

Results of the Public Consultation on an Industrial Policy for the Security Industry

1. Introduction

On the 14th of March the European Commission launched a Public Consultation in preparation of the upcoming Communication Industrial Policy for the Security Industry (planned for early 2012).

2. Consultation document

The objective of this consultation was to collect the stakeholders' views on the envisaged policy measures aimed at an enhancing the security of the European citizens through a dedicated EU security industry policy.

Stakeholders were invited to express their opinions on the main problems the EU security industry faces today, namely:

- Ø the fragmentation of the EU security markets,
- Ø the lack of EU wide standards.
- Ø the fragility of the EU industrial base, and
- Ø the integration of societal aspects in the development of security technologies.

Participants were given the possibility to add comments or suggest additional options to those suggested by the Commission on the majority of the questions. Respondents had furthermore the possibility to upload documents/position papers on a number of questions in the consultation. This opportunity was seized by a large number of participants; around 100 documents were uploaded by the respondents.

A number of stakeholders did not fill out the online questionnaire, but sent in position papers on possible policy measures for an Industrial Policy for the Security Industry. These position papers do not appear in the statistics, the content of these papers has nevertheless been taken into account in the overall analysis.

<p><u>General remark on the analysis of the consultation:</u> The text passages in <i>italic</i> are quotes taken from the contributions to the consultation.</p>

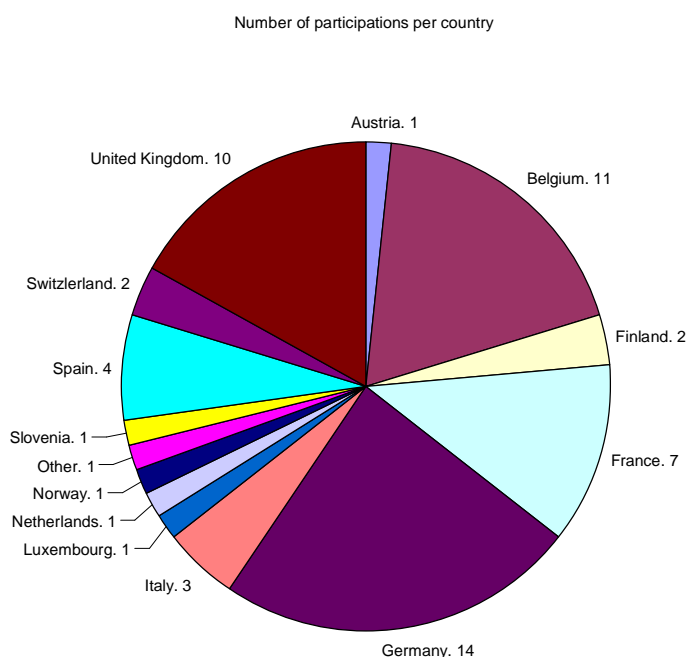
Respondents were able to rank their responses on a scale of 1 (do not agree at all/no effect) to 4 (agree very much/ very strong effect).

Two participants submitted a position paper, in which they explained that, according to their interpretation, security services should be a part of the questionnaire. Their submission to the questionnaire has therefore a different scope, which includes services.

3. Responses to the consultation

The European Commission received in total 59 responses to the public consultation. Contributions were received from stakeholders in 13 countries (one additional participant did not specify his country of origin), including 2 EFTA countries.

Table 1: The respondent's countries of origin



Background of the respondents

The respondents can be classified into ten main categories: micro or small enterprises, medium enterprises, large enterprises, business associations, national administrations, Regional or local administrations, academic institution or think tank, non governmental organisation, individuals and others. The high participation of SME's (19%) should be noted.

Background of the respondents		
Stakeholder category	Number of replies	Percentage
Micro or small enterprise (fewer than 49 employees, turnover less than €10 million)	6	10.20%
Medium enterprise (between 50 and 249 employees, turnover less than €50 million)	5	8.50%
Large enterprise (more than 250 employees)	19	32.20%
A business association	13	22%
A national administration	4	6.80%
Regional or local administration	1	1.70%
An academic institution or think tank	3	5.10%
Non governmental organisation	4	6.80%
An individual	1	1.70%
Other	3	5.10%

4. Responses on the chapters

Subsidiarity principle

The initiative of the Commission to launch specific policy measures on a dedicated Security Industry Policy was met with a very large approval. A number of participating Member States explicitly welcomed and encouraged the proposals of the Commission, stating that the security industry should finally be recognised as a specific industrial sector with a need for dedicated policy mechanisms.

