce the level of security in the areas which are already covered by existing national schemes.
- Any important consideration related to the development of these standards including; the identification and prioritisation of possible needs for pre-and co-normative research and certification systems relevant to the development of European standards

or other standardisation deliverables for security systems, equipment and applications including justification and an indicative time schedule for such an activity

- The overall economic costs and benefits of the potential standardisation work to be done in the selected security sectors should be evaluated in order to be taken into account in the final selection of work programmes.

The work shall be carried out in two phases:

3.1 In Phase 1, a preparatory study should identify the state of play in security standardisation in Europe, and list a set of sectors for priority treatment, as well as the particular stakeholders needing to be involved in each of these sectors.

The results of this phase should be submitted to the European Commission, which will subsequently select the sectors to be covered and will request the execution of phase 2.

3.2 In Phase 2, for each selected sector, the specific standardisation needs will be identified and comprehensive standardisation programmes with suitable and realistic roadmaps shall be prepared.

The resulting standardisation programmes should be submitted to the European Commission, which will consult the Committee 98/34 and Security Committees as appropriate prior to the execution of the programmes.

The specific standardisation programmes agreed upon in the second phase will then be implemented on the basis, where appropriate, of mandates covering specific areas. The execution of the specific standardisation tasks shall be carried out in close co-operation with all the relevant stakeholders.

European Standardisation bodies are invited to ensure that the deliverables developed meet European legislative and other requirements, in particular as regards privacy and Intellectual Property Rights (IPR).

CEN, CENELEC and ETSI are also invited to develop security sector specific implementation guidelines, as complementary documents of general nature. These guidelines are intended to assist the user in the choice of proper technologies for determined security applications.

4. EXECUTION OF THE MANDATE

4.1 Requirements to the ESOs.

The Commission hereby asks CEN, CENELEC and ETSI to fulfil the tasks as described above, while taking into account the rationale of this Mandate stated in the justification.

CEN, CENELEC and ETSI are required to keep close contacts with the Commission services and to ensure that their activities are coordinated in a way to create a consistent and coherent set of security interoperability frameworks at the international level, including a set of performance standards for the identified security sectors. In this respect, the following principles shall be followed:

- The development efforts, in the first instance, should be targeted at the international level.

- Results of relevant EU research projects and national guidelines for Security application shall be taken into account.

- Particular attention shall be given to the involvement of national organisations and authorities concerned with the implementation of the Directive 95/46/EC and Directive 2002/58/EC, including the European Data Protection Supervisor and the Article 29 Working Party.

CEN, CENELEC and ETSI are also requested to consult with the European Commission DG Joint Research Centre in order to explore if the Commission's research institutes dispose of specific competence to support the standardisation work.

4.2. Arrangements for the execution of the Mandate

Within two months of the date of acceptance of this Mandate by CEN, CENELEC, and ETSI, they shall present a joint report to the Commission services setting out the arrangements they have made for the execution of this Mandate. Particular attention shall be given to the involvement of all the relevant parties and to the working arrangements with relevant industry fora and consortia.

4.3 Work Plan

4.3.1 Phase 1. CEN, CENELEC and ETSI shall provide, within 8 months of the acceptance of this Mandate the result of the preparatory study and a list of sectors for priority treatment to be agreed by the Commission services. The Commission will endeavour to review the study and select some security sectors within a further three months.

4.3.2 Phase 2. CEN, CENELEC and ETSI shall provide the proposed standardisation programmes and roadmaps related to the agreed security sectors within 6 months of the acceptance of the report of Phase 1 and the Commission's selection of priority sectors, for consideration for subsequent execution in a possible future phase.

CEN, CENELEC and ETSI are also requested to consult with the European Commission DG Joint Research Centre in order to explore if the Commission's research institutes dispose of specific competence to support the standardisation work.

5. ORGANISATIONS TO BE INVOLVED

The execution of the Mandate should be undertaken in close cooperation with the widest possible range of interested groups and particularly: the Joint Research Centre of the European Commission (JRC), the European Network of Law Enforcement Technology Services (ENLETS), European Network of Forensic Science Institutes (ENFSI), Security industry organisations like European Organisation for Security (EOS), European Research Institutes and Agencies as well as those of National Agencies and European Technology Platforms with a relevant interest in this domain.

International cooperation shall be ensured, in particular with IEC, ISO and ITU, as appropriate. Particular consideration should be given to ISO TC 223 "Societal Security". Examples of committees active in the field of Security are ISO/TC 247, ISO/IEC JTC 1/SC 17, ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 37 and ISO/TMB/SAG-S.

As appropriate, CEN, CENELEC and ETSI will invite the representative organisations of consumers’ interests (ANEC), and small and medium-size enterprises (NORMAPME) to participate in the work, together with other stakeholder organisations with a relevant specific interest in the subjects, in particular end-users of security systems.

In order to deal properly with the interaction of ICT as a security technology enabler the participation of ENISA is appropriate as well.