Framework Service Contract for the Procurement of Studies and other Supporting Services on Commission Impact Assessments and Evaluations

Ex-post Evaluation of the Preparatory Action on Security Research (PASR)

Interim Evaluation of FP7 Security Research

Final report

January 2011

Centre for Strategy & Evaluation Services

P O Box 159
Sevenoaks
Kent TN14 5WT
United Kingdom
www.cses.co.uk
# Contents

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>1</td>
</tr>
<tr>
<td>1.3</td>
<td>1</td>
</tr>
<tr>
<td>1.4</td>
<td>4</td>
</tr>
<tr>
<td>1.5</td>
<td>8</td>
</tr>
<tr>
<td>2.</td>
<td>9</td>
</tr>
<tr>
<td>2.1</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>22</td>
</tr>
<tr>
<td>2.5</td>
<td>23</td>
</tr>
<tr>
<td>3.</td>
<td>27</td>
</tr>
<tr>
<td>3.1</td>
<td>27</td>
</tr>
<tr>
<td>3.2</td>
<td>32</td>
</tr>
<tr>
<td>3.3</td>
<td>34</td>
</tr>
<tr>
<td>3.4</td>
<td>41</td>
</tr>
<tr>
<td>3.5</td>
<td>47</td>
</tr>
<tr>
<td>3.6</td>
<td>54</td>
</tr>
<tr>
<td>3.7</td>
<td>58</td>
</tr>
<tr>
<td>4.</td>
<td>61</td>
</tr>
<tr>
<td>Part 1</td>
<td>61</td>
</tr>
<tr>
<td>4.1</td>
<td>61</td>
</tr>
<tr>
<td>4.2</td>
<td>62</td>
</tr>
<tr>
<td>Part 2</td>
<td>63</td>
</tr>
<tr>
<td>4.3</td>
<td>63</td>
</tr>
<tr>
<td>4.4</td>
<td>65</td>
</tr>
<tr>
<td>4.5</td>
<td>78</td>
</tr>
<tr>
<td>5.</td>
<td>80</td>
</tr>
<tr>
<td>5.1</td>
<td>80</td>
</tr>
<tr>
<td>5.2</td>
<td>82</td>
</tr>
<tr>
<td>5.3</td>
<td>90</td>
</tr>
<tr>
<td>5.4</td>
<td>95</td>
</tr>
<tr>
<td>6.</td>
<td>97</td>
</tr>
<tr>
<td>6.1</td>
<td>97</td>
</tr>
<tr>
<td>6.2</td>
<td>100</td>
</tr>
<tr>
<td>6.3</td>
<td>107</td>
</tr>
<tr>
<td>A.</td>
<td>110</td>
</tr>
<tr>
<td>B.</td>
<td>117</td>
</tr>
</tbody>
</table>

**APPENDICES (BOUND SEPARATELY)**

<table>
<thead>
<tr>
<th>A.</th>
<th>List of interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.</td>
<td>Bibliography</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>C. Interview checklists</td>
<td>120</td>
</tr>
<tr>
<td>D. Sample of EU Security projects</td>
<td>130</td>
</tr>
<tr>
<td>E. Indicators paper</td>
<td>134</td>
</tr>
<tr>
<td>F. Full survey results</td>
<td>135</td>
</tr>
<tr>
<td>G. National security research programmes</td>
<td>158</td>
</tr>
<tr>
<td>H. Case studies (thematic standalone cases)</td>
<td>172</td>
</tr>
<tr>
<td>I. Standardisation</td>
<td>173</td>
</tr>
<tr>
<td>J. Future perspectives</td>
<td>176</td>
</tr>
</tbody>
</table>
List of Acronyms and Glossary

CSA   Coordination and Support Action
CBRNE Chemical, Biological, Radiological, Nuclear and Explosives
CP    Capability project
CIP   Competitiveness and Innovation Programme
CSA   Community and Support Action
DG ENTR European Commission, Directorate General for Enterprise & Industry
DP    Demonstrator project
EC    European Commission
EIP   Entrepreneurship and Innovation Programme
EIS   European Innovation Scoreboard
ERA   European Research Area
ESR   Evaluation Summary Report
ESRP  European Security Research Programme
ESRIF European Security Research and Innovation Forum
FP6   6th Framework Programme for Research and Technological Development (2002-06)
FP7   7th Framework Programme for Research and Technological Development (2007-13)
GA    Grant Agreement
GMES  Global Monitoring for Environment and Security
GoP   Group of Personalities
HEI   Higher Education Institution
IP    Integrated Project
IPEG  Innovation Policy Expert Group
IPR   Intellectual Property Rights
IRC   Innovation Relay Centre
IRE   Innovating Regions in Europe
NoE   Network of Excellence
PO    Project Officer
REA   Research Executive Agency
RIS   Regional Innovation Strategy
RIS-NAC Regional Innovation Strategies in Newly Associated Countries
SEC AG Security Advisory Group (20 experts providing independent advice to the Commission
SEC PC Security Programme Committee
SME   Small and medium enterprise
TtG   Time to Grant
Definition of key terms:

A number of key terms are used in the report relating to the various stakeholders that are involved in FP7 Security. A short definition of these is now provided:

**Beneficiaries** - organisations that have participated as part of project consortia in Security Research projects funded through FP7 Theme 10 Security (2007-2013) and PASR (2004-2006).

**End-users** - organisations in the public sector that could potentially make use of the results of FP7 Security Research. This term is sometimes shortened in the report to ‘users’. Examples of the types of users concerned include the emergency services, law enforcement agencies, intelligence agencies, public bodies responsible for public health and safety and some types of NGOs (e.g. those in the field of Crisis Management and Emergency Response). Other types of users include policy makers at EU, national and regional levels.

Indirectly, industry, academia and research institutes should also benefit from the results of Security Research.

The term ‘**prospective end-user**’ is used to describe public sector organisations that have not yet participated in projects, but could potentially do so in future, or may not wish to participate directly, but have a potential interest in taking up or further developing research results.
1. Introduction, evaluation aims and methodology

1.1 Introduction

This document contains the final report in respect of the Ex-post Evaluation of the Preparatory Action for Security Research (PASR) and the Interim Evaluation of FP7 Security Research. The independent evaluations were carried out by the Centre for Strategy & Evaluation Services (CSES) for DG Enterprise and Industry (‘DG ENTR’) between January and November 2010.

1.2 Evaluation aims and scope

The overall aims of this assignment are, in summary, to:

Table 1.1: Evaluation aims

- Evaluate the effectiveness and quality of research activities managed by DG Enterprise and Industry in respect of EU Security Research (PASR in the 2004-06 period and FP7 Security Research to date in the 2007-13 period) and EU Space Research (FP7 Space Theme 9)
- Evaluate the efficiency and effectiveness of programme management and implementation arrangements
- Assess ex-post progress towards the achievement of the objectives set in respect of the PASR Preparatory Action and progress at the mid-term in the programme lifecycle towards the objectives of FP7 Security and FP7 Space
- Gather an evidence base on the utility and effectiveness of EU funded research in the fields of space and security so as to facilitate the Ex-post evaluation of FP7 Space and Security Research
- Make recommendations to strengthen the effectiveness of programme implementation in FP7 Space and Security respectively and help to facilitate the preparation of FP8

Article 21 of the Commission’s Implementing Rules requires interim and/or ex-post evaluation of all programmes and activities, including pilot projects and preparatory actions, exceeding 5 million EUR. In addition to meeting accountability and transparency requirements, the evaluation examines the impact, usefulness and quality of EU Security Research to date. This should help to improve the quality, effectiveness, utility and strengthen the impact of Security Research funding in the remainder of FP7 and input to the preparation of an eventual successor programme in FP8.

The Evaluation Steering Group was comprised of Commission officials from the Security Research Unit H3 “Security Research and Development" and representatives from the evaluation function within Unit A4 Planning and Management. Discussions have also been undertaken with the GMES Bureau (Unit H4), since funding for the development of pre-operational GMES services will support the aims of EU Security Research in some areas, notably crisis management and maritime security.

The time scope of the Interim evaluation of FP7 Security Research was the first two calls for proposals. However, the statistical analysis of programme expenditure to date includes the third calls for proposals so as to ensure a ‘real-time’ element to the evaluation. The timeframe of the Ex-post Evaluation of the Preparatory Action for Security Research (PASR) relates to projects funded under the 2004-2006 period, during which 3 annual calls were supported.

1.3 EU policy and legislative context - EU Security Research

1.3.1 EU policy context

The terrorist attacks of September 11th 2001 and more recent attacks in Europe, such as the London and Madrid bombings of mass transport networks underlined the need for greater coordination at EU level to ensure the security of EU citizens in the context of increasingly globalised security threats. The European Security Strategy ‘A secure Europe in a better world’ was adopted by the Council in
December 2003 identified a number of challenges to Europe’s internal and external security. These centre on the connected threats of terrorism, the proliferation of weapons of mass destruction, regional conflicts, failing states, and organised crime. The strategy also advocates ‘Better coordination between external action and Justice and Home Affairs policies is crucial in the fight both against terrorism and organised crime.’

The EU Security Strategy called for a more strategic approach to promoting EU security, with greater coherence, stronger capabilities and greater coordination and cooperation between relevant actors. A Group of Personalities (GoP) was set up in 2003 to identify key principles and guidelines for the establishment of a European Security Research Programme to support the aims of the EU’s foreign, security and defence policy.

In order to strengthen the coherence of EU Security, the 2004 GoP report called for: a) More effective coordination between national and European research activities (b) Systematic analysis of security-related capability needs, from civil security to defence (c) The full exploitation of synergies between defence, security and civil research (d) Specific legal conditions and funding instruments for security-related research at the European level, and (e) Institutional arrangements that are efficient and flexible enough to combine Member State and EU efforts and to involve other interested partners.  

The GoP noted the difference between the EU and US in expenditure on security research. ‘The Department of Homeland Security will have a budget of $1 billion in 2004 with a consequence that: “the EU is at risk of becoming more dependent and vulnerable in this essential area”’. The report stressed the need to maximise investment in security research by capitalising on dual use research potential between the civil and defence areas to promote resource pooling and the cross-fertilisation of research results. Various Commission Communications have since emphasised the importance of supporting security research at EU level to strengthen the security of European citizens, and to improve industrial competitiveness. The Commission Communication Security Research: The Next Steps (September 2004) emphasised that Europe needs to invest in fostering a “security culture” that harnesses the strengths of the security industry and research community to address challenges more effectively and to promote innovation.

The European Security Research Advisory Board (ESRAB) was established by the European Commission in April 2005 to define research and development needs for civil security on a medium-long term basis. The ESRAB final report was published in September 2006. ESRAB established a framework for structuring technology development, and defined core missions and cross-cutting missions. The defined core missions are border security, protection against terrorism and organised crime, critical infrastructure protection, and restoring security in crisis situations. The cross-cutting missions defined were: analysis, integration, connectivity and interoperability, developing new capabilities and technologies and demonstration programmes. These, together with the implementation of PASR shaped the formulation of the FP7 Security Research Programme.

CSES’ research found that 8 out of 27 EU Member States presently implement national civil security research programmes. Others may also fund defence research that has potential civil security crossover, but it is clear that FP7 fills a gap in funding provision for civil security research. A clear
Introduction, evaluation aims and methodology

Community Added Value is that prior to FP7 Security Research, there was an absence of transnational, collaborative research in this area.

In response to the evolution of security threats and challenges facing the EU (internal, external), there was growing political will at EU and Member State levels to invest in European security research in order to meet key challenges to the security of EU citizens.

The Programme Decision establishing FP7\(^6\) provides the sole legal base for the programme and the basis on which this evaluation of FP7 Security has been carried out. However, it is worth noting that security research is an area in which the EU policy and legislative context is evolving.

For example, there have been a number of relevant policy developments since FP7 SEC was adopted and these have links to the thematic areas being supported. Examples include the adoption of policy communications across different areas of the Commission: the EU programme for Critical Infrastructure Protection, the EU Counter-Terrorism Strategy, the EU CBRN Action Plan (2009), a Communication on security scanners in aviation security (2010) and a policy Communication on Reinforcing the Union’s Disaster Response Capacity (2008).

The Commission Communication, an EU Internal Security Strategy in Action: Five steps towards a more secure Europe \(^7\) (November 2010) provides an update of the 2003 European Security Strategy and proposes a programme of joint work for 2011-2014 between the Commission and Member States on internal security issues, such as combating and preventing serious and organised crime, terrorism and cybercrime, in strengthening the management of our external borders and in building resilience to natural and man-made disasters. The strategy sets out five strategic objectives and specific actions, such as disrupting international crime networks, preventing terrorism and radicalisation, and raising levels of security for citizens and businesses in cyberspace. FP7 SEC has potential to contribute in current and future calls through specific research topics. For example, under preventing terrorism, the protection of transport is a key action, and under the objective of strengthen security through border management, specific actions include improving interagency cooperation at national level.

Additionally, the EU2020 Strategy and recent industrial policy developments affect the overall strategic environment in which FP7 SEC is being implemented. For example, the 2010 Commission Communication on an Integrated Industrial Policy stresses the importance of achieving further progress on harmonisation and standardisation and of strengthening the competitiveness of the EU security industry which is characterised by fragmentation.

Appendix J ‘Future Perspectives’ summarises key policy and legal developments since FP7 Security was adopted. Some of these will have implications for the preparation of FP8 SEC.

1.3.2 EU legislative context

The FP7 Programme Decision derives its legal competence from a number of areas of the EC Treaty (Treaty of Nice). Some of the most important areas of legal competence in the Treaty (at the time the Programme Decision was adopted in 2006) from the perspective of Security Research are now highlighted. It should be noted that this overview describes the situation when the programme decision was adopted. Since this time, the Lisbon Treaty has been adopted, although the legal base for the programme cannot change until FP8.

Title V of the Treaty in the Area of Justice, Security and Liberty makes provision for the EU to work together with the Member States to strengthen security in respect of the EU’s external borders. It

\(^6\) DECISION No 1982/2006/EC of 18 December 2006 concerning the 7th RTD Framework Programme 2007-2013

\(^7\) COM(2010) 673 final, Brussels, 22.11.2010
Introduction, evaluation aims and methodology

states that the Union shall ‘constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States. The EU shall frame a common policy on asylum, immigration and external border control’.

