FP7 SECURITY ADVISORY GROUP

ANNUAL SUMMARY

June 2011 – June 2012

Issue 1.0

Andrew Sleigh
FP7 SecAG Rapporteur and Vice Chairman

June 2012

CONTENTS

1. INTRODUCTION

1.1. The Security Advisory Group (SecAG) consists of 21 independent experts drawn from security end-user organisations, academia and industry, plus 3 members from the European Commission (EC). All the members have broad experience in security matters and also have specific deep knowledge of particular operations, technologies or implementation. The SecAG was created in 2007 with an evolving membership.

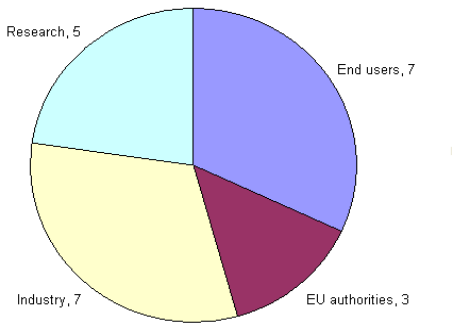
1.2. The SecAG provides expert, independent advice to the EC on the content of the annual work programme Call. These invite competitive submission of proposals for the Cooperative element of the Security Theme in the FP7 programme. The final version of the work programme is formulated by the EC and approved by the FP7 Security Theme Programme Committee representing the Member States and Associated Countries. The SecAG also supports the EC in organising workshops relevant to security research. The SecAG has no role in the assessment of project proposals, nor in the management of projects awarded funding.

1.3. During 2011/2012 the SecAG followed a similar approach as for previous years, forming working groups (interacting mainly by email) around the six primary mission areas to identify new topics, to review and refine topics submitted by Member States and other proposers, and lead discussions during the meetings. SecAG meetings bring the working group inputs together, offer revisions to topics to improved clarity and focus, and advise on priorities. This year benefitted from most topics proposed by Member States being submitted early in the autumn of 2011, enabling the SecAG to follow and constructively add to the priorities of the Programme Committee. The quality of material supporting submitted topics further improved for this round, enabling better understanding of the objectives and potential benefits of each topic during assembly of the programme.

1.4. As in previous years, many more topics were submitted than could be accommodated in a manageable work programme.

1.5. The membership of the advisory group is appointed by the EC, with members serving 2 year terms. The group's Chairman, Julio Martinez Meroño has a user background, who is also in attendance at Programme Committee meetings, and the Vice Chairman, Andrew Sleigh has a research industry background. The membership is profile is summarised in the chart below.

SEC AG Membership



2. THE SecAG PROCESS 2011-2012

2.1. The SecAG met four times during 2011/12. Minutes of these meetings are available of the Europa website, with the main activities at each meeting being:

28th October 2011. Reviewed the planning note that had been prepared by the EC and discussed topics received from Member States. The main part of the meeting debated the output from the six working groups. Each group had revised the introductory text for each mission area and developed a list of areas where new topics would be especially appropriate. This reflected the discussion held in the previous meeting in June 2011 where the outcome from the 2012 work programme was reviewed and recommendations for the 2013 work programme developed. Summaries were received on the workshops on *Security Industry Policy* and *Competitiveness Through Standardisation.*

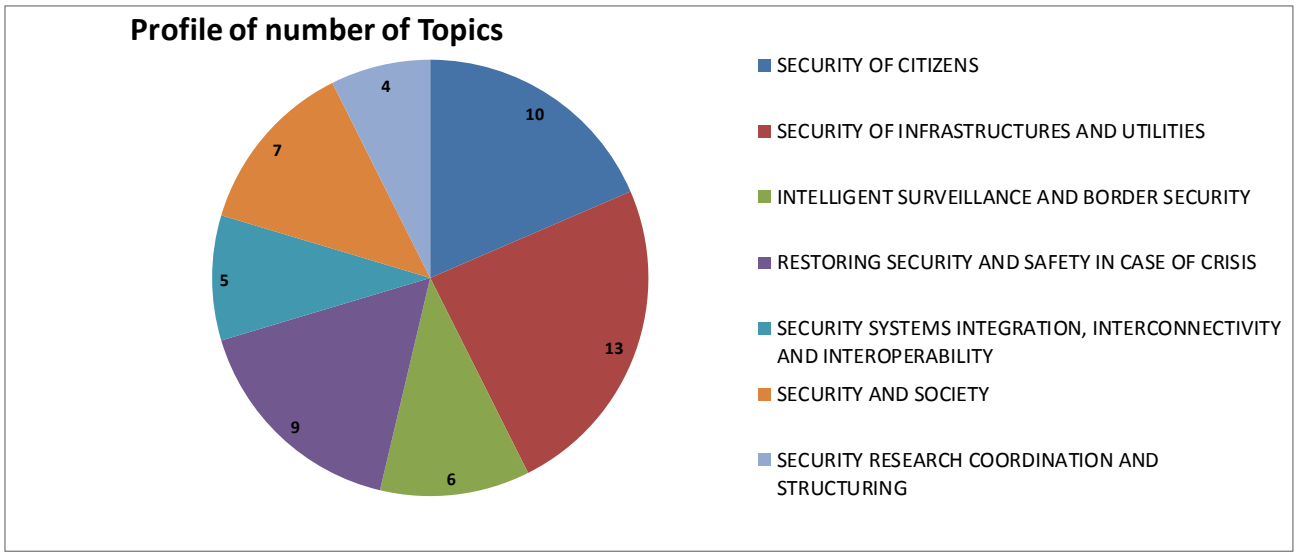
10th & 11th January 2012. The first day was devoted to workshops on each of the six primary mission areas. Each mission area had a 2 hour session (in two streams) where the strategy was reviewed and the portfolio of topics received was analysed. As a result a number of the topics were clarified, re-drafted or integrated in preparation for the 2nd day where priorities were discussed as a basis for the EC to take into account in formulating the draft work programme. A small number of topics were identified as needing additional input, and this was followed up after the meeting by additional material either from SecAG members or the originating proposers of the topics.

