



EUROPEAN COMMISSION

MEMO

Brussels, 30 July 2012

Security industry: Commission proposes Action Plan to enable growth – further details

The European Commission announced today the adoption of an Action Plan dedicated to support the competitiveness of the EU Security Industry (see [IP/12/863](#)). This Memo provides more detailed information on the rationale behind the Action Plan and the scope of the central policy measures.

The security market has three distinctive features:

- It is highly fragmented and divided along national or even regional boundaries. Security, as one of the most sensitive policy fields, is one of the areas where **Member States are hesitant to give up their national prerogatives**.
- For the most part **buyers** in the security market **are public authorities**.
- It has a **strong societal dimension**. Security measures and technologies can have an impact on fundamental rights and often provoke fears e.g. of a possible undermining of privacy.

Expected benefits of the action plan

- The creation of **harmonised standards and certification procedures** for certain security technologies should significantly reduce development and marketing costs, thus enhancing the competitiveness of the EU security industry. It is conservatively estimated that for alarm systems and airport security equipment, harmonised standards would allow savings of up to €29 million per year in terms of testing and certification costs. These measures should also improve the value for money ratio of public and private security spending.
- The **introduction of Pre-Commercial Procurement (PCP)** should radically reduce the gap between research and market, raising the competitiveness of the EU security industry and increasing the end user involvement in the production of novel technologies. A tentative assumption of a 1% increase in the annual growth rate due to R&D support through a PCP scheme would lead to extra sales of €2 billion by 2020.
- The better **exploitation of civilian-military synergies** should reduce the risk of funding duplication and increase the overall efficiency of research efforts. For software defined radio alone it is estimated that hybrid standards could lead to an overall sales increase of €1 billion until 2020.

There is currently no clear definition of the security industry due to the fact that:

- the security industry is not covered as such by the main statistical nomenclatures (NACE, Prodcod, etc.)
- the production of security-related items is divided between a wide range of product categories
- there is no industrial statistical data source available at European level
- procurers of security equipment and systems can be reluctant to provide information on security expenditures.

The EU security industry can nevertheless broadly be subdivided into the **following sectors**: aviation security; maritime security; border security; critical infrastructure protection; counter-terror intelligence (including cyber security and communication); physical security protection; crisis management and protective clothing.

1. Overcoming market fragmentation

Standardisation: Divergent national standards pose an obstacle for the creation of a true internal market for security. For this reason, the Commission will ask the European Standardisation Organisations (CEN, CENELEC and ETSI) to establish concrete and detailed standardisation roadmaps. These roadmaps should focus on the next generation of tools and technologies.

Conformity assessment procedures: There are currently no EU-wide certification systems for security technologies. Following an impact assessment analysis and consultation of stakeholders, the Commission propose two pieces of legislation: one to establish an EU wide harmonised certification system for airport screening equipment; and another to establish an EU harmonised certification system for alarm systems. The objective is to achieve mutual recognition of certification systems.

Exploiting synergies between security and defence technologies: Emphasis should be given to a better exploitation of synergies between the two technology areas. The Commission intends to issue, in close cooperation with the European Defence Agency, 'hybrid standards' standardisation mandates to the European standardisation organisations. A first mandate will soon be issued for software defined radio.

2. Reducing the gap from research to market

Aligning funding programmes, exploiting Intellectual Property Rights (IPR) routes: To reduce the existing gap between research and market, the Commission proposes to use the new IPR rules provided in Horizon 2020. Border security and aviation security are the most promising areas.

Pre-commercial procurement (PCP): PCP should enable public users to play a more central role in the innovation cycle, through the purchase of novel technologies. The Commission intends to devote a significant part of the security research budget to this instrument and encourages Member States to launch similar initiatives at national level, in compliance with relevant EU public procurement law.

Third party liability limitation (TPLL): To ensure that the threat of liability does not deter development of the security industry, the Commission has launched a tender for a major study analysing the legal and economic implications of third party liability limitation. The study will also look into possible alternatives to TPLL, such as those introduced through the US Safety Act; for example a voluntary industry fund, a Commission recommendation, etc.

3. Better integration of the societal dimension

Societal impact "checking" during the R&D phase: The Commission considers that any impact on societal and fundamental rights should already be taken into account through engagement with civil society before and during the R&D phase. The Commission will involve citizens and make societal impact testing obligatory.

Privacy by design and privacy by default during the design phase: Due to the difficulty in translating societal considerations into technological requirements, and the different issues related to security among Member States, the Commission will introduce the concept of "privacy by design" and "privacy by default". The Commission will issue a mandate to the European Standardisation Organisations to develop a standard modelled on existing quality management schemes, and also incorporating the management of privacy issues in the design phase.

A dedicated **expert group** set up by the Commission will meet at least once per year to monitor the announced policy measures and bring together all relevant actors in the security field.

[More information](#)