COUNCIL OF THE EUROPEAN UNION

Brussels, 22 August 2012

13050/12

IND 129
COMPET 523
RECH 324
TRANS 265
MAP 52
MI 521
PI 101
COSDP 676
FRONTEXT 2
PROCIV 136
COTER 86

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	27 July 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	COM(2012) 417 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Security Industrial Policy Action Plan for an innovative and competitive Security Industry

Delegations will find attached Commission document COM(2012) 417 final.

Encl: COM(2012) 417 final

EUROPEAN COMMISSION

Brussels, 26.7.2012
COM(2012) 417 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

Security Industrial Policy

Action Plan for an innovative and competitive Security Industry

{SWD(2012) 233 final}

1. INTRODUCTION

Providing security is one of the central concerns of any society. There is no policy area without a crucial component of security. A safe and secure environment is the very basis on which any stable society is founded upon. A competitive EU based security industry offering solutions for enhanced security can make a substantial contribution to the resilience of European society.

The security industry represents a sector with a significant potential for growth and employment. Over the last ten years the global security market has grown nearly tenfold from ~€10 billion to a market size of ~€100 billion in 2011. Numerous studies show that the EU's as well as the worldwide security market will continue to have a growth rate which is beyond the average GDP growth.[1]

In response to this significant potential for market growth, the Commission made the security industry one of the essential parts of the EU 2020 flagship initiative *"An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage*".[2] Therein the Commission announced the launch of a dedicated initiative on a Security Industry Policy.

This Action Plan is the first stepping stone of this dedicated initiative. The overarching aim is to enhance growth and increase employment in the EU's security industry.

Thanks to their level of technological development many EU (security) companies are still among the world leaders in most of the segments of the security sector. Recent evolutions and market forecasts do, however, indicate that the market shares of European companies on the global market are bound to decrease constantly over the next years. Industry forecasts and independent studies predict that the current market share of EU companies in the security sector could drop by one fifth from around 25% of the world market in 2010 to 20% in 2020, if no action is launched to enhance the competitiveness of the EU security industry.

The market leading US companies are still the technological front runners, they additionally also benefit from a harmonised legal framework and a robust internal market. This gives them not only a reassuring basis but also the benefit of a clearly recognised and distinguishable US brand, which has proven to be a highly valuable advantage compared to EU companies in terms of international competition.

This lack of a similar "EU brand" is especially critical if one considers that the central future markets for security technologies will not be in Europe but in emerging countries in Asia, South America and the Middle East.

Asian countries are closing the technological gap that separates them from EU companies at an increasing rate. Without a technological advantage, the EU companies will be confronted with fierce competition, also in view of the production cost disadvantage often faced by EU firms.

---

1 All the figures and studies mentioned in this Action Plan are further detailed in the Staff Working Document (SWD) accompanying this Action Plan.

2 COM (2010)614 final.

The primary aim of the Commission is thus to establish a better functioning Internal European Market for security technologies. Favourable Internal Market conditions, enhancing competition and lowering production costs through the exploitation of scale economies, are also essential to strengthen the position of the EU security industry in those emerging countries that represent the future of the security sector. A special emphasis should be given to the support for SMEs in their efforts to access international markets in third countries.

The European Security Research and Innovation Forum (ESRIF), the subsequent Commission Communication[3] already addressed a number of these issues. For the ICT sector the promotion of security is an integral part of the equipments and products being offered by ICT companies and is key to future competitiveness. This will also be adressed in the the upcoming European Strategy for Internet Security. To date, however, there has not been a consistent EU-wide approach to make the EU security industry more competitive and innovative.

As present studies and stakeholder opinions[4] have shown, the pressure of global competition will target manufacturing of products and technologies rather than services, as those form the vast majority of export potential in the security industry. This Action Plan therefore does not cover security services as such (e.g. on site security personnel), but only those security services that relate to the installation and maintenance of security devices.