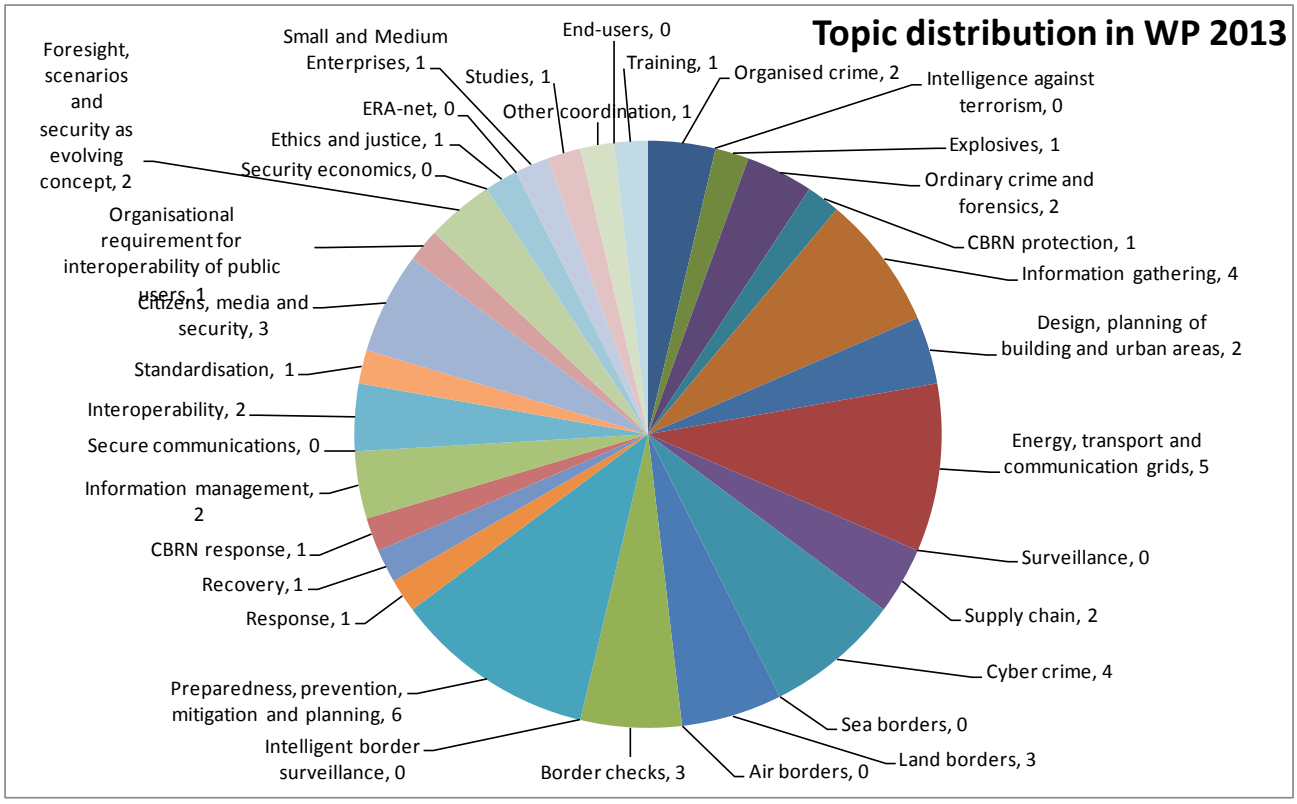
17th February 2012. This meeting focused on finalising the 2013 work programme, taking into account comments made by the Programme Committee. Attention was paid to the topic descriptions to ensure they were clear and deliverable, and areas of coverage between topics refined. Many specific re-drafting recommendations were contributed by members in the days after the meeting. An update on Horizon 2020 was given, and with a short discussion of the role of the SecAG during the remainder of 2012 before it is disbanded.