Article 75 attests to the EU’s role regarding the prevention and combating of terrorism and related activities (with particular reference to blocking financial transactions). Article 77 also refers to the important coordination role played by the Union monitoring and ensuring the security of EU external borders. It relates to policies on border checks, asylum and immigration, including the carrying out of checks on persons and efficient monitoring of external border crossings. Article 83 relates to the EU’s role in combating crime including: illicit drug trafficking, people trafficking, organised crime, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

The legal framework has evolved since the FP7 Programme Decision was adopted in 2006. The adoption of the Lisbon Treaty raises interesting possibilities for the programme’s future development in the context of EU external actions in areas such as crisis management and humanitarian assistance. Given that this is an interim evaluation, the achievements of FP7 Security Research must be assessed solely on the basis of the FP7 Programme Decision. In Appendix J, the main legal developments since the programme was drawn up are summarised under the section on ‘future perspectives’.

1.4 Methodological approach

The work was structured over three phases. A summary of the methodology for the evaluation is provided on the following page:

Figure 1.1: Methodological overview

A representative sample of 15 EU countries was selected for the field work, and agreed with the European Commission in Phase 1. The main criteria for country selection were:

- Ensuring balanced geographic coverage between Member States;
- Achieving a focus on those countries that have been especially active in participating in PASR and FP7 Security Research;
- Ensuring that EU countries that have a significant share of the European Security Research
**Introduction, evaluation aims and methodology**

industry were included; and

- The need to include EU countries that have national security research programme for comparative purposes.

The final list of 15 countries agreed with the Commission was: Austria, Belgium, the Czech Republic, Denmark, France, Germany, Greece, Italy, Lithuania, the Netherlands, Poland, Romania, Spain, Sweden, and the UK. While not in the country selection, a user in Croatia was also interviewed.

The selection of projects supported through PASR and FP7 Security Research to be examined through the case study research was agreed between CSES and the Commission following discussion in Phase 1. The following selection criteria were applied in selecting the projects (see Appendix D).

**Table 1.2: Selection criteria for projects**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thematic coverage</td>
<td>the Commission determined in the specifications that thematic case studies would be undertaken in the areas of focusing on CBRN detection and prevention, Aviation Security, Maritime Security, Crisis management and emergency response and a horizontal case on SME participation in FP7 Security</td>
</tr>
<tr>
<td>Project size</td>
<td>balance between small, medium and large sized projects to reflect the full diversity of projects</td>
</tr>
<tr>
<td>Project type</td>
<td>balance between Collaborative Projects (CPs), Cooperation and support actions (CSAs) and Networks of excellence (NoEs)</td>
</tr>
<tr>
<td>Type of organisation fulfilling lead coordinator role</td>
<td>a balance between projects led by different types of beneficiaries, including universities, research institutions, industry and SMEs</td>
</tr>
<tr>
<td>Coverage of FP7 Security missions and cross-cutting themes</td>
<td>appropriate balance between the 4 missions and the 3 cross cutting themes (these are set out in section 2.1)</td>
</tr>
<tr>
<td>Geographic distribution of lead project coordinators</td>
<td>a balance between the countries selected.</td>
</tr>
<tr>
<td>Extent of involvement of end-user organisations</td>
<td>priority was given to projects that included the direct involvement of end-users. Projects that do not directly involve end-users have also been selected to allow for comparison</td>
</tr>
<tr>
<td>Diversity of users</td>
<td>a broad spectrum of public sector organizations and agencies are potential users of EU Security Research. Good coverage of the different types of users was ensured</td>
</tr>
</tbody>
</table>

In total, 25 projects were selected from PASR and 32 from FP7 SEC. The level of project coverage achieved to ensure that the sample was representative is set out in the following table:

**Table 1.3: Proportion of projects covered in sample**

<table>
<thead>
<tr>
<th></th>
<th>Projects selected</th>
<th>Projects total</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PASR</strong></td>
<td>25</td>
<td>39</td>
<td>64</td>
</tr>
<tr>
<td><strong>FP7 SEC</strong></td>
<td>32</td>
<td>53 (following first 2 sec calls)</td>
<td>60</td>
</tr>
<tr>
<td>Total</td>
<td>57</td>
<td>92</td>
<td>61</td>
</tr>
</tbody>
</table>

**Interview programme**

A central element of the methodology was carrying out an interview programme with stakeholders in the European Security Research Programme (ESRP). This included a focus on carrying out discussions

---

8 FP7 projects were categorized depending on the size of the EU contribution to total project cost. Small projects were defined as being projects of less than <1.5m euros, medium projects were between 1.5m and <3m euros, and large projects >3m euros

9 Examples of users include the emergency services, law enforcement agencies, public bodies responsible for public health and safety, and policy makers, a full typology is provided later in the report
with beneficiaries\textsuperscript{10} in both PASR and FP7 SEC and with users. In order to avoid bias in the sample towards those with a favourable viewpoint on the programme, the interviews were extended to include not only users involved directly in projects, but also prospective end-users.\textsuperscript{11} The breakdown of discussions undertaken through the interview programme compared is provided below:

### Table 1.4: Interview programme overview – Security Research evaluation

<table>
<thead>
<tr>
<th>Interview category</th>
<th>Interviews completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Commission and REA officials – programme management</td>
<td>11</td>
</tr>
<tr>
<td>Commission officials - officials with responsibility for different security policies e.g. counter-terrorism, CBRN, aviation</td>
<td>9</td>
</tr>
<tr>
<td>Relevant officials from other EU-level organisations (e.g. JRC, CEN/ CENELEC, EDA)</td>
<td>4</td>
</tr>
<tr>
<td>National contact points</td>
<td>6</td>
</tr>
<tr>
<td>National authorities and members of Programme Security Committee</td>
<td>10</td>
</tr>
<tr>
<td>Representatives from security industry associations</td>
<td>3</td>
</tr>
<tr>
<td>Representatives from EU committees and expert advisory groups, e.g. ESRIF, Security Advisory Group</td>
<td>4</td>
</tr>
<tr>
<td>Beneficiaries FP7 Sec and PASR (SMEs, industry, research institutes, universities)</td>
<td>46</td>
</tr>
<tr>
<td>End-users FP7 SEC and PASR and prospective users</td>
<td>43</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>136</strong></td>
</tr>
</tbody>
</table>

While the terms of reference specified a target of 70-100 interviews for the evaluation of EU Security Research, during Phase 1, CSES were asked by the European Commission to expand the interview programme to 130 discussions to strengthen the evaluation findings. This was agreed, with a particular emphasis on increasing the number of discussions with end-users, and expanding the scope of these interviews to include prospective end-users.

A stratified sample was drawn up in Phase 1 for the different categories of stakeholder involved in FP7 Security Research. With regard to the sample’s representativeness, approximately half of all PASR and half of all FP7 projects were selected for analysis. In the case of each project, an effort has been made (where possible) to interview both the lead coordinator and at least one partner organisation. While many discussions were undertaken on a face to face basis in 14 Member States, some interviews have also been carried out by phone. A full list of interviews is provided in Appendix A.

The focus was on carrying out discussions with beneficiaries and users in PASR and FP7 SEC. To ensure that views were representative of the wider security research community and to avoid bias, where possible, the views of prospective beneficiaries and users were also sought.

Discussions were carried out with Commission officials involved in programme management, and with REA officials involved in the evaluation and selection process and in project monitoring (Technical Officers, legal and financial officers). Additionally, CSES held discussions with a number of EU policy officials with responsibility across the Commission services for different policy areas that should benefit from research in particular areas, such as drugs, counter-terrorism/ CBRN, crisis management and aviation security. Wider stakeholders interviewed include a sample of National Contact Points and members of the Security Programme Committee and Security Advisory Group and

\textsuperscript{10} Beneficiaries are organisations that have participated in Security Research projects funded through FP7 Theme 10 Security (2007-2013) and PASR (2004-2006).

\textsuperscript{11} Prospective end-users include public and private organisations that have not participated directly in projects, but have a strong potential interest in taking up or further developing results.
participants in ESRIF. Some national and regional authorities were also interviewed, including those involved in managing national and regional Security Research Programmes.

More than 40 end-user organisations were interviewed and a further 58 end-users completed the survey of users. This included a combination of users involved in the programme and prospective users to ensure that a balance was achieved and to eliminate potential bias. The user community is made up of organisations ranging from first responders and emergency services through to police forces, border control and intelligence agencies. It is clearly difficult to quantify the size of the user community. However, through the interview programme and survey of users an effort has been made to ensure that a wide range of users were consulted as part of the evaluation research.

The discussions were carried out using structured interview checklists, tailored to the type of stakeholder concerned (Appendix C). CSES carried out two online surveys, the first survey was targeted at beneficiaries in project consortia in both PASR and FP7 SEC was carried out in June and July 2010. 72 responses were obtained. The survey sample and response rates are set out below:

**Table 1.5: Survey of beneficiaries**

<table>
<thead>
<tr>
<th>Beneficiary survey</th>
<th>Survey sample</th>
<th>No. responses</th>
<th>% response rate</th>
<th>No. of projects in response (FP7 SEC)</th>
<th>% of projects total (calls 2007, 2009)</th>
<th>No. of projects in response (PASR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beneficiaries</td>
<td>520</td>
<td>72</td>
<td>13.8</td>
<td>47</td>
<td>71.2</td>
<td>41</td>
</tr>
</tbody>
</table>

*Note: 72 responses, multiples responses were possible, some beneficiaries took part in more than 1 project*

The survey achieved 72 responses, some of who had been involved in more than one project. The survey was sent to beneficiaries in both PASR and FP7 SEC and several email reminders were sent to potential respondents. Although the response rate (13.8%) was low, the proportion of projects covered was quite high (71.2% for 2007, 2009). In some cases, consortia agreed between one another to submit a single survey response for the consortium, rather than separate responses from each organisation.

A survey of end-users that have participated in EU Security Research projects was carried out. This also targeted wider user organisations to ensure that a control group element was built into the sample. The survey was carried out between early October and November 2010. The response obtained is set out below:

**Table 1.6: Survey of end-users**

<table>
<thead>
<tr>
<th>User survey</th>
<th>Survey sample</th>
<th>No. responses</th>
<th>% response rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users in project consortia</td>
<td>85</td>
<td>44</td>
<td>51.8</td>
</tr>
<tr>
<td>Prospective users</td>
<td>65</td>
<td>14</td>
<td>21.5</td>
</tr>
<tr>
<td>Total</td>
<td>150</td>
<td>58</td>
<td>38.7</td>
</tr>
</tbody>
</table>

58 responses were received. There were challenges in obtaining a response from users involved in projects and especially from prospective user organisations, despite email follow-up chasing. The full survey results from both surveys are provided in Appendix D.

**Desk research**

Among the documentation reviewed were a review of annual calls for proposals in PASR and FP7 SEC, a review of the project fiches produced, and a detailed assessment of the projects selected in Phase 1. Various project-related materials were made available to the evaluators, including a sample of
**Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research**

**Section 1. Introduction, evaluation aims and methodology**

deliverables and project monitoring reports. A quantitative review of statistics from the CORDA database on projects supported was undertaken. A comparative analysis of a sample of national security research programmes against the ESRP was also undertaken.

**Workshop**

In order to present the results from the evaluation, CSES organised a workshop on the 30th November in Brussels. The workshop was attended by ca 100 participants from 17 EU countries, representing public security research institutes (24%), SMEs (23%), Universities (17%), large industry (15 %) and National Authorities (15%), including end-users. The presentations are available online.

**1.5 Report structure**

The final report is structured as follows:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction – evaluation aims, EU policy and legislative context and methodology adopted.</td>
</tr>
<tr>
<td>2</td>
<td>Programme Management and Implementation – programme management arrangements, human and financial resources, statistics on participation/financial implementation.</td>
</tr>
<tr>
<td>3</td>
<td>Evaluation findings – programme level. Feedback from the interview programme and survey work in respect of the implementation of PASR and FP7 Security Research. An assessment of horizontal issues (structuring security research, coordination activities, and the societal and ethical aspects) is then provided.</td>
</tr>
<tr>
<td>4</td>
<td>Beneficiary feedback and achievements and research results – feedback on participation in EU Security Research (Part 1). A typological framework for assessing outcomes, and review of research results and wider outcomes, including soft outcomes (Part 2).</td>
</tr>
<tr>
<td>5</td>
<td>Users and EU Security Research – the nature and extent of the role played by users in PASR and FP7 Security Research projects is examined. The take-up of research results is considered.</td>
</tr>
<tr>
<td>6</td>
<td>Conclusions and Recommendations – summarises the evaluation findings and analyses the key evaluation issues of efficiency, effectiveness, sustainability, utility and community value added.</td>
</tr>
</tbody>
</table>

The report is supported by a number of separately bound appendices. These include:

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>List of interviews</td>
</tr>
<tr>
<td>B</td>
<td>Bibliography – programme documentation, policy documents, evaluations and studies</td>
</tr>
<tr>
<td>C</td>
<td>Interview checklists – tailored to the different types of stakeholders in FP7 Security Research</td>
</tr>
<tr>
<td>D</td>
<td>Survey results – findings from i) the survey of beneficiaries in PASR and FP7 Security Research and ii) the survey of users</td>
</tr>
<tr>
<td>E</td>
<td>Selection of EU Security projects – the list of projects analysed for the case study research that have informed the evaluation more generally</td>
</tr>
<tr>
<td>F</td>
<td>Indicators paper – key issues in setting up a monitoring and indicator system</td>
</tr>
<tr>
<td>G</td>
<td>National security research programmes – detailed supporting analysis of how these operate and the extent of complementarity with FP7 SEC</td>
</tr>
<tr>
<td>H</td>
<td>Security Themes in PASR &amp; FP7 SEC work programmes – examines the extent of prioritisation and degree of continuity of particular themes in PASR &amp; FP7 SEC annual work programmes/calls for proposals</td>
</tr>
<tr>
<td>I</td>
<td>Case studies – four thematic case studies on CBRN, Aviation Security, Maritime Surveillance, Crisis management and emergency response. A horizontal case study on SMEs in FP7 SEC.</td>
</tr>
<tr>
<td>J</td>
<td>Standardisation – a review of developments in the area of harmonisation and standardisation</td>
</tr>
</tbody>
</table>

12 [http://www.cses.co.uk/security-workshop/]
Programme management and implementation

2. Programme management and implementation

An overview of PASR and FP7 Security Research is first presented (Section 2.1). Eligibility information and geographic scope are then provided (Section 2.2). Programme management and implementation arrangements are then considered (Section 2.3). Financial implementation to date, including issues relating to the expenditure profile and absorption capacity are examined next (Section 2.4). In Section 2.5, a statistical analysis of participation in PASR and FP7 Security Research (including SME participation) is then presented.