The Commission will make use of all the tools at its disposal to create a true Internal Market for security technologies, thus providing a strong home base for the EU security industry with a view to gain market shares in emerging markets.

The Commission will ensure that any initiatives taken for the development of the Internal Market for security technologies respect the Charter of Fundamental Rights, particularly the right to privacy and personal data protection.

2. THE EU SECURITY INDUSTRY AND MARKET

The global security market is estimated to be worth some €100 billion (2011 figure) with around 2 million persons employed worldwide. The EU security market has an estimated market value in the range of €26 billion to €36.5 billion with around 180,000 employees (2011 figures).

However, there is currently no clear definition of the security industry and a methodical classification of this industry is hindered by a number of factors:

- The security industry is not covered as such by the main statistical nomenclatures (NACE, Prodcom, etc.).
- The production of security-related items is hidden under a wide range of headings. Statistics for these headings do not distinguish between security and non-security related activities.
- There is no statistical data source available at European level from the industry itself.

[3] COM (2009)691 final.
[4] See the SWD.

- From a supply-side perspective, procurers of security equipment and systems can be reluctant to provide information on security expenditures.

In order to remedy the lack of data on the security industry and its market, the Commission will develop an empirical basis on which more reliable figures on the security markets can be obtained. Cooperation with the main trade associations is essential to such an undertaking.

The EU security industry can nevertheless broadly be subdivided into the following sectors[5]:

- aviation security;
- maritime security;
- border security;
- critical infrastructure protection;
- counter-terror intelligence (including cyber security and communication);
- crisis management/civil protection;
- physical security protection; and
- protective clothing.

The security market has three distinctive features:

(1) **It is a highly fragmented market divided along national or even regional boundaries.** Security, being one of the most sensitive policy fields, is one of the areas where Member States are hesitant to give up their national prerogatives.

(2) **It is an institutional market.** In large parts the security market is still an institutional market, i.e. the buyers are public authorities. Even in areas where it is a commercial market, the security requirements are still largely framed through legislation.

(3) **It has a strong societal dimension.** Whilst security is one of the most essential human needs, it is also a highly sensitive area. Security measures and technologies can have an impact on fundamental rights and often provoke fear of a possible undermining of privacy.

3. THE MAIN PROBLEMS FACED BY THE EU SECURITY INDUSTRY

These three distinctive features of the security market are also the determinants for the three main problems that the EU security industry faces:

(1) The fragmentation of the EU security market

---

[5] This list is not exhaustive, a more detailed overview on the various sectors and the technologies they encompass can be found in the SWD.

The main problem is the highly fragmented nature (e.g. the lack of harmonised certification procedures and standards) of the EU security market. Divergent approaches have effectively led to the creation of at least 27 different security markets, each of them being split into a large number of security sectors.

This not only creates a rather unique situation with respect to the Internal Market, but has also a considerable negative impact on both the supply side (industry) and the demand side (public and private purchasers of security technologies). It leads to high barriers to market entry and makes true economies of scale very difficult, if not impossible. Moreover, it leads to a lack of competition among suppliers and suboptimal use of public money.

(2) The gap between research and market

When performing R&D on new technologies, it is often very difficult for the EU based security industry to predict whether there will be in the end a market uptake, or even to get some sort of reassurance that there will be a market at all. While this is a widespread problem which can also be found across many industrial sectors, it is particularily pertinent for the security industry, which is mostly faced with an institutional market.

This leads to a number of negative consequences: for example, potentially promising R&D concepts not being explored, which in turn means that certain technologies that could improve the security of the citizen are not available to the demand side.

(3) The societal dimension of security technologies

The societal acceptance of new products and technologies is a general challenge across different industrial sectors. There are, however, a number of specificities that distinguish security technologies from other areas. Security technologies might directly or indirectly concern fundamental rights, such as the rights for respect for private and family life, protection of personal data, privacy or human dignity.