15th June. This was the final meeting of the SecAG and focused on assessing the achievements of the FP7 Security Theme so far. The meeting was conducted around a structured list of criteria of success that had been circulated with the agenda, and this discussion forms the basis of the considerations reported in this document.

3. WORK PROGRAMME 2013

3.1. The charts below give the breakdown of the number of topics against each mission area and mission sub-areas. It can be seen that there is a balanced coverage with some increased emphasis on Security of Citizens and Security of Infrastructures and Utilities.


Profile of number of Topics
10
13
6
9
5
7
4
SECURITY OF CITIZENS
SECURITY OF INFRASTRUCTURES AND UTILITIES
INTELLIGENT SURVEILLANCE AND BORDER SECURITY
RESTORING SECURITY AND SAFETY IN CASE OF CRISIS
SECURITY SYSTEMS INTEGRATION, INTERCONNECTIVITY AND INTEROPERABILITY
SECURITY AND SOCIETY
SECURITY RESEARCH COORDINATION AND STRUCTURING


Topic distribution in WP 2013
Foresight, scenarios and security as evolving concept, 2
Small and Medium Enterprises, 1
Studies, 1
End-users, 0
Training, 1
Organised crime, 2
Intelligence against terrorism, 0
ERA-net, 0
Other coordination, 1
Ethics and justice, 1
Security economics, 0
Explosives, 1
Ordinary crime and forensics, 2
Organisational requirement for interoperability of public users, 1
CBRN protection, 1
Information gathering, 4
Citizens, media and security, 3
Design, planning of building and urban areas, 2
Standardisation, 1
Interoperability, 2
Secure communications, 0
Energy, transport and communication grids, 5
Information management, 2
CBRN response, 1
Surveillance, 0
Recovery, 1
Supply chain, 2
Response, 1
Cyber crime, 4
Preparedness, prevention, mitigation and planning, 6
Sea borders, 0
Intelligent border surveillance, 0
Land borders, 3
Border checks, 3
Air borders, 0

3.2. Last year's Annual Summary of the SecAG activity noted a number of specific areas where improvement in the programme would be beneficial:

- Members felt a need for greater visibility of the results of projects underway from earlier rounds, especially to appreciate whether follow-on topics should be introduced, or whether more research was needed in areas making limited progress. ***This is still seen as an issue, as is discussed in Section 4.***
- Several Sec AG members expressed concern about transition of research to generate impact upon security outcomes, and upon the extent to which topics will enhance the competitiveness of industry. There remains a desire to ensure that the direct needs of users and enhancing competitiveness have close alignment wherever possible. It was felt that the potential user demand and routes to market could have been made more explicit in the topic descriptions, with this lack of transparency of opportunity risking discouraging industry investment. ***We believe good progress has been made in WP2013.***
- During the year the SecAG discussed at some length how to increase the engagement of end-users in the research projects. This is seen as an important way to focus research and accelerate its uptake. It is recognised that encouraging user engagement in research will always be a challenge, and several SecAG members would like to see more attention paid to this in future programmes. ***This remains a key concern as discussed further in Section 4.***
- The trend towards topics that integrate technological and societal research seen in the previous Work Programmes has continued and several SecAG members felt should receive further emphasis in the future. ***WP2013 had addressed this issue well.***

3.3. Members felt that the process for developing the 2013 Work Programme was an improvement over previous years, continuing the evolution that has taken place throughout the Security Theme, which was new to FP7. This year the process benefitted from:

- Earlier submission of candidate topics enabling the SecAG to assess and offer amendments to programme topics during its workshop meetings during the autumn 2011 and January 2012 meetings before compilation of the draft programme takes place in February.
- Priorities were established by the Programme Committee at the start of the work programme formulation in October, earlier than had occurred in previous years and so able to feed into the SecAG deliberations.
- Stronger supporting information was provided from topic proposers. Fuller details have been provided on potential benefits, the criteria for success, and benefits to end-users and to competitiveness of industry which has enabled a clearer programme to be produced with a stronger basis for prioritising the selection of topics.
- The 2-day workshop meeting held in January added significant value, enabling SecAG members to debate the topics and overall programme shape, offering advice on how to configure objectives to generate maximum value. This has led to topics being better defined, which should help bidding consortia to be efficient in designing their proposals.
- It was felt that the complementary expertise across SecAG membership, which balances users, academics and industry, was particularly effective and creative in

identifying where topics needed strengthening in the definition of objectives or in linking user needs to technological opportunities.