2.1 PASR and FP7 Security Research – scope, aims and objectives

2.1.1 Preparatory Action for Security Research (PASR) 2004-2006

The Commission launched the Preparatory Action on the Enhancement of European industrial potential in the field of Security Research 2004-2006 (“PASR”) to test the feasibility of going ahead with a full European Security Research programme within the RTD Framework Programmes. The legal basis for PASR was Article 157 of the EC Treaty on the ‘competitiveness of the Community’s industry’. The Commission’s Directorate-General for Enterprise and Industry (DG ENTR) was responsible for its preparation and implementation.

Following input by the Group of Personalities (GoP) to determine a strategic security research agenda, the following five themes were defined for PASR:

- Theme A - Improving situation awareness
- Theme B - Optimising security and the protection of networked systems
- Theme C - Protecting citizens from terrorist attacks with CBRN and energetic substances
- Theme D - Enhancing crisis management
- Theme E - Achieving interoperability between EU security organisations

The Activities and Work Programme for the Preparatory Action were included in the Commission Communication establishing the Preparatory Action 13 (COM (2004) 72). Three calls for proposals14 were launched in the 2004-2006 period. The main aim was to develop, demonstrate and validate technological solutions in each of the above areas. There was already a thematic dimension to the topics in some calls, although given the limited funding scope and the more innovative and experimental nature of a preparatory action, there was in-built flexibility in the call for applicants to develop proposals based around broad themes15.

The Commission undertook an internal review of PASR thematic research topics supported in the 2004 and 2005 calls and identified a number of areas that had not sufficiently been covered by 2004 and 2005 calls. These included critical infrastructure protection, protection and countermeasures against CBRN

---

14 The first Call was launched on 31 March 2004, the second Call was launched on 5 February 2005 and the final call on 10 February 2006.
15 Examples of topics suggested in PASR Calls included: studies in support of security solutions with an emphasis on human behaviour, perceptions of security and privacy, investigating the management of IPR and legal arrangements for the exchange of classified information between organisations participating in EU security research located in different Member States, and the integration of security supply chains.
Programme management and implementation

and explosives incident management and humanitarian operations. The integration of SMEs was also seen as an important element that had not received enough attention. In the 2006 call, therefore, project priorities encouraged included: Networked systems; Protection against terrorism; Crisis management; Interoperability and integrated systems; and Situation awareness.

PASR projects were designed to be mission-oriented and to deliver tangible results, so as to provide the basis for the future European security research programme. There was also a focus on encouraging project consortia to involve users.

PASR had a budget of €45m, with the budget divided equally between each of the 3 annual calls for proposals. PASR’s implementation can be seen as an important step in addressing the need for Community action in this area, and was intended to test the feasibility of going ahead with a full Security Research Programme through the RTD Framework Programmes.

With regard to geographic eligibility, unlike FP7, which is open not only to EU27 countries, but also associated countries in FP7, such as the US and Israel, PASR was confined to EU25 countries only.

As far as co-financing rates are concerned, for supporting activities financed through PASR, Community funding of up to 75% of the eligible costs was provided. This included up to 10% for management activities (financed at 100%). For collaborative research projects, EU funding of up to 75% of eligible costs was provided. The co-financing rate varied between (75% of industrial research, 50% of pre-competitive development activities). With regard to project duration, PASR allowed for the funding of between one and two years for research projects, whereas supporting activities were allowed to have a duration of between six months and three years.

2.1.2 FP7 Security Research

The RTD Research and Technological Development Framework Programme is the EU’s main instrument for funding (pre-operational) research and for establishing the European Research Area (ERA). The FPs provide multi-annual funding support to promote ‘world-class’ research, strengthen Europe’s scientific and industrial base, foster innovation, improve competitiveness and contribute to quality in employment.

The 7th Framework Programme (FP7)\textsuperscript{16} with a budget of EUR 50.5 bn was adopted in 2006 and covers the 2007-2013 period. The aim of FP7 is to contribute to the EU becoming the world’s leading research area through investment in world-class ‘state of the art’ research excellence. Its objectives are to: strengthen the scientific and technological base of European industry and to encourage international competitiveness, while promoting research that supports EU policies. FP7 is grouped into four programmes: Cooperation, Ideas, People and Capacities. The main instruments through which research funding is provided through FP7 include transnational collaborative projects and networks, which promote collaboration between publicly funded research and industry.

Following the successful implementation of PASR, a fully-fledged EU Security Research programme (FP7 Security - Theme 10) was included for the first time in the RTD Framework Programmes. FP7 Security, which has a budget of EUR1.4 billion, falls within the Cooperation objective, which fosters collaborative research across Europe and other partner countries and is the core of FP7. Funding from the European Commission’s DG Enterprise is supplemented by national co-financing for Security Research projects from beneficiaries and in some cases from national government funds to support R&D.

\textsuperscript{16} DECISION No 1982/2006/EC, 18 December 2006
The overarching objectives of FP7 EU Security Research are to: make Europe more secure for its citizens; strengthen industrial competitiveness; promote research excellence and state-of-the-art; support the (re)structuring of the European security sector; and to prevent the fragmentation of research efforts and strengthen critical mass in particular areas of security research. The specific objectives\(^{17}\) are to develop the technologies and knowledge for building the capabilities needed to promote the security of EU citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security, to stimulate cooperation between providers and users of civil security solutions, to improve the competitiveness of the European security industry and to deliver mission-oriented research results to reduce security gaps.

In order to achieve these aims, four security ‘missions’ and three cross-cutting missions were defined:

**Table 2.1: Structure of Security Theme**

<table>
<thead>
<tr>
<th>Security missions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security of citizens</strong></td>
<td>Delivering technological solutions for civil protection, including bio-security and protection against the risks arising from crime and terrorist attacks.</td>
</tr>
<tr>
<td><strong>Security of infrastructures and utilities</strong></td>
<td>Analysing and securing existing and future public and private critical/ networked infrastructure (e.g. in transport, energy, ICT), systems and services (including financial and administrative services).</td>
</tr>
<tr>
<td><strong>Intelligent surveillance and border security</strong></td>
<td>Focusing on technologies and capabilities to enhance the effectiveness and efficiency of systems, equipment, tools and processes and methods to improve the security of Europe's land and coastal borders.</td>
</tr>
<tr>
<td><strong>Restoring security and safety in case of crisis:</strong></td>
<td>Focusing on technologies providing support for diverse emergency management operations (such as civil protection, humanitarian and rescue tasks)</td>
</tr>
</tbody>
</table>

**Cross-cutting missions:**

| Security systems integration, interconnectivity and interoperability | Intelligence, information gathering and civil security, focusing on technologies to enhance the interoperability of systems, equipment, services and processes, including law enforcement, fire-fighting, civil defence and medical information infrastructures, as well as on the reliability, confidentiality and integrity of information and traceability of transactions and processing. |
| Security and society                                                   | Socio-economic analyses, scenario building and activities related to: cultural, social, political and economic dimensions of security, communication with society, the role of human values and policy making, citizens’ perceptions of security, ethics, protection of privacy, societal foresight and systemic risk analysis. Technologies that safeguard privacy and liberties, while addressing vulnerabilities and new threats, as well as the management and assessment of the impact of possible consequences. |
| Security Research coordination and structuring                        | Coordination of EU and international security research efforts and development of synergies between civil, security and defence research, improvement of legal conditions, and encouragement to the optimal use of existing infrastructures |

The Decision establishing FP7 stresses the need for links between other areas of FP7 and Security Research where appropriate. A security dimension is relevant in a number of FP7 thematic areas, such

as ICT, aeronautics and air transport, nanotechnologies, secure economics, social issues, the humanities and law.

**Funding instruments**

Funding schemes in FP7 Security include Collaborative Projects (CPs), Cooperation and Support Actions (CSAs) and Networks of Excellence (NoEs). An explanation of these instruments is provided below:

Table 2.2: FP7 funding instruments

| **Collaborative projects (CPs)** | CPs are research projects with clearly defined scientific and technological objectives and specific expected results (such as developing new knowledge or technology to improve European competitiveness). They are carried out by consortia made up of participants from different countries, and from industry and academia. |
| **Networks of excellence (NoE)** | These are designed for research institutions willing to combine and functionally integrate a substantial part of their activities and capacities in a given field, in order to create a European “virtual research centre” through “Joint Programmes of Activities” based on the integrated and complementary use of resources from entire research units, departments, laboratories or large teams. |
| **Coordination and support actions (CSAs)** | These are actions that cover not the research itself, but the coordination and networking of projects, programmes and policies. |

CPs and CSAs are the instruments that have been used in FP7 Security Research calls, and it is envisaged that NoEs may also be supported in future calls.

In order to support the achievement of objectives at the theme-specific level, FP7 SEC has adopted a Building Block Approach to supporting theme-specific implementation. This approach was advocated in the ESRAB stakeholder exercise. There are 3 types of building blocks - ‘capability projects’, which aim to build and/or strengthen security capabilities across the 4 security missions, ‘integration projects’, which aim at strengthening mission-specific capabilities and developing security systems and demonstrating their performance and ‘demonstration programmes’ - research aiming at large-scale integration, validation and demonstration of new security systems of systems, and promoting state of the art.

The approach is largely sequential, although some projects may be going on in parallel that seek to achieve progress across different types of projects. The following diagram sets out the approach.

**Figure 2.1: The Building Block approach to FP7 Security Research**
The different types of projects require differing levels of budget allocation in order to achieve their aims. The following table sets out the approach:

**Table 2.3: FP7 Security Research - project type and funding range**

<table>
<thead>
<tr>
<th>Project type</th>
<th>Details</th>
<th>Project funding range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demonstration</td>
<td>Systems of systems demonstration</td>
<td>Phase 1 feasibility projects</td>
</tr>
<tr>
<td></td>
<td>- Combination of IP results</td>
<td>&lt;€1m</td>
</tr>
<tr>
<td></td>
<td>- Multi-mission</td>
<td>Phase 2 full demonstration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>project €10m – €30m</td>
</tr>
<tr>
<td>Integrated</td>
<td>System development and validation</td>
<td>€5m – €10m</td>
</tr>
<tr>
<td></td>
<td>- Combination of capabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Mission specific</td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td>Capability development</td>
<td>€1– €5m</td>
</tr>
<tr>
<td></td>
<td>- Technology development</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Multi mission and mission specific</td>
<td></td>
</tr>
</tbody>
</table>

FP7 Security Research places a strong emphasis on ‘demonstration projects’, which are seen as the ‘flagships’ of the programme. Phase 1 Demonstration Projects are of 12 – 18 months duration and define strategic roadmaps that take into account relevant completed, ongoing and planned work and indicate further research needs for integration projects and capability projects under the Security theme. Such projects are funded through Coordination and Support Actions (CSAs).

Phase 2 Demonstration Programmes carry out research aiming at ‘large scale integration, validation and the demonstration of new state of the art security systems of systems. They depend upon the compatible, complementary and interoperable development of requisite system and technology building blocks of the integration projects and capability projects. They are intended to promote the application of an innovative security solution, which implies a strong involvement of end users, taking into account the relevant legal and society related issues and strong links to new standardisation’ (definition of a DP: DG ENTR). Such projects are funded through Collaborative Projects and require significant R&D investment. They are up to 4 years in duration.

Support has been provided in the first two calls for a number of Phase 1 Demonstration Projects with up to 1m euros in funding to test the feasibility of technologies or applications. In the 3rd and 4th Calls of FP7 Security, a number of larger-scale Phase 2 Demonstration Programmes are being supported varying in size from €10m – €30m. The emphasis on large-scale demonstration projects reflects the need to ‘successfully demonstrate the appropriateness and performance of novel solutions’.

### 2.2 Type of beneficiaries and geographic scope

#### 2.2.1 Types of beneficiaries eligible for FP7 Security Research

With regard to the types of organisations eligible, potential beneficiaries in FP7 Security Research are the same as those in other parts of the RTD Framework Programmes. The following types of organisations can participate: research institutes, universities and other academic institutions, SMEs, large firms as well as users: public agencies working in the security arena (local, regional or national), institutions running research infrastructures of transnational interest organisations and researchers from third countries, international organizations and civil society organisations. There are different co-financing levels for participants in FP7 SEC depending on the beneficiary type. For example, SMEs,
research institutions and universities have higher levels of co-financing (75%) than large firms (50%) for collaborative research projects, as shown in the following table.

Table 2.4: Co-financing rates: FP7 Security Research Programme

<table>
<thead>
<tr>
<th>Funding schemes</th>
<th>Public bodies, higher education institutions, research organisations and SMEs</th>
<th>Large firms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research and technological development activities</td>
<td>75%</td>
<td>50%</td>
</tr>
<tr>
<td>Demonstration activities</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Coordination and support actions</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Management, audit certificates and other Activities</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Co-financing rates for FP7 SEC are the same as those across the FP7 Cooperation Programme overall. SME co-financing has been increased to 75% for Collaborative research projects across FP7 overall, compared with 50% in FP6. There is scope for higher EU co-financing for large firms in the case of particular types of projects (this needs to be demonstrated in the proposal): up to 75% for the development of capabilities in domains with a very limited market size and a risk of "market failure" and accelerated equipment development in response to new threats.