The problems assosciated to the societal acceptance of security technologies results in a number of negative conseqences. For industry it means the risk of investing in technologies which are then not accepted by the public, leading to wasted investment. For the demand side it means being forced to purchase a less controversial product which however does not entirely fulfil the security requirements.

4. TACKLING THE PROBLEMS

The Commission identified a number of key policy actions to enhance the competitiveness of the EU security industry, stimulate its growth and promote the creation of jobs. The key policy actions concern:

- **Overcoming market fragmentation**, through: the creation of EU wide/international standards, the harmonisation of EU certification/conformity assessment procedures for security technologies and a better exploitation of synergies between security and defence technologies.

- **Reducing the gap from research to market**, by: aligning the funding programmes and an enhanced exploitation of Intellectual Property Rights (IPR) routes, as well as

the full use of Pre-commercial procurement (PCP) in the context of security research in Horizon 2020[6].

- **Better integration of the societal dimension**, by thoroughly assessing social impacts including impacts on fundamental rights, and by creating mechanisms to test the societal impact during the R&D phase.

4.1. Overcoming market fragmentation

4.1.1. Standardisation

Standards play a major role in defragmenting markets and helping industry in achieving economies of scale. Standards are also of upmost importance for the demand side, notably with regard to interoperability of technologies used by first responders, law enforcement authorities, etc. Additionally, standards are essential for ensuring uniform quality in the provision of security services. Creating EU-wide standards and promoting them on a world wide level is also a vital component of the global competitiveness of the EU security industry.

However, only a few EU-wide standards exist in the security area. Divergent national standards pose a major obstacle for the creation of a true internal market for security, thus hindering the competitiveness of EU industry. Overcoming these national divergences is a quintessential step, if the EU wants to contribute significantly to the creation of global standards.

The Commission already announced in its Communication on a Strategic Vision for European Standards the need to speed up standardisation efforts in the security area[7]. Therefore, the Commission mandated in 2011 the European Standardisation Organisations to gather a detailed overview of existing international, European and national standards in the security area, as well as to set out a list of standardisation gaps. Major gaps were identified in the following areas:

– Chemical, Biological, Radiological, Nuclear and Explosives – minimum detection standards as well as sampling standards, including in the area of aviation security;

– Border security – common technical and interoperability standards for automated border control systems, as well as standards for biometric identifiers; and

– Crisis management/ Civil protection – standards for communication interoperability, as well as interoperability of command and control, including organisational interoperability, as well as mass notification of the population.

Action 1: Based on these initial priorities, the Commission will ask the European Standardisation Organisations to establish concrete and detailed standardisation roadmaps. These standardisation roadmaps should focus on the next generation of tools and technologies. To do so, end-user and security industry involvement and policy coherence will be essential.

Implementation period: from mid 2012

6 COM (2011) 809 final.
7 COM (2011)311 final.

4.1.2. Certification/ conformity assessment procedures

There are currently, no EU-wide certification systems for security technologies. National systems differ widely, thus significantly contributing to the fragmentation of the security market. The Commission has identified areas where[8], in an initial phase, it would make the most sense to set up an EU-wide certification system, starting with:

– airport screening (detection) equipment; and

– alarm systems[9]

As regards airport screening equipment, there exists a whole body of EU legislation which sets out performance requirements for such equipment[10]. However, this legislation does not contain the required conformity assessment mechanism so that certification of screening equipment in one Member State would be mutually recognised in any other Member State. The lack of harmonised standards and legally binding conformity assessment of airport screening equipment at the EU level causes fragmentation of the Internal Market.

As regards alarm systems, some European performance standards already exist. Moreover, there exists the industry-led certification mechanism CertAlarm. However, this system is faced with the problem that it is privately run and that Member State authorities have no obligation to accept certificates established under the scheme.