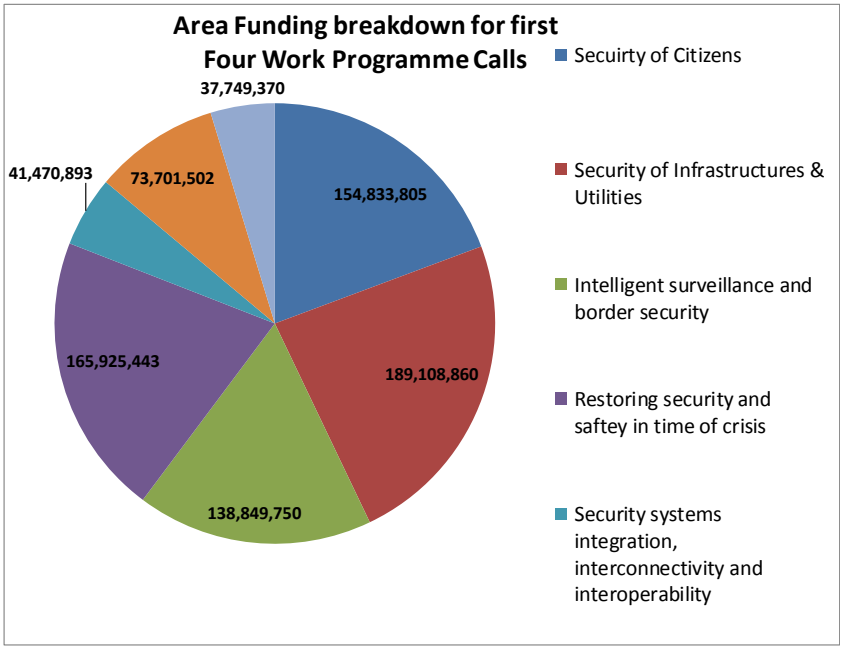
3.4. The societal dimension is now a central part of the programme. The initial Calls for the Security Theme had limited coverage of societal aspects, and they tended not to be integrated with technological research. The 2013 work programme has societal aspects as a core component and many topics bridge technological and societal dimensions. This is seen as a major achievement.

3.5. Many topics were submitted with a good analysis of the need, and how successful output from the research might be deployed through commercial offerings or process change in user organisations. This is important for Capability topics and is essential for Integration topics and Demonstrators. We believe the WP2013 gives clearer articulation of how potential benefits would be realised and how participating industry partners would achieve a return on their investment.

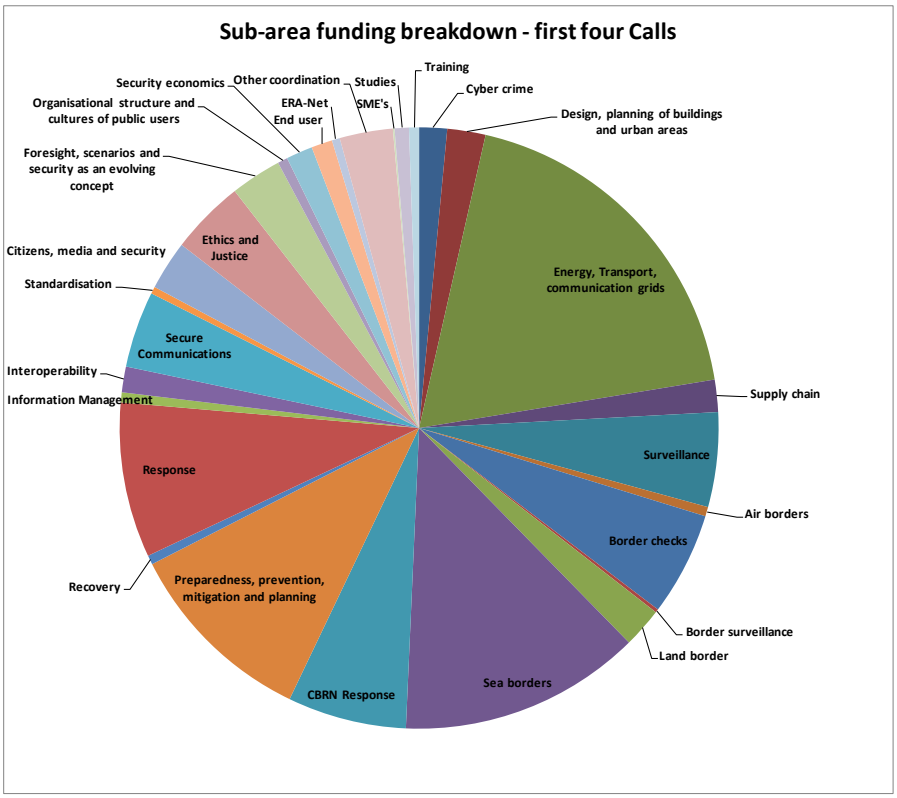
4. REFLECTIONS ON FIRST FOUR WORK PROGRAMME CALLS

4.1. Analysis of funding for first 4 WP Calls

The charts indicate the balance of funding for projects for the first four Calls in the FP7 Security Theme. This shows an even balance between the first four mission areas, a smaller but significant funding for Security and Society, with Interoperability and Research Coordination receiving the lowest levels.



The profile across sub-areas shows greater variation, with Energy & Transport, Sea Borders, Preparedness and Mitigation and Response being the largest.



