



PSC Europe

PSC-EUROPE/014-2011

DG ENTR's Public Consultation on an Industrial Policy for the Security Industry

PSCE REPLY

PREPARED BY: PSCE Secretariat
DATE: 13-05-2011
PSC Europe: Final version

DRAFT REPLY: PSCE, April 2011
DG ENTR's Public Consultation on an Industrial Policy for the Security Industry

1. RESPONDENT PROFILE

1.1. Name

Eric DAVALO

1.2. email address

secretariat@psc-europe.eu

1.3. You are/you represent

Public Safety Communication Europe

1.4. Name of Organisation

Public Safety Communication Europe

1.5. Job title (optional)

President

1.6. Day-time phone number (optional)

+32 (0) 2 738 07 63

1.7. In which country are you/is your organisation based? Please specify

Belgium

1.8. What is your/your organisation's main sector of activity?* (compulsory) (between 1 and 250 characters)

Public Safety Communication Europe Forum (PSCE) is a permanent autonomous organisation aiming at improving provision of public safety communications and information management systems and the safety of the citizens during crisis and emergency situations. PSCE provides a unique common platform for researchers, industry and users enabling regular exchange of ideas, information, experiences and best practices.

1.9. What security solutions does your company produce/offer? (optional) (between 1 and 300 characters)

While PSCE does not directly offer any security solutions, PSCE is an information platform for members from user, industry and research in the field of Public Safety Communications

2. MARKET FRAGMENTATION

2.1.1. Certification/conformity assessment procedures - Problem definition (1 – do not agree at all; 4 – agree very much)

	Do not know	1	2	3	4
Do you agree that the lack of harmonised certification/conformity assessment procedures for security technologies affects the market					x

fragmentation?					
----------------	--	--	--	--	--

2.1.2. Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market fragmentation: (1 no effect, 4 very strong effect)

	Do not know	1	2	3	4
Option 1: No change - certification/conformity assessment procedures will continue to be regulated by national systems.		X			
Option 2: EU wide harmonised certification/conformity assessment procedures covering all (or at least as many as technically possible) security products				X	
Option 3: Step by step: certification/conformity assessment procedures focused on certain priority areas or priority technologies where there is a clear EU added value.					X

Other option. (Please describe - upload of additional documentation is possible) (optional) (between 1 and 500 characters)

Option 2 would be the most desirable one but is unrealistic and might take too long to implement. Option 3 might therefore be preferable even if the overall market fragmentation is not being reduced at once. It should be seen as a way to pave the way for option 2.

Upload of additional documentation? No.

2.1.3. Could you please specify for which products, technologies and/or systems you experienced problems due to differing national certification/ conformity assessment procedures? (optional) (between 1 and 500 characters)

PSCE is not directly involved in certification procedures, but its members regularly report problems in having too diverging, lengthy and hence expensive procedures in different member states for certification/conformity assessments.

Upload of additional documentation? No.

2.2.1. Standardisation - Problem definition (1 – do not agree at all; 4 – agree very much)

	Do not know	1	2	3	4
Do you agree that the lack of EU wide standards for security affects the market fragmentation?					x

2.2.2. Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market fragmentation: (1 no effect, 4 very strong effect)

	Do not know	1	2	3	4
Option 1: No change: continue the ad-hoc, piece meal approach whereby the Commission mandates the ESO's to develop EU-wide standards based on immediate needs. In parallel industry develops on its own initiative EU-wide standards.		X			
Option 2: Industry driven - the Commission would stop mandating the ESOs to develop standards, but would leave this process entirely to industry				X	
Option 3: Step-by-step end-user driven standardisation based on a careful identification of existing, national, European and international standards, via Commission mandates to ESO's					X

Other option. (Please describe - upload of additional documentation is possible) (optional) (between 1 and 500 characters)

No.

Upload of additional documentation?

The current process (option 1) is largely ineffective as it takes too long. The public and the private side should not engage in separate initiatives, but avoid duplications of efforts. Initiatives should be coordinated.

An industry-led process (option 2) would have the advantage of including those who have the expertise and the knowledge of what standards are needed. Yet it would result only in voluntary or de facto standards, and as such the market fragmentation will be reduced only according to market speed and rules. Disadvantage here: users are not or not directly involved.