In the future, products certified on the basis of an EU wide certification system could receive an "EU Security Label", similar to the CE marking used in the field of product safety. As suggested by ESRIF, such a label could act as a 'seal of quality' for security products (made and validated in the EU).

It is conservatively estimated that for these two product categories industry would be able to make savings in terms of testing and certification costs of up to €29 million per year.

Harmonising the certification procedures for airport screening systems and alarm systems should also have a positive effect on the creation of a clearer European identity for these technologies, a possible "EU brand". This brand" should contribute to enhancing the global competitiveness of the EU companies with regards to their US and Chinese competitors.

---

8 Details on the rationale and the criteria for the selection of the targeted areas can be found in the SWD.

9 It should be noted that the alarm systems represent a highly important segment, with a market size of €4.5 billion or 50% of the physical security market.

10 See Regulations EC 300/2008, EC 272/2009 and EU 185/2010.

Action 2: Subject to a thorough impact assessment analysis and consultation of stakeholders, the Commission would propose two legislative proposals: one to establish an EU wide harmonised certification system for airport screening (detection) equipment; and one to establish an EU harmonised certification system for alarm systems. The objective is to achieve mutual recognition of certification systems**.**

Implementation period: mid 2012 – end of 2014

4.1.3. Exploiting synergies between security and defence technologies

One can clearly distinguish between a (civilian) security and a (military) defence market. However, the existence of these two separate markets can in itself be considered a fragmentation. To some extent, this fragmentation is normal, given that the industrial base supplying these two markets is not fully identical and that the end-users differ, application areas differ, and so do the requirements. However, this fragmentation is felt upwards at the level of R&D and capability development, and is felt downwards at the level of standardisation. It leads sometimes to the duplication of R&D efforts and the impossibility of making use of economies of scale due to differing standards in these two markets.

As regards R&D, civil-military synergies are currently being sought with the European Defence Agency (EDA) through the *European Framework Cooperation*. Under this cooperation there is an on-going coordination between the Security Theme of the 7th Framework Programme (FP7) and EDA's defence research activities. The aim is to synchronise this research with a view to avoid duplications and to profit from possible synergies. The Commission intends to continue and expand this cooperation under Horizon 2020.

As regards even more upstream cooperation, whilst such cooperation in view of a more synchronised capability planning would be useful, the Commission considers that in the civil security domain there is such a multitude of public authorities involved that it is currently not possible to establish common capability planning with the defence domain, where there is usually only one actor per Member State, i.e. the national defence ministries.

As regards downstream cooperation, the Commission considers that the development of 'hybrid standards', i.e. standards that apply both to civil security and defence technologies, should be actively pursued in areas where technologies are the same and application areas are very similar. The Commission is considering a number of promising areas for such 'hybrid standards', including software defined radio and certain technological requirements for unmanned aircraft systems (e.g. sense and avoid technologies, airworthiness requirements). For software defined radio alone it is estimated that hybrid standards could lead to an overall sales increase of one billion Euros.

Action 3: The Commission intends to issue, in close cooperation with the European Defence Agency, standardisation mandates to the European Standardisation Organisations for 'hybrid standards'. A first mandate will soon be issued for software defined radio.

Implementation period: from mid 2012

4.2. Reducing the gap from research to market

4.2.1. Aligning funding programmes, exploiting IPR routes

The Commission's proposal for Horizon 2020, establishes a close link with a number of policy areas, notably with home affairs. To this end, Horizon 2020 foresees specific IPR rules for security research, allowing the Commission and its Member States not only to have access to the foreground of security research projects, but also to make – on fair and reasonable terms – use of that foreground in subsequent procurement[11].

This should lead to a more direct and faster exploitation of the results of EU security research by the national authorities and a closer cooperation with the mostly public end-users, thus enhancing greatly the efforts to overcome the gap from research to market in the security area.

In addition, the two components of the Internal Security Fund, proposed for the next financial period, dealing respectively with external borders and visa and police cooperation, preventing and combating crime, and crisis management, foresee the possibility for Union funded actions to test and validate results stemming from EU security research projects[12].