4.2. COMMENTS ON FIRST FOUR CALLS

Members of the SecAG discussed their reflections on the first four Work Programme Calls at their meeting on 15th June 2012, which are captured under the following headings.

a) ACHIEVEMENTS

The Security Theme was new to FP7, so relatively few projects have completed their programmes in full at this time. Nevertheless, a number of projects have produced commercially successful solutions (e.g. INFRA) or hardware that is being sold (e.g. SECTRONIC). Industry members of the SecAG reported that their companies are exploiting research progress into products from projects still underway. Likewise research activities are contributing to standards formulation and to the development of processes and policies in user organisations. The programme has established strong collaborative relationships between partners that are delivering benefits to consortium partners in the areas of the research but also forging linkages that are applying to other opportunities. The forging of relationships between end-users and industry/academia are an especially valuable outcome. FP7 projects have been instrumental in exposing end-users to future thinking and helped researchers understand the issues and operational priorities of security organisations. It is notable how much the programme has evolved, both in terms of the way the work programmes have been produced and the introduction of additional criteria relating to security and ethical considerations.

Workshops held in association with the FP7 Security programme have proved an effective way to get the different groups of stakeholders to interact creatively and has provided an avenue for sharing successes.

b) IMPACT AND ACCESS TO PROJECT RESULTS

There is a need to improve access to output from projects. Currently there is no searchable database that brings together the achievements and exploitable outputs from projects. Project websites can be removed after a project completes. While the primary exploitation route will generally be within the consortium partners, many wider opportunities may be missed if parties external to the project are not aware of successes. This is especially true of Coordinated Study Actions and Capability Projects where the outputs will normally be developed subsequently as part of a larger endeavour to deliver value. The SecAG felt that the EC should put much greater emphasis on enabling access to results, and be imaginative in finding ways to do this efficiently. This might include commissioning organisations external to the EC to aggregate and archive project data.

There is a need to be proactive in communicating the benefits from research, especially to users. This could take the form of case studies, scenario descriptions, pilot implementations, talking to user communities. We need to prepare them to be more fully involved.

c) ADDRESSING THE AIMS OF ESRAB

The ESRAB report formed the basis of the Security Theme in FP7, setting out the principal mission areas and identifying top-down priorities. ESRIF added to the context during the programme. The SecAG consider that all the key areas identified by ESRAB have been addressed by projects with a high probability that desired outcomes will be achieved as projects complete their lifecycles. There is also good coverage of the more detailed needs and opportunities set out by ESRIF.

d) REPRESENTATION OF INTEREST GROUPS

Participation in projects includes large companies, SMEs, universities and research institutes, user and policy organisations. Analysis of participants shows the Security Theme has the highest proportion of SME participants, with SME involvement invariably as a partner under a larger project led by a big company, reflecting the difficulty of managing the overhead of leading a project. This should improve in the most recent work programmes, which have a dedicated topic for SMEs. End User participation has been significant, but could have been stronger and deeper as discussed below and in Appendix 1. The dominant university engagement has been from technology disciplines, engagement from social sciences and legal departments has been lower, possible because they lack awareness of the Framework Programme. There is a gap in representation of civil associations & NGOs which should be considered for future programmes, and there is also consideration of how ordinary citizens might be engaged, especially in addressing 'privacy by design', and how techniques such as ‘crowd sourcing’ are applied to meeting Security needs.

e) INVOLVEMENT OF END USERS

End user participation is a crucial aspect of the FP7 Security Theme, and has grown progressively during the course of the programme. A particularly good example is the strong engagement of end-users in the Border Surveillance mission area, where close engagement has helped users think about the future, exposing them to ideas about how their

activities could evolve. This is a significant gain. In other instances user organisations have changed their internal organisation as a result of involvement in FP7, for example by creating specific roles to link research projects to internal activity. In the best cases, end-users are involved in the project formulation at the outset, and have a direct role in the project execution. Direct experiences of users on the SecAG show that benefit is maximised if users play an intimate role in the definition of a project plan and work as an integral part of the project team. However, more often end-users have been engaged late in the project plan development and have had limited interaction during a project's execution. This greatly diminishes the value end-users contribute to the research and also limits the benefit they derive from being involved.

User organisations face specific problems in participating in FP7 projects. It can be difficult for government organisations to meet EC requirements for a defined legal entity. Generally they do not use time sheets or have other ways to attribute direct costs to a project code. It can be difficult for funding to be articulated to the unit participating in the programme, and so involvement can appear as an additional overhead to local management, even if funding is received by the organisation. This discourages government partners taking a direct role in consortia.

One recommendation is for user organisations to identify an 'innovation champion' to lead on engagement in projects. This could be someone in mid-career with senior potential who would have the freedom to be part of the project team but would also be able to act as a conduit to the wider organisation, both to provide relevant input to the project and stimulate internal innovative thinking about the future. Such an individual would offer direction and perspective, promulgate successes and results, and be able to sell the benefits with the (often hierarchical) organisation.