2.2.2 Geographic scope of FP7 Security Research and involvement of associated and third countries

The eligibility rules on participation are set at the level of FP7 overall and also apply to Theme 10 Security. Entities are eligible from all EU27 Member States and the Associated Countries (countries that pay into the overall budget for FP7). These include EEA/ EFTA countries (Iceland, Norway, Lichtenstein and Switzerland), EU candidate countries (e.g. Croatia, Turkey), and Israel. The same conditions apply for both EU Member States and Associate Countries. Wider potential beneficiaries include the International Cooperation Partner Countries - Russia and other Eastern European and Central Asian states, developing countries, Mediterranean partner countries and Western Balkans countries. Participation by industrialised high-income countries is possible on a self-financing basis'.

Cooperation with “third countries” is encouraged through FP7. The aim is first to support European competitiveness in selected fields through strategic partnerships with third countries, secondly to encourage the best third-country scientists to work in and with Europe; and to address specific problems that either have a global character or are commonly faced by third countries. Cooperation has potential to be mutually beneficial in areas of security research. For example, global cooperation is needed to promote greater standardisation and interoperability, with particular reference to areas such as aviation security, tackling terrorism and CBRN.

2.3 Programme management and implementation

Factual aspects relating to programme management and implementation arrangements are now summarised. In Section 3.3, the effectiveness of implementation arrangements is analysed. The role of different actors in FP7 Security Research is first set out. The Commission and the Research Executive Agency (REA) are responsible for programme management and monitoring, but the Security Programme Committee, the Security Advisory Group and the National Contacts Points also play an important role.
within the overall implementation structure. The main areas addressed include (i) the procedures for evaluating Calls for Proposals, project selection and grant awards, (ii) administrative expenditure and human resources on programme implementation (iii) project monitoring and iv) promotion and dissemination activities.

2.3.1 PASR

PASR was managed by the Commission services directly. While the early stages of planning for PASR were carried out by staff from DG RTD, responsibility was then transferred for the management, implementation and monitoring of PASR projects to DG ENTR. Evaluation and selection procedures, as well as eligibility checks were carried out by the Commission, which was then responsible for drawing up a list of all proposals evaluated ranked in priority order based on their final score. The list of proposals retained for negotiation took into account the budget available. A reserve list was also retained, and at least in one year, additional projects were funded from the reserve funding set aside.

The main evaluation criteria for assessing proposals under each of the 3 PASR calls included: the relevance of the proposal to the PASR Work Programme; reinforcement of the competitiveness for European industry and potential for exploitation; scientific and/or technological excellence and contribution to tangible and demonstrable improvements in security; the building of effective partnerships between (public) users, industry and research; the ability of the consortium to protect classified information if necessary, and clear plans for the management of intellectual property.

Project officers (POs) were then responsible for monitoring the implementation of individual projects. This was viewed by officials interviewed as having been a useful exercise in that it gave an in-depth understanding about how well projects were working on the ground.

2.3.2 Role of the Commission and the REA in programme management

During the first two and a half years of FP7, the European Commission’s DG Enterprise was responsible for programme management and implementation, including monitoring aspects. DG ENTR officials from the Security Research Unit (H3) were responsible from January 2007 - June 2009. Key responsibilities include the preparation of Calls for Proposals and guidance for applicants, the evaluation of project applications, contracting procedures, the monitoring of projects underway and project closures. DG ENTR officials have also fulfilled a project officer role and been responsible for monitoring projects in particular thematic areas of FP7 Security, such as CBRN, maritime security, crisis management etc.

The Research Executive Agency (REA) was established to administer the RTD Framework Programmes. In June 2009, the REA assumed responsibility for most day-to-day programme management aspects including managing technical aspects of the launch of Security Calls for Proposals and the evaluation and selection process of project applications, financial management and project monitoring (with the exception of larger demonstrators and classified projects, which remain under DG ENTR).

Responsibility for EU Security Research policy issues remains the responsibility of the Commission’s DG ENTR, which is guided in its work by various bodies, including the Security Advisory Group (SEC AG), the Security Programme Committee (see below) and the work of ESRIF (a forum which brought together 600 experts in security research and contributed to the development of a strategic security research agenda). The work of the ESRAB and ESRIF stakeholder fora has also influenced the drawing up of the annual work programmes and calls for proposals and the research topics selected.

The Commission is also responsible for promoting the dissemination of research outcomes and networking among relevant security actors. Specific topics to be covered in calls for proposals are also
determined by the Commission, taking into account the views of stakeholders such as the Security Advisory Group, a network of security research experts, and the Security Programme Committee.

2.3.3 Role of other bodies in FP7 SEC management and implementation structures

The Security Programme Committee, comprised of representatives from Members States and Associated States, is responsible for reviewing the annual work programme (and call for proposals) before it is adopted and for the security procedure, in which the selection process is validated. Members of the Committee are from a variety of backgrounds, but are mainly from relevant government Ministries dealing with security research or broader security issues at national level.

In common with other areas of FP7, a Security Advisory Group (SEC AG) was set up in November 2007 to provide expert steering and guidance to the European Commission in managing FP7 SEC. SEC AG consists of 20 security experts acting in an individual expert capacity. The membership of the Security Advisory Group (SAG) rotates and a new advisory group was established in 2010. The role of the group is to assist the Commission and to provide feedback that will assist in improving the effectiveness of programme implementation. Its main task is to provide written advice on the Work Programme for Security Research, and in particular, to give opinions on the proposed research topics of forthcoming calls. SEC AG meets 2 – 3 times per year and worked in close cooperation with the European Security Research and Advisory Forum (ESRIF) in the 2007-2009 period. The composition of the SEC AG was examined, since some stakeholders have suggested that this body is industry dominated. However, in fact, there is balanced representation between experts from the security industry, consultancy, academia / research institutes and users from both the Member States and the Associated States.

The network of FP7 Security Research National Contact Points plays an important role in promoting participation in FP7 SEC and in providing advice, guidance and information about the programme. NCPs are national structures financed by national governments across EU27 and Associated States. They provide personalised support in proposers' own languages and can assist in partner identification. NCPs also play an important dissemination role. NCPs operate differently across different countries from a highly centralised to a decentralised network approach. Diverse actors serve as NCPs ranging from government ministries to universities, research centres and consulting firms.
All of the main processes and procedures involved for FP7 SEC in selecting projects following a call for proposals, and the negotiation and contracting process are based on the approach adopted across FP7 overall. The procedure for evaluating calls and making funding decisions is summarised below:

Figure 2.2: FP7 Security Call for Proposals and Project Award procedures

Calls for Proposals are included in the annual work programmes. Once calls are launched, there is then a 4 month period for applications. After the receipt of proposals following call closure, the REA first carries out an eligibility check to ensure that they are compliant from an administrative perspective. Proposals are then evaluated by independent external evaluators appointed in the following six weeks or so after the call deadline date to assess the technical content of applications.

Only project proposals achieving the highest scores above the evaluation threshold will subsequently enter into the negotiation phase which may lead to a grant agreement. Applications are then assessed by between 3 and 5 independent external evaluators, depending on the type of project. An evaluation ‘consensus’ meeting is then held at the REA in Brussels, with individual evaluation scores compared. An Evaluation Summary Report (ESR) is then produced. Both applicants and the Security Programme Committee are then informed about the results of the preliminary assessment.

The Commission has produced general guidelines for FP7 in its Rules for the submission of proposals, and the related evaluation, selection and award procedures. The procedures apply across FP7 overall.

---

Detailed evaluation criteria are set out in the annual FP7 SEC work programme and in the Rules for Participation in FP7. The main evaluation criteria include: (1) scientific and/or technological excellence; (2) relevance to the objectives of the specific programmes; (3) the potential impact through the development, dissemination and use of project results; and (4) the quality and efficiency of the implementation and management. Specific evaluation criteria are then provided in the guidance for applicants under each SEC call, depending on the type of funding scheme. The criteria are quite general, and reflect those of FP7 overall, rather than relate specifically to security research.

Following provisional project selection, an important characteristic of FP7 Security is the Security Scrutiny procedure by national authorities in the Security Programme Committee. The aim of security scrutiny which is unique to FP7 SEC is to assess projects that have been flagged up as ‘sensitive’ i.e. projects in which the applicants have indicated that classified information would be involved during project implementation. In such projects, the table of deliverables must specify the level of classification for each deliverable. The Security Committee Members are requested to verify that the level of classification is appropriate, that this does not compromise national security and that dual use aspects are given full consideration. The scrutiny procedure takes place following the evaluation of proposals and before the start of the negotiation of selected projects. The process can add 2 - 5 months to Time to Grant (TtG) prior to the negotiation phase.

The Commission included procedures in FP7 for a review in all project proposals that have been provisionally selected, but raise ethical questions. Such project applications are subject to an Ethical Review whose aim is to ensure that EU funding is not allocated to research that does not comply with relevant EU legislation and that sufficient consideration of ethical considerations is taken into account. The aim is to safeguard fundamental rights and to ensure adequate respect for the ethical and societal dimension of EU Security Research. In FP7 SEC, examples of the sorts of issues raised during ethical screening processes include:

- **Dual use** – projects where there is a need to monitor technologies to ensure that they cannot be used for non-civilian purposes
- **Privacy concerns** – e.g. monitoring and surveillance technologies such as the tracking of suspicious/abnormal behaviour in public places using new-generation CCTV cameras and the deployment of new technologies (e.g. body scanners)
- **Health and safety considerations in relation to the general public** - e.g. the deployment of new technologies, such as body scanners raises some health concerns

The independent evaluators responsible for assessing project applications may flag up projects that they identify as raising ethical considerations. Applications may then be subject to more detailed ethical screening by the ethical review board, which consists of both Commission officials and external experts.

While no applications have been stopped on purely ethical grounds to date across FP7 overall, ethical screening has led in a number of instances to revisions to applications to address concerns identified at the proposal stage in relation to ethical issues. Project consortia have been asked to further develop parts of their application to show how they will take into account ethical concerns raised. Recommendations have also been made that specific steps must be taken to address ethical considerations, such as setting up an external advisory panel of experts, ensuring that dual use is monitored, etc.
In the 3rd FP7 Monitoring Report (DG RTD, July 2010), disaggregated data was made available for the first time. This showed that in 2009, 11 Security Projects were submitted to an ethical review. This is relatively low compared with other areas of FP7, such as ICT (21), Food, Agriculture and Fisheries, Biotechnology (35) and Health (39). The ethical screening procedure applied to projects in which an ethical review has been flagged up has often led to recommendations being made that have had a positive influence in strengthening the ethical aspects of projects. For example, sometimes projects have been required to put in place an external advisory committee to advise on ethical aspects at key junctures in project implementation.

In so far as possible, the Ethical Screening process and Security Scrutiny procedure are carried out in parallel, but some projects may undergo both and must be undertaken sequentially. The Commission then ranks the applications, according to their project score. Unsuccessful project applicants are informed about the decision and negotiations then begin with successful applicants. Grant Agreements (GAs) are then signed between the Commission and successful applicants19.

Time to Grant (TtG), measured in terms of the number of days between the closure of the call and the signature of the GA is a key programme efficiency indicator used across FP7 and benchmarked between the different thematic areas. Programme management statistics from DG RTD’s Third FP7 Monitoring Report (July 2010) provide data on time to grant. In the following Figure, the average time to grant across different areas of the Cooperation Programme within FP7 is provided:

Figure 2.3: Time to Grant Agreement, (Mean average), FP7 Programmes (days)

Average TtG for FP7 SEC was 530 days, the longest lead time to grant across FP7 by a small margin. The graph shows that long contracting timescales is a problem across other areas of FP7, and 7 out of 10 thematic areas take >400 days to sign the GA. As noted earlier, the Security Scrutiny procedure adds more time to the assessment process, and while ethical screening takes place in other areas of FP7 Cooperation, there are clearly unique features in FP7 SEC, notably the need to consider dual use issues, since FP7 SEC is a civil security research programme.

19 Regression requests can be filed from unsuccessful applicants and after reconsideration the final list of successful applicants is compiled.
Commission and REA officials would like to reduce TtG. However, in practice, it has thus far proved difficult to shorten lead times. The improvement of ICT systems that support the REA during the selection and negotiation process may be able to reduce lead times and according to one interviewee, it should be possible to reduce the level to about 480 days. However, any major reduction in TtG cannot be achieved without changes across FP7 overall since the REA’s Security Unit follows the rules and procedures for FP7 drawn up by DG RTD. It should also be stressed that the REA has to follow the rules laid out in the EU Financial Regulation and the administrative and financial validation of all partners, while necessary, is time consuming. There is an inherent tension between the need to ensure sound financial management of EU funds and to reduce TtG on the other.

2.3.4 Project monitoring and project closures

Project monitoring includes reviewing the content of periodic project monitoring reports, and checking deliverables against the proposal and description of deliverables in Annex 1 of the contract. Technical Project Officers (POs) at the REA are responsible for monitoring the quality of technical content of most projects. POs also take part in the kick-off meeting of projects and in key project review meetings (usually a meeting is held midway through implementation), and can play a key role in steering projects. The REA is also responsible for the project closure process.

Although monitoring responsibilities have now largely been transferred to the REA, as noted earlier, DG ENTR remain responsible for monitoring projects with classified deliverable and large-scale demonstration projects.

2.3.5 Awareness-raising and promotional activities

Among the main promotion and dissemination activities include: activities to raise awareness about, and promote participation in FP7 Security Research, the promotion of networking and cooperation between relevant FP7 Security actors (providers and users) and activities to promote the exploitation and dissemination of research outcomes. However, the Commission already has a secure bunker in Brussels, which provides a mechanism for the submission of classified project information. This arrangement appears to be working well.

Various actors play a role in promoting participation in FP7 Security Research, in particular, the European Commission’s DG ENTR, the REA and the network of FP7 National Contact Points for Security Research respectively. With regard to the promotion of participation in FP7 Security Research, the Commission publicises general information about FP7 Security Research on the DG ENTR website\(^\text{20}\), the DG RTD website\(^\text{21}\) and on the Cordis website.\(^\text{22}\) The REA has also organised an annual information day in Brussels prior to the launch of Calls for Proposals to provide advice and guidance and practical information about calls. There is strong demand to attend this event from prospective beneficiaries. The Commission and REA also participate in national events, and determine which official will attend depending on language skills and knowledge of security research in particular countries.