For this possibility to be used effectively, the specific IPR rules for security research, which allow the Commission to use these IPR on fair and reasonable grounds, are a necessary feature, in order to be able to exploit security research results in subsequent testing and validation.

Where Union capacities are needed, the Commission will consider reinforcing these testing and validating measures through the actual purchase of prototypes for the EU, if adequate.

Action 4: The Commission will make full use of the new IPR rules provided for security research in Horizon 2020[13], in particular through the possibility provided in the two specific programmes of the Internal Security Fund to test and validate results stemming from EU security research projects.

Implementation period: from beginning 2014

4.2.2. Pre-commercial procurement

PCP[14] is a very useful tool in bridging the gap from research to market. The Commission underlined its importance already in its Innovation Union Communication[15], in particular in domains, where there is an institutional market or a market largely driven by legislation, given that public procurement of innovative products and services is vital for improving the quality and efficiency of public services at a time of budget constraints. Eventually, PCP should enable public users to play a more central role in the innovation cycle through the purchase of novel technologies. Procurers should act as "agents of change".

---

11 COM (2011)810 final.

12 COM (2011)750 and 753 final.

13 The adoption of these rules is however still subject to approval by the European Council and the European Parliament.

14 PCP is understood here as an approach to procure R&D services, whereby the IPR does not belong (exclusively) to the contracting authority. See COM (2007)799 final.

15 COM (2010)546 final

Nevertheless, to date only few Member States have made use of PCP schemes in the security area. At EU level, in the FP7 Security Theme, a pre-operational validation scheme was introduced in the call of 2011, acting as a precursor for a possible future PCP scheme.

Horizon 2020 contains a specific PCP instrument, which should greatly help in overcoming practical hurdles linked to the implementation of PCP.

Based on the US SBIR[16] experience, a tentative assumption of a 1% increase in the annual growth rate due to R&D support through a PCP scheme would lead in the security industry to extra sales of 2 billion Euros between today and 2020.[17]

Action 5: The Commission intends to make full use of the PCP instrument set out in Horizon 2020 and devote a significant part of the security research budget on this instrument. This novel funding approach should bring research closer to the market by bringing together industry, public authorities and end users from the very beginning of a research project. The Commission considers that border security and aviation security are the most promising areas for undertaking PCP.

The Commission will also encourage Member States to launch similar initiatives at national level, in compliance with relevant EU public procurement law.

Implementation period: from beginning 2014

4.2.3. Access to international procurement markets

The EU's public procurement market is traditionally very open. However, this is not always matched by a similar degree of openness by our trading partners. Worldwide, only a quarter of the world's procurement market is open for international competition.

The Commission has proposed a Regulation[18] to help open worldwide public procurement markets and to ensure European businesses have fair access to them. This Regulation is expected to provide a number of tools that will ensure that these objectives are reached.

Action 6: The Commission will make full use of the instruments at its disposal to ensure a fair access of its security industry to international procurement markets. Given the sensitive nature of security technologies, utmost attention will be given to relevant export regulations.

Implementation period: from end 2013

4.2.4. Third party liability limitation (TPLL)

To overcome the gap from research to market and in particular to ensure that the threat of liability does not deter security industry from developing, deploying and commercializing technologies and services that could save lives, the US introduced after 9/11 the US Safety Act. The US Safety Act provides for legal liability limitations for providers of anti-terrorism

16 SBIR stands for "Small Business Innovation and Research" and is a US programme supporting innovation in SMEs using a PCP scheme.

17 See the SWD.

18 COM(2012) 124 final

technologies and services. In third country markets, this legislation might give the market leading US companies a competitive advantage over their EU counterparts.