Organisations that have participated deeply in a research programme can as a result enhance their processes to sustain an innovative outlook, once established this can create momentum with long term impact that goes beyond the scope of an individual project. H2020 should look at these and other ideas to recognise the special position of users, noting that this is an issue that applies especially strongly to the Security Theme, other areas being primarily driven by commercial markets.

f) EXPLORING NEW FRONTIERS

Many topics offered scope for novel research pushing the frontiers of technology. However, most projects have proposed relatively incremental activity, with few examples of "breakthrough" or high risk, high payoff research being offered. This may be influenced by a perception that diverse and large consortia are necessary to be awarded funding, a constraint that is not helpful to 'blue-skies' projects. Consideration should be given to topics and funding models that encourage a balanced response of highly innovative projects

g) LINKAGE TO NATIONAL RESEARCH AND FEDERATION OF EFFORTS ACROSS EUROPE

Linkage to national research activity faces a number of obstacles in the Security field because research activities are fragmented across many national organisations, often involving classified material, and tend to be focused on short term applied research that does not match the longer project timescales typical of the Framework Programme. Enabling activities such as ERA-Net play a part, but linkages across the EU and associate nations are

largely informal. This means the cross-nation relationships formed by project consortia offer a particularly important benefit as they are seen to provide an effective way to bond communities together. It is difficult, if not impossible, to track the impact of this networking, but the SecAG believes the benefit to be substantial. In addition, the annual security research conferences and targeted workshops that have been organised in association with the FP7 Security programme have provided opportunities for exchange of ideas and opportunities across the European security communities.

h) STRATEGIC ALIGNMENT OF PROGRAMME AND 'INDUSTRIAL POLICY'.

SecAG members made several points on how applied research in the security area should be targeted. There is a balance to be struck between a top-down approach that aligns the R&D to identified needs and future procurement plans, and a bottom up approach where capabilities with potential benefit are pursued with the expectation of stimulating future buying. Within some nations (the US for example), applied research is tightly linked to future acquisition plans which means industry investments and user engagement has a clear rationale. EU Framework Programmes have traditionally assumed that by offering a grant matched by industry, the project consortia will optimise the exploitation of the research. This may not be enough where deployment of innovation requires integration across capabilities (which may involve 'hard' technology, user behaviour, policy or regulatory aspects), and where market opportunities are uncertain and dependent upon government priorities. There was strong support amongst the SecAG members for a more top-down approach with greater transparency of opportunities for deployment of research, while recognising that a bottom-up element should always be retained at, say, 30% of the overall funding. H2020 has a greater emphasis on 'innovation' and so this aspect will have increased relevance in that future programme. Instruments such as precompetitive procurement, where member states and EU institutions join together to align research or demonstration activity to planned needs of user organisations, should play a significant role in H2020.

i) TIME AND COST OF BIDDING PROPOSALS.

The time from an original idea to delivering an output is at least 5 years. The cost of preparing a bid can typically be 10% of the project cost. We should find ways of doing things faster and leaner. Approaches include increased standardisation of funding models contracting terms and conditions, defining a range of optional collaboration agreements that consortia can use without negotiation, having a responsive fast-track route for smaller, innovative projects that can rapidly prove a concept, or problem-driven projects that have potential to offer near term solutions.

j) PROCESS FOR FORMULATION OF TOPICS.

Topics are submitted by Member States, by EU organisations, by industry bodies and by SecAG members, with The EC assembling a programme for endorsement by the Programme Committee. The initial drafting of topics is often incomplete, requiring clarification. For example, user generated topics may be weak or over specific on technological approach, or not address potential benefit to industry. Industry generated topics may not capture user need or benefits accurately. To generate effective proposals, topics must be clear about the intended objectives, not over-constrain the solution, and help participants assess the downstream opportunities to get a return in their investment. This is an expert task which

the EC officials undertake, but the input from external expertise on the SecAG has been a major contributor to this process. It is important that access to external expertise is part of the process, and may become more important in H2020 with its integrated view across research and innovation. There would also be benefit in a strategic forum between the Programme Committee and other stakeholders early in the annual work programme formulation, where user needs and technological opportunities can be exposed and priorities discussed.

The SecAG would also support consideration of 'Public Private Partnership' models for formulating programme action, for example drawing upon features of models such as JTI or other targeted programme management arrangements whereby users and suppliers can develop solutions in a responsive and needs-driven context.

5. CONCLUSION

The Security Theme was introduced into the Framework Programme for FP7 and has developed from small the first work programme Call defined by the Group of Personalities in 2007, through 6 further Calls since the SecAG was formed. The structure of 7 Missions established by the ESRAB report has proved an effective framework for developing topics, supported by the 'tree' of sub-missions that were introduced for the early Calls and slightly updated for later Calls. A significant issue throughout the programme has been the need to select a maximum of ~50 topics for each work programme from 200+ submitted each year. This has required careful consideration. Many important topics were submitted in a relatively high-level form and needed clarification and expansion before being included in the work programme. SecAG meetings have been conducted to maximise the creative synergy between industry, academic and user backgrounds. The SecAG members feel they have been able to contribute important expertise to the shaping and prioritisation of topics, supporting the Commission in interpreting the intentions of the Programme Committee representing the priorities of the Member States.