An end-user driven process (Option 3) is crucial for the success of standards, and a step-by-step approach seems reasonable and realistic. Yet, crucial is also the private sector expertise which will have to deliver solutions and services according to pre-determined standards. These standards should not be defined elsewhere. Therefore Option 3 should be enhanced with the inclusion of the private sector in the discussions and the standards definition.

A fourth, and the preferred option, would therefore be to develop standards within the framework of a Public-Private Dialogue and Cooperation, involving users, industry, but also academia/research. This option would combine the best of all other options mentioned above.

FOLLOW UP QUESTION ON MARKET FRAGMENTATION:

2.3. Could you please specify for which products /technologies and/or systems would you consider EU-wide standards most needed to overcome market fragmentation (upload of additional documentation is possible)? (optional) (between 1 and 500 characters)

Standards can be foreseen in all areas of the security domain. Considering the PSCE scope of expertise, it has been proved that in the event of accidents, emergencies or disasters, the various Communities of Interest such as the public and the first responders have difficulty to access and share information between them. Interoperability is needed to solve this key issue within a county, a region, a nation and between nations. There are different levels of interoperability ranging from technical to organizational aspects.

Upload of additional documentation? No.

2.4. Do you consider it useful to include in a possible certification assessment procedure not only products, but also systems (a number of interconnected technologies) and processes (multiple technologies + related services)?

	Do not know
X	Very useful
	Somehow useful
	Not Useful

Upload of additional documentation? No.

2.5. Further suggestions

Do you recommend any additional measures that would effectively tackle market fragmentation? (optional) (between 1 and 500 characters)

Doc. Ref. PSC-Europe/014-2011
DG ENTR's Public Consultation on an Industrial Policy for the Security Industry
PSCE REPLY

Harmonisation of the legal framework regarding liability and privacy and data protection issues, as described later in this consultation.

Harmonized procurement rules could also reduce market fragmentation, as could a better structuring of the demand side, e.g. through the encouragement of joint procurement. European Reference solutions should also be defined.

Upload of additional documentation? No.

2.6. Subsidiarity principle

Do you consider that action by the EU would be necessary to reduce the market fragmentation?

	Do not know
X	Yes
	Yes partly
	No

3. FRAGILE INDUSTRIAL BASE

3.1.1. Could you please provide your views on a level of 1 to 4 (1 do not agree at all, 4 agree very much) on the fragility of the industrial base:

	Do not know	1	2	3	4
Do you agree that the EU security industrial base is fragile?					X

3.1.2. Could you please elaborate on what this fragility of the industrial base consists of in your view (1 do not agree at all, 4 agree very much)

	Do not know	1	2	3	4
Fragile in terms of third country competition					X
Fragile in terms of development of state of the art technologies				X	
Fragile in terms of access to finance					X
Fragile in terms of dependency from the primes			X		

Other option. Please describe (optional) (between 1 and 500 characters).

Fragile in that the security market operates in a restricted and highly specialized market (score 3); fragile in terms of large integrators' dependency on the sustainability and strength of European SMEs for innovative solutions and equipments (score 3).

Upload of additional documentation? No.

The European security industrial base operates in a segmented market which limits the exploitation of economies of scale. This hampers European global competitiveness and innovation. Whereas e.g. US-based companies can draw on the support of a highly organised market and end-user, European companies lack this. Investment and innovation are therefore limited in their effectiveness. Amongst others, a more structured market, most notably a more structured demand side could remedy this.

3.2. Pre-Commercial Procurement

Please indicate on a level of 1 to 4 (1 no effect, 4 very strong effect) which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:

	Do not know	1	2	3	4
Option 1: No change Pre-commercial Procurement in the area of security		X			

would be solely done on a national level					
Option 2: Pre-commercial procurement activities would be carried out in FP8 but without specific financing instruments			X		
Option 3: A focused pre-commercial procurement scheme being built up via the possible future FP8 and/or CIPII funding.					X

Other option. Please describe (optional) (between 1 and 500 characters)

PCP needs to be extended to the security sector. Member States should be allowed to engage in PCP, but joint PCP should also be encouraged to overcome market fragmentation & to tackle larger scale innovation needs.