Market fragmentation:

The need for the EU to act on the issue of market fragmentation has been unambiguously agreed upon by ~ 86% of the participants. Only two out of 59 negated the need for an EU action.

2.6. Subsidiarity principle Do you consider that action by the EU would be necessary to reduce the market fragmentation?		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
Yes	39	66.10%
Yes, partly	12	20.34%
No	2	3.39%

Industrial base

On the question: "Do you consider that action by the EU would be necessary to reinforce the industrial base?" 86% of the participants either answered with "yes" or "yes partly". Not a single respondent answered with no.

3.9. Subsidiarity principle Do you consider that action by the EU would be necessary to reinforce the industrial base?		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
Yes	38	64.41%
Yes, partly	13	22.03%
No	0	0.00%

4.1. Market Fragmentation

4.1.1 Certification/conformity assessment procedures

The vast majority of the consulted participants agreed with the problem definition of the Commission that "the lack of harmonised certification/conformity assessment procedures for security technologies affects the market fragmentation". Out of 59 replies 33 stated to agree very much and 15 stated to agree with the problem definition, only three did not agree. One national representative explicitly stated that a true internal market for security is still a distant concept.

The majority of the participants emphasized the absolute urgency to act on the fragmentation of the EU security markets, underlining that this is the most pressing policy related concern.

This large approval was also clearly reflected in the rankings of the suggested options. The first option "no change", in which the certification would remain at a national level, was rejected by all participants. The most favoured option of the three possible choices was option three the "Step by step approach". The Step by Step approach was considered by most to be the most realistic path to a harmonised certification system in the EU. One of the determining factors for this assessment seemed to be the new and diverse character of the security sector.

A certain number of participants also expressed their support for a more direct harmonisation of EU certification procedures, conceding however that the implementation of a drastic change would probably not be feasible: *"Option 2 would be the most desirable one but is unrealistic and might take too long to implement."*

Option 1: No change - certification/conformity assessment procedures will continue to be regulated by national systems.		
	Number of requested records	% Requested records(59)
Do not know	12	20.34%
1	46	77.97%
2	1	1.69%
3	0	0.00%
4	0	0.00%
Option 2: EU wide harmonised certification/conformity assessment procedures covering all (or at least as many as technically possible) security products		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	2	3.39%
2	15	25.42%
3	26	44.07%
4	8	13.56%
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.		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	3	5.08%
2	5	8.47%
3	10	16.95%
4	32	54.24%

Central stakeholder positions on harmonised EU certification procedures

Independently of their background (SME, large industry, public authority etc.), the stakeholders underlined the clear added value of a European-wide certification regime. The main expected benefits being:

- Ø Reduction of the duplication of certification procedures
- Ø Reduction of the administrative burden for the supply and demand side
- Ø Enhancement of the competitiveness and growth of the EU security industry and
- Ø Support to the creation of an end to end European Security approach from research to commercialisation.

The question of an extension of a possible certification assessment procedure not only to products but also to systems was also received with a large support, 39 respondents qualified it as very useful, 10 as somehow useful and only 2 as not useful.

4.1.2. Standardisation

A vast majority of the participants agreed that the lack of standards affects the fragmentation of the EU security markets. Out of 59 participants 40 agreed very much, 7 agreed and only 7 disagreed on the problem definition (question 2.2.1).

The favoured option of the respondents was, similarly to question 2.1.2., option 3 the "Step by Step approach" (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) with an approval of 75% (30 very agree much 15 agree) followed by option 2 (Industry driven - the Commission would stop mandating the ESOs to develop standards, but would leave this process entirely to industry) with an approval of 30% and 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.) with an approval of 22%.

The majority of the participants agreed that the establishment of EU wide security standards can only be driven by end user requirements.

"An end-user driven process (Option 3) is crucial for the success of standards, and a step-by-step approach seems reasonable and realistic."