APPENDIX 1 Enhancing End-User Participation in FP7 Security Theme
Chaim Rafalowski, with contributions from other SecAG members

The FP7 Security theme has as one of its objectives the participation of end users in the programme. Through the 5 years of the program, a sustained positive evolution can be seen. As Horizon 2020 is being discussed, some reflection is needed.

1. Who are the "end users" for the security theme? 3 main types of end users can be identified:

a) Institutional end users – organisations that are involved in "preparing and responding to an event and recovering from it". It is important to point out that this includes NGO's and organisations that do not depend directly on their respective government. The issues related to these end users will be elaborated further in this document.

b) Industry System Providers, acting in the "demand" side of the products, e.g. aviation, security companies, logistics etc. These end users have a clear economic interest in the results and in the commercialization of the result of the research projects. It is considered that we could do better involving this part of the industry in future programs, and their perspectives should be better understood. In addition to that, there are industries that are not considered as a "regular" costumer to the "security" theme, but should be brought in, such as the pharmaceutical, insurance, media.

c) The general public. This is perhaps the biggest challenge for the program. The general public usually does not have "official representatives" and is not organized in a way that they can be reached easily. The issue of representation of the public with its diverse ideas is essential to ensure effective results. Those usually involved in security research are not familiar with "marketing" that have the tools to better involve the public. It would be advisable, to conduct a research activity to discuss outreaching techniques and better involvement on "common citizens" in research projects.

2. **Bureaucratic issues:** For institutional end users the following are major obstacles to the participation in FP7 projects:

a. Participating involves more work but often no more staff unless participating as a full member of a project consortium. For most of the organizations, having a project means more work for the same staff. In over stretched organizations (as most operating units are), this is a major deterrent to participating in a project.

b. EC requirements: fulfilment of EC financial and administrative requirements is very difficult since the administrative systems are not adjusted, e.g. having a separated bank account for the project, identifying the specific work time dedicated to the project.

c. The need to spend money on the project: participants have to invest considerable amount of time and money during the bidding stage of a project e.g. traveling for meetings. Public sector organisations rarely have a budget for this kind of 'business development'. This budget does not exist for public organizations. This results in not participating in the actual design of a project where users can probably have maximum beneficial input. This is a severe issue for the coordinator of a project, who needs to attend several meetings with EC officers before the project starts, and will have to do work after the project is over (distribution of 2 final payments). It means end-users will very rarely be able to lead a consortium. .

3. **IPR issues:** End users will contribute knowledge to the project that will enable or form part of the IPR. This can be seen to be unfair to users who have no way to create value from the project foreground, unlike industry and universities. This needs to be set against the reduced procurement

risk to eventual deployment of a successful research output, and the deeper awareness gained as an informed customer.

4. **Lack of knowledge about the programme:** Senior managers in the user organizations may not be aware of FP7 and its potential benefits to their organization. More work should be focused in this area, communicating the existence and benefits to senior officers and influencers in user organisations. A good example is the city of Madrid, where the Director of safety and security of the city, Alfonso Gimenez del Alamo, is aware of the program, and facilitates the participation of the city's organizations. This is essential to the successes of the program that not only R&D units of the end users are involved, but also the operational people with the field experience ("boots on the ground). Dedicated workshops to introduce top managers with FP7 results and Horizon 2020 would be essential to promote this.

5. Lack of knowledge among end users: Industrial R&D and researchers speak a language that is not familiar to many end users and uses tools that end users are not used to (mainly a "project management" language). This, on top of language barriers, is an important deterring factor in the participation of "real end users" in projects ("we don't have the persons with the right profile"). This also creates frustration among the industry / researchers ("end users don't know what they want"). As part of the project, a training program for end users on "innovation", "project management" should be offered. This will streamline the work and considered as an added value to the participation by the end users.

6. Terminology: Security is perceived as a topic dealt with by military, police, intelligence agencies and security companies. The theme is about "civil security and safety". Due to the name, organizations that should be interested in relevant topics (e.g. Red Cross societies), ignore it. Better wording for the topic would be helpful.

7. **Research or RD&D?** At the moment, the "quality of S&T" in the proposal is the "heaviest" part of the evaluation. This may bias projects towards an academic approach, an emphasis that that can be rejected by end users. Academic research is evaluated by the "validity" of the results (e.g. P values) and characterized usually by a long work time. When faced with a pressing issue, end users expect a usable result within a short period of time, even if the result at the moment is limited. In addition, there should be scope for projects that are focused on short term *innovation*, even where the research element may be small.

8. Real Participation of End Users: Ideally, end-users should be involved in project proposals from the start, and indeed might take a leading position. However, partly because of FP7 financing rules, end-users may only become involved late in a proposal generation and have limited direct engagement in the execution of a project. Some project involve users through an "advisory board", but this is not seen as a satisfactory alternative to full participation, as they tend to have limited power to influence the end results of the project.

