ANSI Homeland Security Standards Panel

Ninth Annual Plenary Meeting

SECURITY STANDARDISATION PROGRAMMING MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS

Dr. Ignacio Montiel-Sánchez

DG-ENTR H3 / Security Research and Development

European Commission
Enterprise and Industry

WHAT IS A MANDATE?

- A Standardisation Mandate is the mechanism by which the Commission requests the European Standards Organisations (ESOs) to develop and adopt European standards in support of European policies and legislation.

- Draft mandates are drawn up by the Commission services through a process of consultation with a wide group of stakeholders.

- Before being formally addressed to the ESOs, they are submitted for opinion to the Member States in the Standing Committee of the 98/34/EC Directive

WHAT KIND OF MANDATES EXIST?

- Three types of mandates could be considered:
  - **Feasibility study:** To check the feasibility of standardisation
  - **Programming mandates:** Requesting the analysis and elaboration of a standardisation programme and preparation of implementation roadmaps
  - **Standardisation mandates:** Requesting work programmes for the development and adoption of European standards or other deliverables.
- The ESOs, which are independent, have the right to refuse a mandate if they do not think that standards can be produced in the area being covered.
- Please note that European standards, even developed under a mandate and for European legislation, remain voluntary in their use.

The European Standards Organizations (ESOs)

- The European Committee for Standardization
- The European Committee for Electrotechnical Standardization
- The European Telecommunications Standards Institute

➢ “Recognised” by the European Union under Directive 98/34

SCOPE OF THE MANDATE

- Development of a work programme for the definition of European Standards and other standardisation deliverables in the area of **SECURITY**.
    - Including protection against man-made and natural disasters
    - Excluding Defence and Space technologies
- 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**.

TYPES OF STANDARDS (1)

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, syntax and encoding of data messages.

Semantic standards:

- Those that imply a common human understanding of the information being exchanged.

Organisational interoperability standards:

- Protocols, procedures and guidelines to harmonise the functioning and operational work of public and private security related organisations.

TYPES OF STANDARDS (2)

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.

SOME CHARACTERISTICS

- The analysis should cover **existing formal European and international** standards, drawing up a work programme to provide any missing standards or amend existing standards.
- Security measures in line with the security levels determined by **public authorities** and their underlying **risk assessments,** including as well similar needs from **private requirements.**
- Identifying **security needs** and secure **interoperability schemes** between the various nodes and centres for civil security in Europe.
- To meet current and future foreseen **requirements** and suggesting **timescales**.

LIST OF AREAS (not exhaustive)

- **Security of the Citizens**
  - Organised Crime
  - Counter Terrorism
  - Explosives
  - CBRN

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

- **Restoring security and safety in case of crisis**
  - Preparedness and planning
  - Response
  - Recovery

- **Security of infrastructures and utilities**
  - Building design
  - Energy / Transport communication grids
  - Surveillance
  - Supply Chains

OTHER CONCERNS

- Take into account:
  - **Human factor** issues
  - **Privacy** concerns
  - Identification of **operator requirements** for enhancing systems effectiveness

- The **Information and Communications Technologies** (ICT) domain is within the scope of this Mandate as a security enabler.

- ICT as such, not covered by this Mandate, with the exception of **Cryptography**

JUSTIFICATION – RATIONALE

- To ensure an effective **cross-border security** within the European Union and a pan-European approach for the **new EU security "missions".**

- Specific standards frameworks are required to meet **policy objectives** and to **harmonize** the internal market.

- Create the link between **R&D** activities and a clear **procurement** and **validation** strategy.

- Impartiality, objectivity and involvement of the different **stakeholders** and **operators**, particularly **SMEs**.

- Identify **minimum performance levels** for the different security areas.

- More consolidated European **security market** and better cooperation among security **stakeholders** at national and European levels.