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.		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	21	35.59%
2	17	28.81%
3	12	20.34%
4	1	1.69%
Option 2: Industry driven - the Commission would stop mandating the ESOs to develop standards, but would leave this process entirely to industry		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	22	37.29%
2	12	20.34%
3	17	28.81%
4	1	1.69%

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		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	1	1.69%
2	6	10.17%
3	15	25.42%
4	30	50.85%

A number of business associations also expressed their interest for a fourth possible option, in which standards would be developed within the framework of a Public-Private Dialogue and Cooperation.

Possible areas of interest for EU wide security standards

- Border management systems
- Cybersecurity
- Crisis management and civil protection
- Sensor and system limitations
- Identity management and biometry
- Critical infrastructure protection
- Aviation security (airport scanners)
- CBRNE
- IT security
- PKI (Public Key Infrastructures) standards or cryptographic mechanisms and secure protocols

4.2. Fragile industrial base

The responses to the problem definition on this specific point were relatively evenly spread over the possible answers. Categorising the EU security industrial base as generally fragile would not reflect the reality of the markets. Most participants stated that the EU security industrial base cannot be labelled as fragile, given that European security companies are among the market leaders in many high tech areas.

Do you agree that the EU security industrial base is fragile?		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	3	5.08%
2	17	28.81%
3	17	28.81%
4	14	23.73%

The EU industrial base was however categorised as fragile in a number of specific areas by a majority of the participants, namely in terms of third country competition (64% approval) and to a lesser degree in terms of access to finance (61% approval). The main aspect on which the participants call for EU action is the strengthening of the competitiveness of the EU industry on a global scale. A common statement on this issue was submitted by a series of different participants (mainly business associations).

"The industrial base across the EU is however fragile in the sense that it is currently losing out to industries in countries such as the United States in a fiercely competitive global security market; in significant part owing to the support industries outside receive from their host Governments. The industrial policy framework for helping companies in the EU to compete in the security market is currently insufficient. Subsidies and related initiatives such as the US Safety Act mean that the security industry across the EU is losing its competitive edge in the global market."

One of the participating business associations also pointed out two additional factors which, according to them, also contribute to the fragility of the EU industrial base, namely:

- Ø *"Fragile in that security solution and service providers operate in a restricted and highly specialized market"*
- Ø *"Fragile in terms of large integrators' dependency on the sustainability and strength of European SMEs for innovative solutions and equipments [...] Unfortunately Europe's SME base is increasingly vulnerable as administrative burdens and costs to comply with an increasing amount of legal regulations is becoming more and more enterprise-threatening. The Commission is therefore urged to engage in positive action to support the SME base, e.g. by easing their access to funding and by simplifying bureaucratic procedures."*

3.1.2. Could you please elaborate on what this fragility of the industrial base consists of in your view:

Fragile in terms of third country competition		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	2	3.39%
2	11	18.64%
3	13	22.03%
4	25	42.37%
Fragile in terms of development of state of the art technologies		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	9	15.25%
2	13	22.03%
3	12	20.34%
4	18	30.51%
Fragile in terms of access to finance		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	3	5.08%
2	11	18.64%
3	12	20.34%
4	24	40.68%
Fragile in terms of dependency from the primes		
	Number of requested records	% Requested records(59)
Do not know	18	30.51%
1	5	8.47%
2	17	28.81%
3	12	20.34%
4	7	11.86%

4.2.1. Pre Commercial Procurement

The issue of Pre Commercial Procurement addressed in question 3.2. of the questionnaire generated an unequivocal response from the respondents.

- Ø Option 1: No change Pre-commercial Procurement in the area of security would be solely done on a national level. Approval rate = 11%
- Ø Option 2: Pre-commercial procurement activities would be carried out in FP8 but without specific financing instruments. Approval rate = 20%
- Ø Option 3: A focused pre-commercial procurement scheme being built up via the possible future FP8 and/or CIPII funding. Approval rate = 76%

A number of participants underlined the crucial role Pre Commercial Procurement in the security sector could play in the future attempts to harmonise the EU security markets. Pre Commercial Procurement schemes could, in combination with certification and standardisation measures, bring together all relevant actors and ensure a better integration of the end users and their specific requirements.