It is evident, that the US Safety Act is born out of the specific US legal context, where class action is a recurrent feature. Whilst it is not foreseen to establish an equivalent to the US Safety Act in Europe, there is, however, a need to better understand and study how far liability issues deter industry from bringing promising technologies and services to the market.

No general consensus exists among industry stakeholders on this issue and a thorough legal analysis on the compatibility with national or EU regulations has yet to be conducted.

Action7: 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 as introduced through the US Safety Act, such as for example a voluntary industry fund, a Commission recommendation, etc. This study will take due account of fundamental rights' implications.

Implementation period: 2012 – mid 2013

4.3. Better integration of the societal dimension

4.3.1. Societal impact "checking" during the R&D phase

A better integration of the societal dimension into security industry activities would help in reducing the uncertainty of societal acceptance. This should allow for an efficient use of R&D investment, as well as allowing the demand side to purchase products which fulfill entirely their security requirements and at the same time are accepted by society.

The Commission, therefore, considers that the societal and fundamental rights impact should already be taken into account through societal engagement before and during the R&D phase. This would allow addressing societal issues early on in the process.

The Commission already undertook a number of activities with a view to mainstream the societal dimension in the FP7 Security Theme. In view of Horizon 2020, it is, however, now time to consolidate these efforts, to engage society in research and innovation and make societal impact checking more systematic.

The Commission will involve society and make societal impact testing an obligatory part, where appropriate, of all its future security research projects[19]. The Commission will specifically "check" the societal impact of new technologies in all its security PCP schemes outlined above.

4.3.2. Privacy by design and privacy by default during the design phase

On the one hand, it is extremly difficult to translate societal considerations into technological requirements, which is further complicated by the wide variety of security products on the

[19] With the exception of "unsuited" areas, such as for instance basic technology research and projects on foresight and scenarios.

market. On the other hand, societal issues related to security vary considerably among Member States.

The Commission, therefore, considers that the best way forward is to introduce the concept of "privacy by design" and "privacy by default"[20] at the design phase. To this end, the economic operator wishing to have his production process audited as being "privacy by design" fit, would have to fulfil a set of requirements defined through an appropriate EU standard. This standard will be voluntary. The Commission is, however, convinced that there will be strong peer pressure for companies to follow such a standard which should gain a similar recogition value as for example the ISO 9000 management standard.[21]

Action 8: The Commission will issue a mandate to the European Standardisation Organisations to develop a standard modelled on existing quality management schemes, but applied to the management of privacy issues during the design phase.

Implementation period: mid 2012 – mid 2015

5. MONITORING

The monitoring of the announced policy measures will be overseen through a dedicated expert group set up by the Commission. This group will bring together all relevant actors in the field of security.

This group will meet at least once per year to monitor progress.

6. CONCLUSION

This is the first Action Plan by the Commission specifically targeting the security industry. Not only are the announced measures, therefore, a first, but also the comprehensiveness of the approach, ranging from the R&D phase up to standardisation and certification, a novelty. Depending on future assessments, possible next areas for harmonisation could include the land and maritime transport sectors as well as addressing TPLL.

It should be kept in mind that all the Actions listed in this document are closely linked to the willigness of the Member States to cooperate with the European Institutions, standardisation bodies, public and private stakeholders to overcome the fragmentation of the EU security markets. The Commission thus encourages the Member States to support the Commission in its initiative to enhance the competitiveness of the EU security companies and reduce the existing barriers to market entry.

The Commission is convinced that the policy measures outlined in this Action Plan will strongly contribute to improve the competitiveness of the European Security Industry. The Commission's objective is to provide to the EU security industry a strong home base from which to be able to expand into new and emerging markets, where in the future major growth for the security market can be expected.

---

20 For more details on privacy by design, see SWD.

21 COM(2012) 11

Such growth inside and outside the EU has to go hand in hand with the reinforcement of measures aimed at better integrating the societal dimension into security industry activities. Privacy by design and respect of fundamental rights needs to be embedded as a key aspect into all EU security technologies.