9. **Networking**: networking is a key element in the institutional end user's world while accepting new products / methodologies. Projects that provide this opportunity for networking are considered with higher value by end users (especially in the current economic environment). Project coordinators should be encouraged to reserve funding to enable the participation of end users in the

project's activities. The EC should encourage whenever possible joint events (of different projects) to maximize the use of resources.

10. **Technology versus human factors**: Most of FP7 projects where technological (and even high technology) and rightly so. In a world with dramatically shrinking security budgets, and declining manpower, there is a need to shift a bit the focus.

a. Understand that new technology to be integrated will be evaluated under the criteria – "does it change the roles of the game", and only those who actually change the game will be accepted (change the game for example = much cheaper, with significantly less personnel, much safer, something new and essential).

b. Give a greater emphasis on the personnel involved (staff and volunteers); their needs, learning style, reactions under stress, decision making styles, emotional well-being, and create projects that will support them.

11. Stimulating an innovative culture in user organisations. If end users are to become engaged in research and innovation projects, it is importance they have and innovative culture themselves, with internal procedures that support adoption of new ideas. This embraces a wide set of aspects from organisational governance to how managers are incentivised. You cannot 'bolt on' innovative improvement onto an end user organisation, it needs already to be part of the makeup. One answer is for researchers to seek out user organisations that have developed an innovative leaning, and focus engagement on them, then use that relationship to lever in others. This requires detailed knowledge of organisations and the people in them (the outlook of their leaders is very significant). Few research teams or even companies have the resources or networking ability to deduce this. A potentially important idea for engaging innovative end-users is the use of ‘living labs’ where new ideas for products and processes can be demonstrated and tested in a realistic context with real end-users taking part. In other domains (eg consumer electronics, defence) this approach has been used with success and proves an effective way to clarify needs, stimulate uptake of ideas that reduce costs or enhance capability, and reduce risk for procuring organisations. This type of facility should be considered as part of the H2020 programme, either as a central facility, or by providing a federating management umbrella for distributed capabilities that might be with user or industry organisations.

12. Roadmaps and forming an “Innovation Architecture”. Whilst some research topics aim at complete solutions, many are directed at developing intermediate capabilities (technology, processes or both) that will create the building blocks from which various companies can configure solutions to meet specific market-driven needs. Experience in several technological fields suggests this is a very important avenue for taking research to market. It is helped by having roadmaps that link end user aspirations to the component technology options. Such roadmaps can be especially helpful in focusing longer term research on mid-term results that can be taken to market earlier than the final goal. There is a gap in the security economy of who can do this, largely because of the inhomogeneous nature of the market. An important step would be for key organisations to formally take on the role of owning the 'innovation architecture' for a domain (this would include technology roadmaps, lists of important problems/aspirations, etc.). Frontex and Europol would be candidates in their part of the security space.

APPENDIX 2 – SUMMARY OF FP7 SECURITY RESEARCH WORKSHOPS

List of Workshops 2011-2012:

Workshop on Security Industrial Policy

In Brussels: 18 October 2011

- Participants: ~100.
- The aim of the workshop was to confirm and validate the results of the public consultation held from March to May 2011. The Workshop was divided in four thematic sessions: Certification and standardisation, Pre Operational Validation/Pre Commercial Procurement, Civ/Mil Synergies and Third party Limited Liability.
- Weblink: http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5316&lang=en&title=Workshop%2Don%2DSecurity%2DIndustrial%2DPolicy%2D

The DG ENTR contact person for this domain is Mr. Christoph Castex (Christoph.CASTEX@ext.ec.europa.eu)

Workshop on crisis and disaster management

In Brussels: 25 January 2012

- Participants: ~130.
- Objective: Identify priorities and technical recommendations for a demonstration programme (Phase II) which is expected in the next call (SEC-2013-1).
- Four panel sessions were held on the following topics:
  - EU Policy Context in the Area of Crisis and Disaster Management.
  - R&D Approaches and Solutions of Relevance for the Demonstration Programme.
  - End User Involvement.
  - Cross-border Crisis Management Experiences as Suitable or Potential Examples for Demonstrations
- Weblink: http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5624&lang=en&title=Toward%2Da%2DDemonstration%2DProgramme%2Don%2DCrisis%2Dand%2DDisaster%2DManagement

The DG ENTR contact person for this domain is Mr. Tristan Simonart: (Tristan.SIMONART@ec.europa.eu)

Workshop on Supply chain security

In Brussels: 31 January 2012

- Participants: ~220
- The objective of the workshop was to discuss the roadmap and priorities that should be taken into consideration for a future FP7 European R&D demonstration programme on "Logistic and Supply Chain Security".
- The 31 January workshop here was split into plenary discussions and theme-specific sessions. During the plenary debate end-users and policymakers from different public sectors elaborated their needs regarding supply chains.
- Weblink: http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5739&lang=en&tpa_id=168

The DG ENTR contact person for the supply chain security workshop is Mr. Paolo Salieri (Paolo.Salieri@ec.europa.eu).