*"It is especially important for sectors such as security where the primary customers are public bodies and where applications of innovative technologies are highly regulated."
"[...] it would be a valuable "route to product" for end-users and security companies across the EU."*

4.2.2. Defence and Security Procurement

The ratings of the respondents on the two options concerning the Defence Procurement Directive did not suscite any distinctive majority, which could allow a clear assessment. One quarter of the participants choose the "do not know" answer, none of the options assembled a clear approval rate.

According to the statements made by the participants, this is largely due to the fact that the Defence Procurement Directive has only been in place for a relatively short amount of time. A judgement of its efficiency would therefore be premature.

Option 1: No change - The Defence Procurement Directive will now provide a clear and sufficient framework to contribute effectively to reducing market fragmentation.		
	Number of requested records	% Requested records(59)
Do not know	15	25.42%
1	15	25.42%
2	23	38.98%
3	4	6.78%
4	2	3.39%
Option 2: Encourage security customers to pool their investment resources in order to achieve interoperability and economies of scale.		
	Number of requested records	% Requested records(59)
Do not know	14	23.73%
1	9	15.25%
2	5	8.47%
3	16	27.12%
4	15	25.42%

4.2.3. Synergies between civil and defence technologies

Out of the three options proposed to the participants on synergies between civil and defence technologies, the second option "step by step approach" was clearly the one which received the most positive answers (53%). Option 3 (a dedicated civil-military research programme as part of FP8) had an approval rate of 30% and option 1 (No change) an approval rate of 15%.

The majority of the participants expressed their interest in an enhanced cooperation between the Commission and EDA on possible civ-mil synergies. The establishment of a dedicated defence theme was judged to be unrealistic and a possible threat to national defence research budgets. Most respondents agreed that an extended European Framework Cooperation would be the adequate platform for such an enhanced cooperation. It should be noted that most key actors from large industry groups, business associations to Member States supported this option.

"In general, we believe that the establishment of a dedicated civil-military research programme is not necessary, as dual-use research already exists in the present research schemes. In addition, such a dedicated programme could incite national MoDs to cut their investments, which would have a globally counter-productive effect. [...] has welcomed and supported the European Framework Cooperation (EFC) that has been created to systematically synchronize the R&T investment [...]."

Two participants also expressed their concern regarding a possible "militarisation" of civilian research. They stressed that security research should only focus on the civilian dimension and that defence research should be explicitly excluded from EU security research.

Option 1: No change - the Commission would continue to coordinate research activities between FP7 and EDA on an ad-hoc basis		
	Number of requested records	% Requested records(59)
Do not know	10	16.95%
1	31	52.54%
2	9	15.25%
3	7	11.86%
4	2	3.39%
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		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	10	16.95%
2	9	15.25%
3	22	37.29%
4	9	15.25%
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		
	Number of requested records	% Requested records(59)
Do not know	13	22.03%
1	18	30.51%
2	10	16.95%
3	3	5.08%
4	15	25.42%

4.2.4. International markets

The results on the questions related to the possible options on international markets were unambiguous. The "no change" option was rejected by all but three participants. The two options which would incite action to open up the international markets for security products were both met with an approval of 77%. The third option was slightly favoured, with three more rankings "very strong effect" than the second option.

These results reflect also the importance accorded by the participants to the issue of third country competition in the context of question 3.1.2. "Fragile industrial base".

Option 1: No change - the EU would not undertake any specific activities to encourage access to third markets for the EU security industry		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	46	77.97%
2	2	3.39%
3	2	3.39%
4	1	1.69%
Option 2: Opening up of international markets for security products by making full use of the EU's trade policy strategy.		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	1	1.69%
2	6	10.17%
3	21	35.59%
4	24	40.68%
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.		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	2	3.39%
2	4	6.78%
3	18	30.51%
4	27	45.76%

4.2.5. Third party limited liability protection

The question of "Third party limited liability protection" was the issue with the highest amount position papers uploaded by the participants. The most active participants on this issue were the representatives from the various business associations and the large industry groups. They submitted exhaustive and detailed proposals on the creation of an EU Third party limited liability protection system for security technologies.

The importance attributed by the responders to the issue of liability was translated distinctively in the rankings. Option 1, under which the EU would not get active, was rejected by 80% and approved by only 3% of the participants. Option three, which would leave the introduction of liability related legislation to the Member States, was also met only with an approval around 25%. The only option, which was rated as having a strong effect, was option number 2 with an approval of 73%, according to which the EU would introduce harmonised rules at EU level on Third Party Liability Limitations.