While the Commission has as yet not developed a formal communication strategy on the dissemination of results, the Security Research Unit undertakes various activities to promote awareness about FP7 SEC to encourage the wide dissemination of research results.

\(^\text{21}\) http://ec.europa.eu/research/fp7/index_en.cfm?pg=security
\(^\text{22}\) www.cordis.europa.eu/fp7/security/home_en.html
Programme management and implementation

Among the tools to raise awareness about FP7 Security and its achievements are the holding of conferences and workshops and the development of publications. In the past, annual European Security Research Conferences, which bring together approximately 1000 representatives from research, industry, EU institutions, public authorities and other stakeholders with an interest in the security of Europe's Citizens, have been organised in Member States holding the rotating Presidency with the support of the Security Research Unit within DG ENTR.

During 2010, DG ENTR organised a series of stakeholder workshops on different thematic areas of FP7 Security including aviation security, maritime surveillance, CBRN and the societal and ethical dimension of security research, communications, interoperability and networked systems. The purpose has been to promote discussion and encourage cooperation among relevant stakeholders, to strengthen policy understanding and knowledge in particular thematic areas and to disseminate informational about projects and research results to date. It is anticipated that further thematic workshops will be held during the remainder of FP7 SEC.

DG ENTR has also produced publications to promote FP7 SEC projects such as a project Compendium in 2010 ‘Investing into security research for the benefits of European citizens’, (which contains 75 project examples) and the Security Research in Focus magazine (August 2010) which has been disseminated at Security Research workshops. This could provide an opportunity to publicise the results achieved through PASR projects among relevant providers and users.

2.3.6 Management and exploitation of classified information

The management and exploitation of classified information is managed by the European Commission directly. Mechanisms have been put in place for storing classified information. There is a procedure in the FP7 evaluation rules for applications and project evaluations where experts will have to deal with classified information, ‘the appropriate security clearance shall be required before appointment’. Some FP7 SEC applications make clear that their project will involve some classified elements. A three standard scale is used – restricted (only to be shared among the members of the project consortium), confidential and secret. As noted earlier in relation to the description of procedures for assessing proposals following a call for proposals, those projects that will include confidential materials ‘sensitive projects’ are reviewed by national representatives from the programme security committee as part of the Security Scrutiny procedure.

The main challenges for the Commission in managing classified information include retaining confidence about the ability to manage classified information while at the same time ensuring that there is reasonable transparency about projects that include classified deliverables. A second challenge is the dissemination of classified project materials to appropriate stakeholders so that research results can be exploited effectively.

Among the issues examined in relation to classified information were the effectiveness of the Commission’s systems for managing classified information. Some concerns were raised through the discussions, by beneficiaries as to whether the Commission has the necessary procedures and technologies in place to handle classified information. However, the Commission already has a secure

---

site in Brussels which provides a mechanism for the submission of classified project information. This arrangement appears to be working well.

Among beneficiaries, many of the larger firms interviewed carry out both civil security and defence research and are accustomed to handling classified and sensitive information. Large firms typically have invested in the infrastructure, technology, procedures, and systems needed to obtain security clearance for personnel to deal with classified information. Moreover, they have the necessary secure IT systems to ensure that data and information can be encrypted and transferred. End-users such as intelligence agencies and national police authorities also have the ability to handle classified information.

The procedures to facilitate information exchange between partners in different countries can be burdensome and national legislation can sometimes prevent the transfer of sensitive data across borders. Another finding was that some SMEs participating in projects do not have the infrastructure or procedures in place to manage classified information. This may prevent projects with classified deliverables from sharing information with, and between, all project partners. However, since there is a division of work into separate work packages, there are usually ways of working around this issue.

On some projects, information cannot be shared by the lead coordinator with all partners due to difficulties caused by varying national procedures on exporting classified information and research materials. A concern raised by some stakeholders was how the Commission will make use of classified information and deliverables and whether it can ensure that relevant research results are disseminated to appropriate users. Some projects have supported the development of secure networks, and this may provide a potential mechanism for information transfer in future.

Another challenge identified is persuading intelligence agencies of the benefits of sharing information and data on an EU wide basis. There were concerns that nationally sensitive data may not be fully secure if it is shared with too many partners. That said, it is clear that some intelligence agencies are interested in some of the projects being supported, where these have potential to add knowledge and insight, for example, foresight and scenario modelling in relation to threats from emerging technologies. Some PASR projects, such as PALMA, piloted the transfer and use of confidential information between project partners. There is a need to reconcile the requirement for confidentiality on the one hand, and ensuring accountability in delivering a publicly financed EU programme on the other. In this regard, periodic monitoring reports play an important role since these provide a publishable summary of project aims and progress made, without revealing any classified elements.

2.4 Human and financial resources

During the first two and a half years of programme implementation, when programme management and monitoring aspects were managed by the Commission’s DG ENTR, the Security Unit only had a small number of staff. It currently has 20 staff. This has remained broadly constant in the past 3 years since the programme got underway. A breakdown of staffing is provided below:

<table>
<thead>
<tr>
<th>Staff type</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of Unit (HoU)</td>
<td>1</td>
</tr>
<tr>
<td>Deputy Head of Unit (HoU)</td>
<td>1</td>
</tr>
<tr>
<td>Project / Policy Officers</td>
<td>11</td>
</tr>
<tr>
<td>Administration</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>20</strong></td>
</tr>
</tbody>
</table>
Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research

Section

Programme management and implementation

There are additionally a further 23 full-time staff at the REA in Security Unit S3 that work directly on programme administration. This includes a combination of Technical Project Officers (POs) and legal and financial officers. A breakdown of the current human resources position is provided in the table below:

Table 2.6: Staff at REA in Security Unit S3 - 2010

<table>
<thead>
<tr>
<th>Staff type</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of Unit (HoU)</td>
<td>1</td>
</tr>
<tr>
<td>Deputy Head of Unit (HoU)</td>
<td>1</td>
</tr>
<tr>
<td>Technical Project Officers (POs)</td>
<td>9</td>
</tr>
<tr>
<td>Legal Officers</td>
<td>2</td>
</tr>
<tr>
<td>Financial Officers</td>
<td>3</td>
</tr>
<tr>
<td>Administration</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
</tr>
</tbody>
</table>

There will be an increase in project monitoring activities from 2011 onwards, as some of the new projects that have been in the contract negotiation phase or have only recently got underway begin to produce deliverables. Accordingly, the REA plans to increase its resources in the remainder of the programming period from the present 23 to planned staffing of 31 (2011), 36 (2012) to 43 (2013).

A maximum ceiling of 6% for Commission administrative expenditure was set out in the Decision establishing the FP7 Programme which applied to the programme overall, not only to FP7 SEC. Article 3 states that ‘the amount deemed necessary for the execution of the Specific Programme shall be EUR 32 413 million, of which less than 6% shall be for the Commission's administrative expenditure’. The Security Research Unit appears to be on target to spend considerably less than the 6% of expenditure on administration. However, it is difficult to estimate the precise proportion of expenditure on programme administration since the figures made available by Unit H5 are currently aggregated at Directorate H level within DG ENTR (i.e. covers Security, Space and GMES respectively), whereas operational expenditure is broken down between these areas.

2.5 Financial implementation and participation in PASR and FP7 Security Research

The assessment draws on the following information sources: DG ENTR data on the implementation of PASR; annual SEC Work Programmes for 2007, 2009 and 2010 (which include an indicative breakdown of funding allocation between funding scheme), the 1st, 2nd and 3rd FP7 Monitoring Reports (DG RTD), the Annual report on the RTD activities of the EU (2007, 2008, 2009); and the 4th and 5th Progress Reports on SME Participation in the 7th R&D Framework (DG RTD). The Annual monitoring report on the RTD activities of the European Union is an additional data source and provides statistics on FP7 overall.

2.5.1 PASR 2004-2006

Since PASR was a Preparatory Action, it was outside the scope of FP6. It had an overall budget of € 45M, divided equally over 3 calls i.e. €15m in each Call. An overview of the budget committed, based on an analysis of the individual project fiches is provided on the following page:

---

26 COUNCIL DECISION of 19 December 2006
Table 2.7: PASR actual spend by budgetary year

<table>
<thead>
<tr>
<th>Year</th>
<th>Total €</th>
<th>Average</th>
<th>Max</th>
<th>Min</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>14,624,500</td>
<td>1,329,500</td>
<td>2,717,640</td>
<td>171,900</td>
</tr>
<tr>
<td>2005</td>
<td>15,226,604</td>
<td>1,171,277</td>
<td>2,651,542</td>
<td>364,000</td>
</tr>
<tr>
<td>2006</td>
<td>15,315,506</td>
<td>1,021,034</td>
<td>2,710,838</td>
<td>218,823</td>
</tr>
<tr>
<td>Total</td>
<td>45,166,610</td>
<td>1,158,118</td>
<td>2,717,640</td>
<td>171,900</td>
</tr>
</tbody>
</table>

Source: CSES analysis

The funding allocated was easily utilised, reflecting the strong demand to take part in the PASR Preparatory Action.

2.5.2 FP7 Security Research 2007 – 2013

FP7 SEC was allocated a budget of 1.4bn EUR over the 2007-2013 period. An analysis of the financial allocation in respect of the first three calls for proposals is now provided. The table below provides an overview of Calls for Proposals launched to date in FP7 Security and the Joint ICT and Security Call.

Table 2.8: EU Security Research in FP7

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Budget (euros):</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP7-ICT-SEC-2007-1</td>
<td>Joint Call between ICT and Security Themes on Critical Infrastructure Protection</td>
<td>40,000,000</td>
</tr>
<tr>
<td>FP7-SEC-2007-1</td>
<td>Security Research Call 1</td>
<td>80,300,000</td>
</tr>
<tr>
<td>FP7-SEC-2009-1</td>
<td>Security Research Call 2</td>
<td>117,900,000</td>
</tr>
<tr>
<td>FP7-SEC-2010-1</td>
<td>Security Research 2010</td>
<td>210,590,000</td>
</tr>
<tr>
<td>Total</td>
<td>NA</td>
<td>448,790,000</td>
</tr>
</tbody>
</table>

Source: DG Enterprise and Industry, CORDA database

The joint ICT and Security Research Call in 2007 launched by DG ENTR and DG INFSO\(^\text{27}\) to promote ICT Security to improve critical infrastructure protection had a budget of €40m (€20m was funded through the ICT Theme and €20m through Security). While the 3\(^{rd}\) Call for Proposals is included in the statistical analysis set out in Section 2, the projects themselves are outside the scope of this interim evaluation. Grant Agreements with successful applicants from the third call have only recently been signed.

Table 2.9: Financial data on participation in FP7 Security Research

<table>
<thead>
<tr>
<th>Indicator</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested EU Contribution ALL</td>
<td>€201.6m</td>
</tr>
<tr>
<td>Requested EU Contribution SMEs</td>
<td>€40.6m (20.2%)</td>
</tr>
</tbody>
</table>


Financial absorption issues (commitment levels to date against the total budget) were also examined. Absorption was considered in relation to the programme overall, and the consumption of funds by SMEs

\(^{27}\) During FP7, DG INFSO will invest 90m EUR on research for ICT Security projects (e.g. improving security in network infrastructures, identity management, privacy, biometrics, trust policies and service infrastructure
Programme management and implementation

in FP7 Security Research against the overall target for the Cooperation Programme of 15%. An overview of the current state of play in respect of financial absorption is set out below.

Table 2.10: Financial absorption against targets in FP7 Security Research

<table>
<thead>
<tr>
<th>Indicator</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total foreseen budget</td>
<td>€ 1,350,000,000</td>
</tr>
<tr>
<td>% of SEC budget used as at 30.04.10</td>
<td>14.9% of budget used</td>
</tr>
<tr>
<td></td>
<td>1 April 2010</td>
</tr>
<tr>
<td>Amount of budget used (overall)</td>
<td>€201.6 m</td>
</tr>
</tbody>
</table>

Source: 5th Progress Report on SME Participation in the 7th R&D Framework, DG Research, 30.04.10

An important issue is whether at interim stage in implementation, there is sufficient financial absorption capacity to commit allocated expenditure in FP7 Security. There are various factors to consider in assessing absorption issues, including: the anticipated expenditure profile for FP7 Security during the 2007-2013 period, expenditure committed to date, the capacity of current and future beneficiaries to absorb funding. The first and second calls for proposals focused on supporting the basic building blocks of FP7 (capability projects and medium-sized integration projects). In the second half of FP7, there will be a switch towards larger-scale demonstration projects which are more capital-intensive. The expenditure profile is geared towards the 2nd half of the programming cycle. While the evaluation scope focuses on the first two calls for proposals in FP7 SEC, it is worth briefly summarising the position in terms of financial implementation in December 2010.

Approximately €520m has been committed across the first 3 Calls for Proposals in FP7 SEC and through the Joint Call. A further €221m is expected to be committed in the 4th call. Funding is weighted towards the 2nd half of the programming period. Large-scale demonstrators will consume considerable resources from the 4th call onwards. Total financial commitments are expected to be close to €750m (53.6%) by summer 2011 once 4th call projects have been selected. Overall, FP7 Security appears to be on track to achieve a high level of funding absorption. The Commission does not foresee problems in committing the allocated funding in the remainder of the period. Many beneficiaries previously participated in the RTD FPs prior to the setting up of a European Security Research Programme. They therefore had familiarity with the different funding instruments and the procedures involved in applying for funding through the RTD Framework Programmes.

2.5.3 Participation in PASR and FP7 Security Research

There was high demand to participate in PASR. The data in the following table shows that PASR was considerably over-subscribed. The number of applications received in each call is provided below (and the number of projects actually funded in the following table).