Given the particularities of the security sector, current FP procedures are inadequate (too long & cumbersome). The needed definition and the innovative output have to match the pace of the threat evolution. A specific funding instrument should thus be foreseen.

Upload of additional documentation? No.

3.3. Defence and Security Procurement

Please indicate on a level of 1 to 4 (1 no effect, 4 very strong effect) which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:

	Do not know	1	2	3	4
Option 1: No change – The Defence Procurement Directive will now provide a clear and sufficient framework to contribute effectively to reducing market fragmentation.			X		
Option 2: Encourage security customers to pool their investment resources in order to achieve interoperability and economies of scale.					X

Other option. Please describe (optional) (between 1 and 500 characters): None.

Upload of additional documentation? No.

3.4. Synergies between civil and defence technologies

Please indicate on a level of 1 to 4 (1 no effect, 4 very strong effect) which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:

	Do not know	1	2	3	4
Option 1: No change - the Commission would continue to coordinate research activities between FP7 and EDA on an ad-hoc basis				X	
Option 2: Strengthening synergies between civilian and defence technologies in a step by step approach via more upstream coordination at the level of capability development and more downstream coordination at the level of development of standards					X
Option 3: In addition to option 2, this option would go beyond coordinated research activities by establishing a dedicated civil-military research programme as part of FP8			X		

Other option: -

Please describe (optional) (between 1 and 500 characters) -

Upload of additional documentation? No.

3.5. International markets

Please indicate on a level of 1 to 4 (1 no effect, 4 very strong effect) which of the policy options described above do you think is most effective and realistic to reduce market fragmentation:

	Do not know	1	2	3	4
Option 1: No change - the EU would not undertake any specific activities to encourage access to third markets for the EU security industry		X			
Option 2: Opening up of international markets for security products by making full use of the EU's trade policy strategy.					X
Option 3: In addition to option 2 - the Commission would aim at fostering the adoption of joint or common approaches at international level, notably in the area of standards via the International Standardisation Organisation. The approach would also provide an opportunity to raise the visibility of the European security industry around the world.					X

Other option: -

Please describe (optional) (between 1 and 500 characters)

It is very important that Europe is not left out of the standards setting discussion. It would be detrimental to the European economy if non-European standards were adopted worldwide. The EU should therefore urgently promote the standard setting at EU level in view of participating in international discussions for international standards.

Upload of additional documentation? No.

3.6. Third party limited liability protection

Please indicate on a level of 1 to 4 (1 no effect, 4 very strong effect) which of the policy options described above do you think is most effective and realistic to address the issue of third party limited liability protection:

	Do not know	1	2	3	4
Option 1: No change - under this option the EU would not get involved in Third Party Liability issues		X			
Option 2: Introducing harmonised rules at EU level on Third Party Liability Limitations for security products/processes/systems in case of a terrorist incident. Under this option the EU would define under which circumstances and conditions companies/system operators could invoke Third Party Liability Limitation. The EU would also define the minimum or maximum financial compensation up to which companies/system operators would be liable for					X
Option 3: Encouraging Member States to introduce such legislation at national level with the Commission as guardian of the Treaty ensuring that such a decentralised approach does not lead to internal market barriers. Under this option, the Commission would set out guidelines to help Member States in setting up Third Party Liability Limitation schemes that would not be contradictory between different Member States, thus leading to internal market barriers			X		

Other option. Please describe (optional) (between 1 and 500 characters):

The lack of appropriate third party liability limitation in the EU jeopardizes the overall sustainability of the European Security Industry, making Europe dependent on security sensitive non-European solutions, & hampering investment & innovation for the protection of EU citizens with the best anti-terrorism technologies and services. To ensure an equal level-playing field, avoid legal uncertainty and costly law suits for determining the applicable jurisdiction the EU should adopt a regulation.

Doc. Ref. PSC-Europe/014-2011

DG ENTR's Public Consultation on an Industrial Policy for the Security Industry

PSCE REPLY

Upload of additional documentation?

3.7. Follow up question on third party limited liability market fragmentation

Could you please specify whether you experienced problems regarding third party liability on a national and/or EU wide level? (optional) (between 1 and 500 characters)

No.

3.8. Further suggestions

Do you recommend any additional measures that would effectively strengthen the security base in the EU? (optional) (between 1 and 500 characters)

None.