It should however be noted that 50% of the participating representatives from national administrations judged the second option to be inadequate. A civil rights group also expressed their doubts on liability, stating that the manufacturers of security technologies should not be freed from all responsibility.

Option 1: No change - under this option the EU would not get involved in Third Party Liability issues		
	Number of requested records	% Requested records(59)
Do not know	10	16.95%
1	44	74.58%
2	3	5.08%
3	1	1.69%
4	1	1.69%
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		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	3	5.08%
2	4	6.78%
3	8	13.56%
4	35	59.32%
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		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	9	15.25%
2	26	44.07%
3	10	16.95%
4	5	8.47%

4.3. Security of the citizen and the society

The problem definition, which stated that security products need to be privacy compliant from the development to the production (also known as "privacy by design"), was met with a large approval. Out of 59 responses 42 (71%) agreed with the problem definition and only 18% disagreed.

Do you agree with the problem definition, that security products need to be privacy compliant from the development to the production? (ranking from 1 do not agree at all to 4 agree very much)		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
1	6	10.17%
2	5	8.47%
3	15	25.42%
4	27	45.76%

4.3.1. How to ensure the integration of ethical/societal aspects in security technologies

The answers on the appropriate inclusion of societal aspects in security were spread to some extent over the various options. The only option which was clearly rejected was the first option, under which privacy by design would remain a voluntary effort for industry. This option was only approved by 17% of the participants and disapproved by 73%.

The differences between the other two options were relatively marginal, a slight preference for option 2 (voluntary system) was nevertheless expressed. Most representatives from large industry groups pleaded for a selected mandatory certification, which would only concern specific security technologies.

"We believe that a mandatory certification assessment (option 3) would only be reasonable in some areas, but not in all. Hence, a case-by-case decision, respecting the distinctiveness of the concerned products/processes, would be far more valuable. "

Three participants furthermore stated that the scope of the question was too restricted to privacy issues and that a broader approach would be more appropriate to ensure a successful inclusion of ethical aspects.

"Ethical/societal implications of security research are not limited to privacy issues. There are for example issues such as dual use goods, the militarisation of security, the ethics of end users (not exclusively in third countries) and reference to human rights and democratic governance in security policy. Beyond that, there is an issue about the privatisation of security with the easier access to cheaper but intrusive technology. Ethics must be an intrinsic part of programme and project design."

Option 1: No change - privacy by design would remain a voluntary effort for industry with no EU wide guidelines and/or requirements		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
1	35	59.32%
2	8	13.56%
3	1	1.69%
4	9	15.25%
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.		
	Number of requested records	% Requested records(59)
Do not know	4	6.78%
1	11	18.64%
2	15	25.42%
3	11	18.64%
4	18	30.51%
Option 3: In addition to option 2 - the certification certification/conformity assessment would be mandatory		
	Number of requested records	% Requested records(59)
Do not know	10	16.95%
1	18	30.51%
2	12	20.34%
3	5	8.47%
4	14	23.73%

4.3.2. Certification procedures

A majority (66%) of the respondents agreed on the usefulness of a merger between a possible ethical certification procedure and a general certification procedure, instead of having two separate certification procedures.

4.2 Certification procedures Do you believe it to be useful to merge a possible ethical certification procedure as detailed in point 4.1. with the certification procedures outlined in point 2.1, instead of having two separate certification procedures?		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
Very useful	16	27.12%
Somehow useful	23	38.98%
Not useful	12	20.34%

4.3.3. Privacy compliant technologies

The respondents were finally given the opportunity to express their preference on the possible inclusion of the "privacy by design" concept in FP security research as mandatory evaluation criteria.

This mandatory inclusion was rejected by a slight majority (52%) of the participants. The preferred option of 58% was the inclusion of the "privacy by design" concept through targeted research projects in the Security Theme of the FP was supported by 58%.

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.		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	14	23.73%
2	4	6.78%
3	9	15.25%
4	25	42.37%
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.		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
1	13	22.03%
2	20	33.90%
3	8	13.56%
4	12	20.34%