Table 2.11: Applications for PASR EU25 + EEA (2004 - 2006)

<table>
<thead>
<tr>
<th>Applications</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projects</td>
<td>123</td>
<td>120</td>
<td>121</td>
<td>364</td>
</tr>
<tr>
<td>Supporting activities</td>
<td>50</td>
<td>36</td>
<td>44</td>
<td>130</td>
</tr>
<tr>
<td>Total</td>
<td>173</td>
<td>156</td>
<td>165</td>
<td>494</td>
</tr>
</tbody>
</table>

Source: DG ENTR, Unit H3

An overview of projects selected for funding is now provided.
Programme management and implementation

Table 2.12: Projects selected PASR 2004-2006

<table>
<thead>
<tr>
<th>Funded projects</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projects</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>23</td>
</tr>
<tr>
<td>Supporting activities</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>16</td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td>13</td>
<td>15</td>
<td>39</td>
</tr>
</tbody>
</table>

Source: DG ENTR, Unit H3

The data shows that a high proportion of total projects (16/39) were supporting activities. This was because the intention of the Preparatory Action was to lay the ground for the full security programme and there was a need to develop the basic networking and coordination activities in order to do so.

An overview of participation in **FP7 Security Research** is provided in the table below (the focus of the evaluation is on PASR and the first two calls for proposals in FP7 Security):

Table 2.13 Data on participation in FP7 Security Research

<table>
<thead>
<tr>
<th>Indicator</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Grant Agreements</td>
<td>66</td>
</tr>
<tr>
<td>No. of participants in Grant Agreements</td>
<td>722</td>
</tr>
<tr>
<td>Nr of SME participations in GA’s</td>
<td>135</td>
</tr>
<tr>
<td>% participations of SMEs</td>
<td>18.7%</td>
</tr>
</tbody>
</table>

Source: 5th Progress Report on SME Participation

66 Grant Agreements had been signed with project consortia by 30th April 2010 (the cut-off period for the evaluation scope), with 722 organisations represented. 18.7% were SMEs - issues relating to SME participation in FP7 SEC are examined in section 5.1 – 5.3). The ratio of applications received to successful applicants in the first 3 Calls was 1:7.6. This indicates strong demand to take part in the programme. With regard to the average size of project consortia, under the Security theme, there were an average of 8.9 partners of which 2.0 were SMEs. The average number of partners in the Cooperation programme overall was 11.1 partners.

CSES was subsequently provided with access to recent data from the CORDA database. While the timescope focuses on the first 2 calls in FP7 SEC, it is worth noting the position in December 2010. There continues to be strong demand to participate in FP7. Across the first three security calls and the joint ICT and Security Call, 131 projects have been supported to date. 50 projects were supported through FP7 SEC in the first 2007 call, 9 in the joint ICT and Security Call (2007) and 32 projects in the 2nd 2009 SEC call. 40 projects were supported in the 3rd SEC call in 2010. In the 4th call for proposals which closed in December 2010, more than 300 proposals were received, reflecting strong demand to take part in the programme among the security research community.

As far as participation by country is concerned, it was notable that there was comparatively low participation by some of the new member states. This reflects the fragmentation of research efforts in some countries, and the need for capacity building to encourage firms from the new member states to take part. In Romania, with this in mind, a national programme was set up to develop capacity and in Lithuania, according to the NCP, consideration is also being given to setting up a national security research programme.
3. Evaluation findings – Programme level

In this section, the programme-level findings are first outlined. The intervention logic and indicators are first presented. The evaluation results are then outlined drawing on feedback on programme management. A summary of the findings from the thematic research on security research and assessment of cross-cutting issues is then provided, followed by a comparative analysis of national security research programmes compared with ESRP.

3.1 Intervention logic – PASR and FP7 SEC

The intervention logic was assessed to check whether the rationale was sound, and whether the links between identified needs, global and specific objectives and the types of activities being supported are sufficiently clear. The logic for the PASR preparatory action was first mapped out below:

**Figure 3.1: Intervention Logic – PASR**

- **Needs, problems**
  - Changing nature of security threats and challenges
  - Lack of national funding for security research in most EU countries
  - Industry fragmentation
  - Absence of harmonised standards and interoperability in some areas
  - Absence of common testing and certification
  - The need to strengthen border security post EU enlargement
  - Unrealised potential for cross-fertilisation between civil/ non-civil security research

- **Global objectives**
  - Test viability of implementing a future European Security Research Programme.
  - Enhance EU industrial potential in the field of Security Research
  - Stimulate critical mass of technologies, knowledge and resources to provide valid solutions to security challenges
  - Foster the pre-conditions to improve the EU’s capabilities in security-related research

- **Specific objectives**
  - Improve situation awareness
  - Protect from terrorist attacks with CBRN and energetic substances
  - Enhance crisis management
  - Achieve interoperability between EU security organisations

- **Operational objectives**
  - Demonstrate and validate proof of concept
  - Test viability for development of pre-standards
  - Foster new and reinforce existing knowledge and data
  - Develop new and strengthen existing capabilities
  - Develop new technologies and innovation
  - Foster research and technological excellence
  - Promote stronger partnerships between users and suppliers

- **Indicators**
  - Number of projects supported (disaggregated by theme)
  - Number of dissemination activities

- **Results (qualitative)**
  - Completion of RTD roadmapping exercises
  - Mapping of standards and development of pre-standards
  - Capability gap analysis
  - Feasibility assessments completed
  - Demonstration of proof of concept
  - Demonstration of technological solutions
  - Development of preindustrial prototypes
  - Improved Technology Watch capabilities

- **Impacts (qualitative)**
  - Improved knowledge and capabilities, technologies and innovation
  - Improved access to research excellence for end-users
  - Better understanding of user needs among providers
  - Wider availability of security products and services for users
  - Strengthened networking among (and between) EU Security research actors – large enterprises, SMEs, research centres, universities and users
  - Improved access for beneficiaries to national and EU Security Research funding
  - Commercialisation of research results and leveraging of IP

**Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research**

*Section 3*
The aim was to cross-check that PASR was drawn up in a way that reflected identified needs and was coherent with the policy framework at the time. Differences between PASR and FP7 Security Research were also examined. The main objective of PASR was to test the viability of the future fully-fledged European Security Research Programme introduced in FP7 SEC.

The results achieved through PASR anticipate those of FP7 SEC, but a key difference is the strong focus on mapping the expected achievements on early-stage R&D and testing and validating proof of concept and the feasibility of pursuing particular areas of Security Research. The intention was to lay the foundation for a full ESRP, with a concentration on support actions.

The average project size was relatively modest. The types of results anticipated include: the completion of roadmapping exercises, the identification / mapping of standards, capability gap analysis, the carrying out of feasibility assessments, the validation and demonstration of technological solutions and demonstration of proof of concept.

Another important outcome was the development of pre-norms in areas relating to standards and internationally interoperable systems. While some of these outcomes may also be relevant to FP7 SEC projects, given the small-scale, pilot nature of PASR projects, they are especially relevant. At this stage there was no specific indicator system. Nonetheless some quantitative results were certainly expected. The logic diagram for FP7 Security Research is presented on the following page:
Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research

Introduction, evaluation aims and methodology

Figure 3.2: Intervention Logic – FP7 Security Research

- Emerging threats and challenges – international terrorism, malevolent use of new technologies and ‘intelligent threats’ such as system-based cyber attacks
- Lack of national funding for security research in most EU countries
- Industry fragmentation
- Absence of harmonised standards and interoperability in some areas
- Absence of common testing and certification

FP7 Theme 10 Security (Cooperation Programme)
- Improve the security of European citizens
- Strengthen industrial competitiveness
- Foster state-of-the-art in Security Research
- Prevent fragmentation of research efforts

FP7 overall
- Promoting the EU to become the world’s leading research area
- Fostering world-class state-of-the-art
- Promotion of trans-national cooperation
- Fostering economic growth and employment through a knowledge economy
- Strengthening human potential in RTD in the EU

Core missions
- Security of citizens
- Security of infrastructure and utilities including networks
- Intelligent surveillance and border security
- Restoring security and safety in case of crisis

Cross-cutting missions
- Security systems integration, interconnectivity and interoperability
- Security and society
- Security research coordination and structuring

Specific objectives
- Strengthen competitiveness of EU civil security research industry
- Stimulate European market for new and emerging security products/systems
- Deliver mission-oriented research results to reduce security gaps
- Stimulate cooperation between providers and users of civil Security Solutions (Intra-EU and third countries and international organisations)
- Enhance national security research activities

Operational objectives
- Foster new and reinforce existing knowledge and data
- Develop new and strengthen existing capabilities
- Develop new technologies and innovation
- Foster research and technological excellence
- Promote stronger partnerships between users and suppliers

Outputs
- No. of projects supported
- No. of partners from third countries in project consortia
- No. of dissemination activities

Results indicators
- No. of patents / other forms of IP developed and registered
- No. of patents used
- No. of downstream applications
- No. of data sources / products/services/technologies developed
- No. of knowledge tools developed (e.g. databases, taxonomies)
- No. of research papers and research citations
- No. of commercial applications developed

Impacts
- No. of users taking up research outcomes
- Strengthened research excellence / state of the art
- Better understanding of user needs among providers
- Wider availability of ‘fit for purpose’ quality security products/services, technologies and data for users
- Strengthened networking and cooperation among EU Security research actors (and with 3rd countries and international organisations)
- Greater scope for revenue generation through commercialisation of research results/leveraging of IP
- Adoption of new standards by public agencies in different areas of security
- Greater interoperability of technologies, networks and systems
- Improved foresight capabilities to predict future security challenges and threats
- Enhanced security capabilities and reduction in gaps
- Better prevention, preparedness and response capacities
- Ultimately, improved security of EU citizens

Thematic areas
- Aviation security
- CBRN
- Crisis management (links with GMES)
- Critical infrastructure protection
- Land border (links with GMES)
- Maritime security
- Networked systems and interoperability

Global objectives
- Establishment of networks of security research suppliers and users

Specific objectives
- Promotion of new technologies and innovation
- Fostering new and reinforcing existing knowledge
- Fostering world-class state-of-the-art
- Fostering world-class state-of-the-art
- Establishing the European Research Area (ERA)
- Establishing and promoting the ERA

Opportunities
- New markets and growth opportunities
- Enhanced collaboration and partnerships
- Strengthened research and technological excellence
- Increased innovation and competitiveness
- Improved security and safety in case of crisis

Challenges
- Absence of common testing and certification
- Lack of standards and harmonisation
- Industry fragmentation
- Absence of common testing and certification
- Lack of national funding for security research in most EU countries

Intervention Logic

- Needs, problems
- Missions
- Operational objectives
- Outputs
- Results indicators
- Impacts
- Specific objectives
- Core missions
- Cross-cutting missions
- Global objectives

Intervention Logic

- Needs, problems
- Missions
- Operational objectives
- Outputs
- Results indicators
- Impacts
- Specific objectives
- Core missions
- Cross-cutting missions
- Global objectives

Intervention Logic

- Needs, problems
- Missions
- Operational objectives
- Outputs
- Results indicators
- Impacts
- Specific objectives
- Core missions
- Cross-cutting missions
- Global objectives

Intervention Logic

- Needs, problems
- Missions
- Operational objectives
- Outputs
- Results indicators
- Impacts
- Specific objectives
- Core missions
- Cross-cutting missions
- Global objectives
Evaluation results

The ‘intervention logic’ is a statement of the rationale for intervention supported by an EU programme and sets out what the programme is supposed to achieve, and how by outlining the causal relationship between aims and objectives, financial inputs and outcomes. At interim evaluation stage, this review helps to check whether the logic is working as intended, throughout the chain of causal relationships. In the logic diagram, the following elements are defined: a summary of problems that the programme is trying to address and of identified needs, the ‘hierarchy of objectives’ (what the Programme is seeking to achieve at different levels from a strategic to a more operational perspective), and illustrations of indicators of success\(^\text{28}\), quantitative and qualitative, at the level of outputs (immediate outcomes), results (intermediate outcomes) and impacts (longer-term outcomes).

At interim evaluation stage, an assessment is needed of the extent to which the needs and problems that FP7 Security Research is trying to address were, and remain relevant. The logic addresses the main threats and challenges identified in the European Security Strategy (December 2003), such as the emergence of new threats to the security of EU citizens linked to globalisation processes, including terrorism and vulnerabilities linked to malevolent use of technologies. These challenges have been addressed through the FP7 SEC Security Research calls launched to date and remain relevant.

Another problem identified in the needs analysis was the importance of strengthening the competitiveness of the European security research industry, given its fragmented nature, and the lack of critical mass in many areas. Safeguarding Europe’s economic well-being from new and emerging threats will require a strong European Security Research industry.

Another aspect of the rationale underpinning FP7 Security is the absence of national funding for security research in most EU countries. Only 8 EU countries fund national Security Research programmes (AT, DE, FI, FR, NL, RO, SE and the UK). Where funding is available, there is limited scope for transnational collaboration. In the context of the financial crisis, the availability of multiannual funding at EU level to provide strategic investment in security research fills an important gap.

The review of FP7 Security Research’s policy objectives starts at the global level and works down to the operational objectives that govern specific activities on the ground. The parts of the Programme Decision that relate to Security Research Theme 10 do not distinguish between general, specific and operational objectives. While the different levels of objectives are not stratified, this appears to be the case for all the themes supported within the FP7 programme.

A finding in relation to the annual work programmes is that while the Missions are well defined, and correspond to the programme’s global objectives, a coherent set of specific and operational objectives is currently missing. At the operational level, the objectives identified have been inferred from the aims set out in annual calls for proposals.

The following observations can be made in respect of the relevance of the Security Programme:

The global aims of the FP7 SEC programme remain highly relevant since the fundamental challenges are the same (even though their manifestations are evolving rapidly). Especially pertinent aims include: the security of citizens, strengthening industrial competitiveness to overcome fragmentation and the lack of critical mass in the security market, and the need to overcome difficulties faced by SMEs in entering the civil security market.

\(^\text{28}\) There is currently no indicator system in place, so these were developed to demonstrate the sort of outcomes that are expected to materialise following programme implementation.
Evaluation results

In order for the European security research industry to become globally competitive, and to respond effectively to emerging threats, it remains important that the programme continues to work towards fostering research and technological excellence and state of the art.