Upload of additional documentation?

3.9. Subsidiarity principle

Do you consider that action by the EU would be necessary to reinforce the industrial base?

	Do not know
X	Yes
	Yes partly
	No

4. SECURING THE CITIZEN AND THE SOCIETY

4.1.1. Problem definition (ranking from 1 do not agree at all to 4 agree very much)

	Do not know	1	2	3	4
Do you agree with the problem definition, that security products need to be privacy compliant from the development to the production?					X

4.1.2. Which option, on a level of 1 to 4 (1 no effect, 4 very strong effect) do you think is effective and realistic to ensure that the ethical/societal dimension of security is introduced in an industrial policy for the security sector?

	Do not know	1	2	3	4
Option 1: No change - privacy by design would remain a voluntary effort for industry with no EU wide guidelines and/or requirements		X			
Option 2: A voluntary certification/conformity assessment system. Under this option the economic operator wishing to have his product/process/system certified for being "privacy by design" fit, would have to fulfil a set of requirements defined by the EU. However, the certification/conformity assessment itself would remain voluntary.					X
Option 3: In addition to option 2 – the certification certification/conformity assessment would be mandatory	X				

Other option. Please describe (optional) (between 1 and 500 characters).

Upload of additional documentation?

Another option in between the voluntary and the mandatory assessment would be to foresee benefits and economic incentives for those that voluntarily certify their solutions. Any certification should be recognized EU-wide.

Not all products are privacy-sensitive. It would not make sense to impose a certification/conformity assessment on any product/service. Companies should decide whether or not they need such an assessment. However, those who decide to participate should receive some benefits, such as facilitated market access or preferential treatment during public procurement processes. EU-wide mutual recognition should however be established to avoid market distortions and unnecessary burden for companies.

4.2 Certification procedures

Do you believe it to be useful to merge a possible ethical certification procedure as detailed in point 4.1. should be with the certification procedures outlined in point 2.1, instead of having two separate certification procedures?

	Do not know
	Very useful
X	Somehow useful
	Not Useful

4.3. Research on Privacy compliant technologies

Which option, on a level of 1 to 4 (1 no effect, 4 very strong effect) do you think is effective and realistic to ensure that the ethical/societal dimension of security is introduced in an industrial policy for the security sector?

	Do not know	1	2	3	4
Option 1: No change - Through targeted research projects in the Security Theme of the FP aimed at developing "privacy by design" technologies. These technologies could then be applied in future security products, processes or systems.					X
Option 2: Making the privacy compliance a mandatory evaluation criteria for all technology related research proposals under the Security Theme of the FP. Under this option, the EU would make it mandatory to address privacy by design in all technology related research proposals of the Security Theme of the FP.				X	

Other option. Please describe (optional) (between 1 and 500 characters)

Privacy compliance should be a mandatory evaluation criteria only for those FP activities It should be encouraged not only with regard to research activities, but also with regard to deployment activities. For that please consult the comments on privacy certification procedures above and the further suggestions below.

Upload of additional documentation? No.

4.4 Further suggestions

Do you recommend any additional/other option that would effectively reinforce the ethical/societal dimension of security in the envisaged industrial policy for the security sector? (optional) (between 1 and 500 characters)

A clear and harmonized legal framework, such as concrete EU guidelines and requirements for Privacy-by-Design could give needed guidance to the security industry on what to do for their solutions and services to be considered privacy compliant. The framework should be defined narrowly enough to avoid

Doc. Ref. PSC-Europe/014-2011

DG ENTR's Public Consultation on an Industrial Policy for the Security Industry

PSCE REPLY

that differing interpretations of the guidelines could result in market distortions and legal uncertainty on part of the industry.

Upload of additional documentation? No.

5. Final questions

5.1 Are you aware of any initiatives in your country that have one of the above goals in mind (upload of documentation is possible)

a) Reducing market fragmentation (optional) (between 1 and 500 characters)

No.

Upload of additional documentation? No.

b) Strengthening the industrial base. (optional) (between 1 and 500 characters)

No.

Upload of additional documentation? No.

c) Introducing the ethical/societal dimension in security technologies. (optional) (between 1 and 500 characters)

No.

Upload of additional documentation? No.