JUSTIFICATION - RELEVANT POLITICAL CONTEXT

- ESRIF Report.
  http://www.esrif.eu/documents/esrif_final_report.pdf

- EC Communication on reaction to ESRIF
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0691:FIN:EN:PDF

- Study on Competitiveness of the EU Security Industry
  http://ec.europa.eu/enterprise/newsroom/cf/itemshortdetail.cfm?item_id=3931

- EC Communication Towards an increased contribution from standardisation to innovation in Europe
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0133:FIN:EN:PDF

- The Stockholm Programme
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF

DESCRIPTION OF THE MANDATED WORK

Overall objectives:

- Increase **harmonisation** of the EU security market and reduce fragmentation.
- Enhance secure interoperable **communications and data management.**
- Develop **common technical specifications** concerning:
  - Interoperability
  - Quality or safety levels
  - Test methods and certification requirements.
- Provide interoperability and comparability to facilitate **innovation**.
- Develop methods for security **vulnerability assessment** by system operators
- Allow companies to **develop tailor-made and cost beneficial** security measures in agreement with a global EU security strategy.

DESCRIPTION OF THE MANDATED WORK

Study and preparation of work programmes including (1):

- Identification of **user requirements** related to possible standards.
- Analysis and comparison of the existing **formal 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 **SME's** will be necessary.

DESCRIPTION OF THE MANDATED WORK

Study and preparation of work programmes including (2):

- Analysis whether standards can reflect a nature of security threats **country specific rather than EU-wide**.
- Analysis whether a standard would **reduce the level of security** in areas already covered by existing national schemes.
- Any important consideration as the identification of possible needs for **pre-and co-normative research and certification systems** relevant to the development of European standards including justification and an indicative time schedule for such an activity.

DESCRIPTION OF THE MANDATED WORK

- The resulting proposed standardisation programmes should be submitted to the EC, which will consult the **Committee 98/34 and Security Committees** as appropriate, prior to the execution of the programmes.
- The different standardisation programmes will then be implemented on the basis of specific **Standardisation Mandates** covering the particular areas selected by the EC.
- Ensure that the deliverables developed meet European **legislative**, **privacy** and Intellectual Property Rights (**IPR**) requirements.
- CEN, CENELEC and ETSI develop security sector specific **implementation guidelines** to assist the user in the choice of proper technologies for determined security applications.

EXECUTION OF THE MANDATED WORK

Requirements to the ESOs:

Keep close contacts with the Commission services and ensure coordination 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.

The following principles shall be followed:

- In first instance, **international level target**.

- Take into account relevant **EU research projects** and **national guidelines** for Security application.

- 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.

EXECUTION OF THE MANDATED WORK

CEN/CENELEC/ETSI will present a **joint report** to the Commission services setting out the arrangements made for the execution of this Mandate.

First Phase.

- A study should identify the **state of play** in security standardisation, existing **gaps** and list a set of **sectors**, as well as the particular **stakeholders** needing to be involved for each of these sector issues.

Second Phase.

- For each selected sector, identification of the specific standardisation needs and preparation of a comprehensive **standardisation programme** with a **suitable and realistic roadmap**

CEN, CENELEC and ETSI shall afterwards execute the Standardisation Mandates on the sectors agreed with the Commission

ORGANISATIONS TO BE INVOLVED

Cooperation with the widest possible range of interested groups:

- Joint Research Centre of the European Commission (**JRC**),
- Security industry organisations (Like **EOS**)
- European **Research Institutes, Technology Platforms and Agencies**.
- **National Agencies**.
- Representative organisations of consumers' interests: **ANEC**
- Representative of Small and medium-size enterprises: **NORMAPME**
- **End-users** of security systems
- **ENISA**
- International cooperation shall be ensured, in particular with **IEC, ISO** and **ITU**, as appropriate.
- Particular consideration to **ISO TC 223** "Societal Security".
- Examples of committees active in the field of Security are **ISO/TC 247**, **ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 37 and ISO/TMB/SAG-S**.

Further information

European Commission - DG ENTR, H3
Security Research & Development

http://ec.europa.eu/enterprise/security/

entr-security-research@ec.europa.eu

Ignacio.MONTIEL-SANCHEZ@ec.europa.eu

Thanks a lot for your attention !