The need to address capability gaps also remains highly relevant. This was clear from both the results of the ESRIF forum, which developed a long-term strategy to address shortcomings in security research, and from the results of the interview programme. For example, about 120 capability gaps have been identified in the CBRN Action Plan, and according to interviewees from DG Justice, FP7 Security Research has the potential to address about 40 of these.

With regard to coherence, the programme’s mission-based approach provides a high-level framework and this was viewed as appropriate by interviewees. However, some modifications could perhaps be made. For example, the Security of Citizens is one of the ‘core Missions’. Since ultimately the security of EU citizens is at the heart of all interventions being supported, this could perhaps be reclassified as a cross-cutting theme.

Nevertheless, it is clear that the thematic dimension within the programme has been progressively strengthened during FP7 SEC, both in comparison with PASR, and over successive FP7 Security calls for proposals. In the 2007 call, the thematic areas of intervention were not clearly set out. However, in subsequent calls in 2009, 2010 and 2011 respectively, there is greater clarity in the work programmes about which thematic areas will be prioritised through calls.

While recognising that the Commission’s intention was to avoid being too prescriptive about which thematic areas would receive support because technologies may have applicability across a number of themes, an overview of the most common areas of intervention would help to better communicate the aims and objectives of FP7 Security to external stakeholders.

The types of thematic interventions being supported, such as aviation security, maritime security, the protection of mass transit systems, CBRN and crisis management and emergency response are of direct relevance to the security of EU citizens. Since some threats are more visible to the general public than others, such as attempted terrorist attacks on airlines and actual terrorist attacks on mass transportation systems in the UK and Spain mean that the programme has already begun to address civil security protection issues of widespread concern to EU citizens, who are the ultimate beneficiaries of security research.

Likewise, in the maritime security field, for example, technology to improve the early detection of illegal immigration by sea in southern Europe helps to directly address some of the security concerns of EU citizens both in relation to illegal immigration and in improving humanitarian assistance for victims of people trafficking.

Since FP7 SEC was adopted, various policy Communications have been issued across different areas of the Commission in areas such as aviation security and crisis management. This has led to improvements in the thematic coherence of annual work programmes, with a better explanation about the underlying policy rationale for the selection of research topics prioritised in calls.

An important task was to assess whether the anticipated causal chain when the programme was set up is working as expected. The analysis found that there are clear linkages between the identification of problems and needs, and the definition of the FP7 SEC programme’s objectives (notwithstanding the absence of a sufficiently detailed set of operational objectives) and the types of activities
supported. However, at present, the programme lacks a coherent set of indicators and a monitoring system to assess project achievements.

At the level of outcomes, a distinction is made between financial inputs, and the effects materialising over different time periods: outputs, results and outcomes. Overall, it can be concluded that:

Table 3.1: Conclusions – intervention logic

- The programme logic is ‘fit for purpose’ and reflects the identified needs of the security research industry and also of European citizens.
- It is coherent with the policy framework at the time the pilot and the fully-fledged ESRP was drawn up;
- There is continuity between PASR and FP7 SEC in terms of the rationale for intervention, with some minor differences (PASR focused more strongly on undertaking preparatory measures to pave the way for larger-scale projects in FP7, e.g. development of pre-standards, and validating and demonstrating proof of concept and the feasibility of new approaches and technologies;
- Nonetheless, it would help in the clear communication of the purpose and direction of the Programme if, as well as an explanation of the aims of the Security research there were explicit statements of objectives at the global, specific and operational levels.
- The logic for FP7 SEC would be strengthened through the implementation of an indicator system and monitoring framework so as to better assess the achievements of the programme on an on-going basis.
- There is a strong focus on strengthening cooperation with third countries in FP7 SEC compared with PASR, which was confined to EU25; and
- Looking ahead, the logic model will need to be reviewed in planning for FP8 and perhaps modified to reflect the evolving policy and legal context, such as the greater potential to strengthen the external dimension of security research activities.

3.2 Indicators and monitoring framework

CSES examined the issues involved in setting up a monitoring framework for FP7 Security research. Currently, there is no indicator system in place. An annexed working paper (see Appendix E) provides an account of the issues to be taken into account and the conclusions on the type of quantitative indicators suitable for a monitoring system. A summary of the issues is provided here.

Indicators are needed for internal management purposes, both within DG ENTR and in relation to DG Research’s overall management and reporting on FP7. They are also needed for external communication, reporting and accountability. Any indicator system developed also has to be consistent with existing Commission frameworks, particularly the relevant core result indicators in DG ENTR’s annual Management Plan and the framework for indicators and monitoring in FP7 that is being developed by DG Research.

Monitoring procedures and the use of indicators have been subject to considerable discussion within the general FP context in recent years. The Report on ‘Tools and Indicators for Community Research Evaluation and Monitoring’ published in July 2009 provides a useful resume of many of the elements of this debate and also provides the basis for specific recommendations. The paper on indicators proposes an adaptation that could apply to Security research.

Evaluation results

However, responding to the concerns of the Security unit, the evaluation team focused on monitoring arrangements that could build on reporting procedures for projects. A selection was therefore made to focus on those based on information from beneficiaries. Put another way, sets of indicators were developed on the basis of the question: ‘what information relating to the performance of the Programme should be required from participants in project reports?’ Here a distinction was made between information necessary for a final assessment of the Programme’s achievements and indicators that can be used at an earlier stage for monitoring progress.

In formulating longer-term performance and shorter-term monitoring indicators, account was also taken of the views of project participants. Details are available in the Indicators Paper, but a contrast emerged between what could be used to judge the success of projects and the information that participants are able to provide. This fed into the distinction between data for final assessment and monitoring indicators. The indicators proposed for consideration are as follows:

**Table 3.2: Project-level monitoring indicators – results and impacts**

<table>
<thead>
<tr>
<th>Results</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of patents registered/ other forms of IP registered</td>
<td>No. of end-users (making use of research outcomes)</td>
</tr>
<tr>
<td>No. of patents used within projects</td>
<td>Revenue generated through IP licensing arising from the project</td>
</tr>
<tr>
<td>No. of new data sources</td>
<td></td>
</tr>
<tr>
<td>No. of new products developed (including prototypes)</td>
<td></td>
</tr>
<tr>
<td>No. of services developed</td>
<td></td>
</tr>
<tr>
<td>No. of technologies developed</td>
<td></td>
</tr>
<tr>
<td>No. of knowledge tools developed (e.g. good practice guides, taxonomies)</td>
<td></td>
</tr>
<tr>
<td>No. of research papers published</td>
<td></td>
</tr>
<tr>
<td>No. of research citations (<em>measure of bibliometric excellence</em>)</td>
<td></td>
</tr>
<tr>
<td>No. of commercial applications developed</td>
<td></td>
</tr>
<tr>
<td>No. of secure information networks set up</td>
<td></td>
</tr>
<tr>
<td>No. of cooperation networks established (i) among users (ii) among wider security research stakeholders</td>
<td></td>
</tr>
<tr>
<td>No. of projects in which proof of concept has been successfully demonstrated</td>
<td></td>
</tr>
<tr>
<td>No. of standards developed</td>
<td></td>
</tr>
</tbody>
</table>

The idea is that project managers will be asked to report on the corresponding details relating to their own projects on a systematic basis and in a standard form, in order to facilitate comparison and aggregation of the monitoring data.

It should be noted that the current list focuses on core project outcomes. It may be that eventually a broader range of economic, social and environmental outcomes could be of interest. Most of these indicators also relate to information that is significant for the ultimate evaluation of programme...
performance. However, because there will often be delays in observing the effects reported on, there is a need for a more reliable indication of the progress over a shorter time period.

The basic performance data was therefore refined, both to derive a more concise set of indicators and also to allow the indicators to be useful at an earlier stage of the Programme’s implementation:

**Table 3.3: Indicators – implementation issues**

<table>
<thead>
<tr>
<th>Indicator</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of research citations (bibliometric excellence indicator)</td>
<td></td>
</tr>
<tr>
<td>Scientific collaboration indicator - co-authorships by participants</td>
<td></td>
</tr>
<tr>
<td>Number of new products</td>
<td></td>
</tr>
<tr>
<td>Number of technologies with clear improvements</td>
<td></td>
</tr>
<tr>
<td>Number of downstream application areas opened up</td>
<td></td>
</tr>
<tr>
<td>No. of patents used</td>
<td></td>
</tr>
<tr>
<td>Contributions to standardisation processes</td>
<td></td>
</tr>
<tr>
<td>No. of users (making use of research outcomes)</td>
<td></td>
</tr>
<tr>
<td>Revenue generated through IP licensing arising from the project</td>
<td></td>
</tr>
</tbody>
</table>

The development of evaluation and monitoring techniques is a continuous process and the indicators proposed above will need to be developed further, though this could be done over a relatively short period. Further work will need to include consultation with project participants, given that most of the data at this level will be derived from project reports. Furthermore, if they are adopted, they will continue to need revision and updating, to the extent that this is compatible with a consistent and stable approach to the setting of objectives and targets. However, it is already possible to see how they could be operationalised, especially given that they would also encourage desirable project outcomes and practices, such as standard development or more consistent IPR management.

Collecting information on indicators will add considerably to the evidence base on the direct effects of projects and it is proposed that this should happen on a systematic basis. The advantages in terms of better policy management will help to promote transparency in the grant system. It should be remembered, however, that indicators are not the whole picture. They are meant to give an indication that an area appears to be going well or alternatively might need early investigation. However, they will undoubtedly make a significant contribution to the more systematic assessment of support for security research that is developing over time.

### 3.3 Effectiveness of programme management and implementation

In this sub-section, an assessment of the efficiency and effectiveness of programme management and implementation is provided (factual aspects relating to the role of the Commission and the REA respectively were set out in Section 2.3).

#### 3.3.1 Management of PASR

Overall, the research found that the management, implementation and monitoring of PASR was well handled. Among the findings were that the application process was clear to understand, and that project officers followed projects closely as part of their monitoring responsibilities and had a good understanding and knowledge about project aims and activities taking place. They were also found to have scrutinised the technical details of projects relatively closely.
Evaluation results

Guidance for applicants in PASR calls was regarded as user-friendly and easy to understand. A seminar organised by the Commission devoted to audit procedures was organised, which was viewed as having been very helpful. The evaluation process from application submission through to initial project selection was relatively short compared with FP7, reflecting the relatively small size of the preparatory action. The contract negotiation process from selection to contracting varied in length, but was typically from 3 – 6 months. The timescales for both the project selection process and the length of contract negotiations was regarded as broadly satisfactory by project participants.

Delays were encountered in contracting on a small number of PASR projects. This was sometimes due to requests for additional administrative information, which had to be collected from all partners and took time for lead coordinators to gather, especially for projects with larger number of partners. One interviewee commented that: ‘Delays were unhelpful in implementing the project efficiently. By the time the project started, some staff had changed post, and there were resource planning complications, and a difficulty in keeping all partners sufficiently focused on project objectives’.

Some areas where there was scope for improvement were identified. One comment was that the funding scheme concerning whether and how non-coordinators may claim management costs was not clearly defined. Another participant stated that there had been difficulties at application stage in ‘identifying the relative cost model to be followed’.

Overall, beneficiaries were satisfied with the management of PASR. For example, a partner involved in the Isotrex project commented that ‘Contracting procedures were well managed and we had strong managerial and technical support from a Commission scientific officer and his support’.

3.3.2 Programme Management

The handover process from DG ENTR to the REA in 2009 and the transition of responsibility for day to day programme management has been well managed, although there were managerial and organisational challenges in transferring responsibility midway through the programme’s implementation. Interviewees were broadly positive about both the Commission and REA’s handling of programme management and the way in which the launch of Calls for Proposals and the selection, evaluation and negotiation process have been managed.

A small number of projects (<5) mentioned challenges linked to the change in project officer midway through project implementation, but given that the organisational handover to the REA took place in 2009, two and a half years into the programme, this was unavoidable, and needs to be kept in perspective. The Executive Agency has made substantial progress in developing the resource capabilities to manage programme implementation. REA Technical Project Officers (POs) were found to be highly qualified with a strong scientific background and relevant technical expertise. Moreover, many POs previously worked for the European Commission in project managing research projects. Monitoring is arranged in such a way that Technical POs are able to specialise in project monitoring in areas that are appropriate to their background and experience. The combination of Technical POs, Legal and Financial Officers working together within the same unit was found to be efficient.

Interviews with a sample of REA Technical POs were undertaken and a key finding was that REA POs are highly qualified, with a strong technical background. Several POs had PhDs in different areas of science and others have an engineering background. There was also strong expertise in particular areas in which projects are being supported, such as ICT and cyber security.
Evaluation results

The decision to retain demonstration projects and sensitive projects which include classified information at the European Commission seems appropriate. Given the potential of the demonstration projects to become programme flagships, there is a need to evaluate the effectiveness of these strategically important undertakings. While the REA might be able to fulfil this task in future, especially if staff numbers increase, it would appear appropriate to retain, for the time being, some monitoring functions at the Commission. With regard to classified projects, the Commission has secure information sharing facilities.

The fact that the text of annual work programmes is set out in the annual PASR and FP7 Security Research work programmes was viewed positively by beneficiaries. This allows time for potential applicants to prepare their application and to form a consortium well in advance of the formal call launch. Indicative timings of the publication of calls were also indicated in annual work programmes, facilitating preparation for applicants. The call for proposals is then open for several months, which again means that there is more than adequate time to find partners and to generate project ideas.

Beneficiaries were asked about their perceptions of the management of calls for proposals and contracting arrangements for FP7 SEC. The results are shown in the table below:

**Table 3.4 How well have contracting procedures been managed by the Commission?**

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very well</td>
<td>20</td>
<td>27.8</td>
</tr>
<tr>
<td>Quite well</td>
<td>41</td>
<td>56.9</td>
</tr>
<tr>
<td>Not well</td>
<td>8</td>
<td>11.1</td>
</tr>
<tr>
<td>Not at all well</td>
<td>1</td>
<td>1.4</td>
</tr>
<tr>
<td>No response</td>
<td>2</td>
<td>2.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>72</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Among the strengths identified include: reliable timing of the launch of calls for proposals, allowing for more effective planning; user-friendly guidance for applicants; the clear setting of security research objectives in calls, the topics were understandable to prospective beneficiaries; and the opportunity for beneficiaries to obtain general advice and feedback on project ideas from the Commission and subsequently the REA before applications are submitted. The main weakness was longer Time to Grant compared with other areas within FP7. Statistics on TtG (Section 2.3) showed that TtG was on average 530 days in the 3rd call, the longest within FP7. This problem is not confined to FP7 SEC and is a problem common to other themes within the Cooperation Programme.

Beneficiaries expressed concerns about the long contracting processes. For example, an organisation involved in the ADABTs project stated that ‘during the time it took to go through the scrutiny process, there was turnover in the responsible project officers at the Commission. Additionally, because of the timeframe taken to grant award, there was also turnover in project managers within the consortium itself. This meant having to repeat information, and to establish new channels of communication’. A partner organisation in INDECT commented that ‘The duration of the process from selection through

---

30 Time to grant is measured in the number of days between call closure and the signature of the GA were benchmarked for FP7 overall.
31 DG RTD’s Third FP7 Monitoring Report (July 2010, focusing on the 2009 period of implementation)
to contracting was 1.5 years. This was longer than expectations and it would be helpful if the process could be accelerated’.

Factors specific to FP7 Security that add to the TtG were explained in section 2.3. In summary, these include i) the security scrutiny procedure for sensitive projects that incorporate classified information, and ii) ethical screening. Although an effort is made to carry out these processes in parallel rather than sequentially, the scrutiny procedure can add 2-5 months to TtG. It should also be stressed that the REA, DG ENTR and all other research DGs must respect the rules and procedures laid out in the EU Financial Regulation. The administrative and financial validation of all partners, while necessary, is time consuming. There is an inherent tension between the need to ensure sound financial management of EU funds and to reduce TtG on the other.

Some beneficiaries were used to relatively long contracting timescales from previous experience of other themes within FP6 and FP7. However, other stakeholders, particularly SMEs and industry, stated that timescales were too long and more appropriate for basic research than near-market applications. The speed of bringing applications to market can be critical to their eventual commercial success. Among the points raised by large companies was that delays in contracting means that they may be unable to utilise their staff effectively. Once the initial decision to enter the negotiation phase has been taken by the Commission, one large company commented that ‘we then mobilised resources for project implementation and could not let the staff involved in the project bid to commence any other long-term projects’.

For SMEs, any delay in projects getting underway was seen as potentially having an adverse impact on cashflow planning. In at least one case, a project led by an SME had to start before the signature of the grant agreement as the leading SME preferred to take the risk of starting the project than losing key staff. Universities and research laboratories also face staffing issues in planning for FP7 SEC projects without certainty about the timing of GA awards.

Delays can also make it more difficult for project partners to engage with end-users. They may be reluctant to commit to get involved in projects if there is uncertainty about when projects will get underway, and the timing of any inputs required, for example, to assist in defining user requirements, take part in scenario modelling exercises, etc. Given the fast changing nature of security issues, users may increasingly demand much shorter R&D lead times from suppliers involved in the development of user-oriented security solutions and technologies. The larger the consortium, the longer it can take to complete the legal and financial validation process of each partner.

Some beneficiaries stated that delays were also due to consortium-related issues, for example, the IMSK project experienced delays due to the time taken for the scrutiny of legal documentation by large firms in the project. This can be complex, especially when one or more partners are contributing proprietary technologies and IT platforms into the project.

Shortening contracting lead times is already a key priority for the Commission and REA. However, while there is some scope to shorten lead times, for example, through further improvements in tailoring ICT systems to help maximise the efficiency of the contracting and negotiation phase, the process cannot presently be shortened significantly, because of the time lag resulting from the security scrutiny procedure, the ethical review process and the legal and financial validation process of all partners in projects which is a requirement in the EU Financial Regulation. These delays heighten
the risk of a partner or partners pulling out of a shortlisted proposal, a development which can in itself produce further knock-on delays.

With regard to the role of National Contact Points, NCPs provide basic information and advice and signpost to further information sources. Sometimes they also play a more specialised role in providing training sessions on financial and legal issues, IPR management, etc. Beneficiaries were asked whether they had had any contact with their NCP.

Table 3.5: In applying for funding, did you make contact with the National Contact Point (NCP)?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>27</td>
<td>37.5</td>
</tr>
<tr>
<td>No</td>
<td>43</td>
<td>59.7</td>
</tr>
<tr>
<td>No response</td>
<td>2</td>
<td>2.8</td>
</tr>
<tr>
<td>Total</td>
<td>72</td>
<td>100.0</td>
</tr>
</tbody>
</table>

More than one-third of beneficiaries in FP7 SEC have had at least some contact with their NCP, although the NCP was often not the source from which they found out about the availability of funding. The role and value added of NCPs was discussed through the interviews. Examples of activities undertaken by NCPs are provided below:

Table 3.6: Examples of activities undertaken by NCPs

In Greece, the NCP (HELP-FORWARD) organised information days for each new call for proposals with the participation of guest speakers from DG ENTR and national representatives. Customised assistance was also provided by phone and by email and meetings have been held with potential participants from the industrial and research community. The Greek NCP keeps records of queries received and the types of services provided maintained using a CRM system. In Greece, the Space and Security priorities accounted for the 2nd highest number of enquiries after the NMP priority.

The Greek NCP estimated that about 15% of their time spent on FP7 SEC related to forthcoming calls, 60% on current calls and 25% on follow up activities once calls had been closed and projects have been provisionally selected and are in the negotiation phase.

The UK NCP holds an information day once a year, with attendance of around 150 people from industry, academic institutions and wider stakeholders. This provides practical advice and information about how to apply to take part, the mechanics of the evaluation process, key research topics, etc. An issue raised was that of dissemination. There is no newsletter or page on the Home Office website about FP7 SEC, although calls and related information are posted on the Technology Strategy Board website along with information about national research funding. The UK NCP also discusses participation directly with potential candidates and receives enquiries by email. Information is circulated indirectly, and there are sometimes meetings at universities on FP7 generally, which NCP representatives are asked to attend. The main questions raised in enquiries relate to the research priorities, funding availability and co-financing, and how to form consortia.

Among the findings were that the level of activity by NCPs in relation to FP7 SEC and the level of cooperation between NCPs varies considerably. Some NCPs saw their role as being reactive – assisting with enquiries rather than going out and promoting the programme. This is reflected in the low proportion of total working time (approximately 10-20%) that some NCPs spend on programme promotion and in providing advice to potential and current beneficiaries. Overall, NCPs were found to have successfully raised awareness and responded effectively to enquiries from prospective and actual beneficiaries. However, there remains an ongoing need to strengthen coordination and
cooperation between NCPs. Stronger networking efforts would encourage information exchange and the sharing of experiences, thus assisting in particular those NCPs new to their role.

### 3.3.3 Evaluation and selection process - FP7 SEC

Among the findings were that the evaluation and selection process overall works well, with evidence that high quality projects have been selected. Another finding was that it was appropriate to base the selection procedures for FP7 SEC on wider DG RTD procedures already in place that have evolved over successive Framework Programmes. This helped to avoid reinventing the wheel. Since the outset of the programme, some modifications have been made to the procedures for evaluating proposals, in particular, the transition to ‘remote evaluation’. Originally, projects were assessed by evaluators physically present with hard copy versions of applications. Now, proposals are reviewed by independent evaluators separately who receive a copy of the proposal electronically.

Remote evaluation was viewed as having improved efficiency, without undermining the quality of the application screening and evaluation process. Evaluators are still called to Brussels for the consensus meeting, and for projects that are sensitive and involve classified information. The external evaluators receive appropriate training on how the detailed evaluation process should be carried out.

Other questions relating to the evaluation and selection process include the extent to which beneficiaries found the application process user-friendly. Overall, most beneficiaries felt that the application process had run smoothly, although some larger consortia were concerned about the amount of administrative and financial information that has to be collected from partners (this cannot be avoided however, unless there are changes to the EU Financial Regulation). Guidance for applicants was viewed as useful and detailed, however it was pointed out that a shorter guidance document could be produced for SMEs and end-users containing simplified information. Public entities potentially interested in taking part in FP7 SEC have very little time and it would help to secure their participation if there were a simplified procedure for them to take part in the programme.

### 3.3.4 Project monitoring and closure

Views on how well project monitoring has worked at the project level were also ascertained through the survey work. The results were positive, with 26.4% stating that this had worked ‘very well’ and a further 62.5% ‘quite well’. Only 6.9% said that project monitoring had not worked well.

**Table 3.7: How well has project monitoring been carried out by your consortium?**

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very well</td>
<td>19</td>
<td>26.4</td>
</tr>
<tr>
<td>Quite well</td>
<td>45</td>
<td>62.5</td>
</tr>
<tr>
<td>Not well</td>
<td>5</td>
<td>6.9</td>
</tr>
<tr>
<td>Not at all well</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>No response</td>
<td>3</td>
<td>4.2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>72</td>
<td>100.0</td>
</tr>
</tbody>
</table>

---

32 The *Rules for the submission of proposals, and related evaluation, selection and award procedures* sets out a rigorous approach to the evaluation and selection process applicable across all thematic areas within FP7
Evaluation results

With regard to the effectiveness of monitoring arrangements generally, applicants must produce periodic and final monitoring reports. A small sample of monitoring reports was analysed, and the quality of these was found to be high. These provide useful information summarising what activities have taken place, the extent of involvement of users and the research results achieved. Project beneficiaries are also required to produce a publishable summary of their project’s achievements and potential impact in future. While this is useful, sometimes, the approach adopted to describing project achievements was not always clear and could be further standardised. There is also a need to disseminate these summaries more widely.

An effort could also be made to simplify reporting requirements for projects involving a significant number of public end-users, since many users attested to their limited time availability, and said that they were concerned about their capacity to fulfil EU project management and reporting requirements without taking on more dedicated staff to deal with project management.

3.3.5 Annual Work Programmes and Calls for Proposals

CSES undertook an appraisal of the content of the Security Research annual work programmes under both PASR and FP7 SEC. These contain the text of Calls for Proposals.

PASR had 3 annual work programmes in the 2004-2006 period, and 5 main research topics: Improving situation awareness; Optimising security and protection of networked systems; Protecting against terrorism; Enhancing Crisis Management and Interoperability and integrated systems for ICT. The more detailed research topics mentioned in PASR calls were broad in scope and purposefully not that prescriptive in their description of activities to be supported. Reflecting the experimental nature of a preparatory action, the intention was to encourage a wide variety of project applications.

Notwithstanding, while PASR projects achieved many positive outcomes, and while there is strong evidence of continuity in FP7 SEC, the work programme would have been more coherent if it had included a clear description of the aims, types of activities and thematic areas from which project applications would be welcome, along with a short overview of expected impacts.

The coherence of the FP7 Security annual Work Programmes were found to have improved over time. The 2009, 2010 and 2011 work programmes provide clearer topic descriptions and a stronger thematic focus than the 2007 work programme, for example. While ‘expected impacts’ were set out at the activity level, in 2007, these were only described for a small number of topics. In subsequent Calls, there has been an effort to standardise the presentation of topics. Under each topic, a description is provided of the technical content / scope, the funding scheme concerned and the expected impact. Information about the thematic priorities in FP7 SEC was less prominent in the 2007 and 2009 work programmes, but was strengthened in 2010 and 2011. Explicit mention of thematic areas such as aviation security, maritime security etc. was more meaningful to beneficiaries and the wider public than the concept of ‘missions’, since these are quite high-level.

While each Work Programme included a short overview of the policy context and rationale of the FP7 SEC programme, it may be helpful in future to provide a summary of the aims which distinguishes between general, specific and operational objectives. The precise configuration of these objectives should be determined by the Security Research Unit (working in conjunction with the Programme Security Committee). This would make it conceptually clearer what FP7 SEC is trying to achieve at different levels.
Evaluation results

It is appropriate that annual SEC Calls for Proposals include a description of indicative priorities for future calls, together with a roadmap outlining the approximate timing. This enables potential beneficiaries to prepare their application well in advance, develop project proposal ideas, and undertake partner identification/consortium formulation.

3.4 Thematic aspects of Security Research

A number of themes have been supported through EU Security Research both in the PASR Preparatory Action and FP7 Security Research. These include: Aviation security; CBRN; crisis management / emergency response; critical infrastructure protection; land border and maritime security and networked systems, interconnectivity and interoperability. During Phase 1 of this evaluation project, it was agreed with DG ENTR that 5 case studies would be produced on the following topics: (1) Aviation security, (2) CBRN, (3) Crisis management / emergency response and (4) Maritime security. Given the focus in EU Security Research on promoting SME participation, the fifth case focused on SMEs.

The case studies have been produced as separate standalone documents (see Appendix H) and include detailed project examples based on the selection of a representative sample of PASR and FP7 SEC projects. A short synopsis of the findings from the 4 thematic cases is now provided:

CBRN

In the CBRN field, a number of projects have been supported which helped the EU to better prevent, prepare and respond to malevolent CBRN attacks. A number of projects were examined in the case study including FESTOS, Watersafe, CREATIF, LOTUS, BODE, BIO3R, HAMLeT, COCAE, FRESP, TIARA. Projects focusing on preventing CBRN attacks were carefully selected to include the development of regulatory measures for dual-use and precursor CBRN materials. Prevention phase projects also emphasised establishing new databases with secure interfaces for the collection and collation of operational intelligence and biological pathogens among law enforcement agencies. State-of-the-art modelling platforms were created with a greater capacity for first responder inputs. For example, significant scenario mapping was carried out under the IMPACT project, which provided the ground work for a European doctrine for first responders to CBRN incidents.

Projects in the area of preparedness were primarily focused on the mobility and robustness of devices to detect CBRN materials at various distances. One of the problems addressed by CBRN projects was the lack of functionality and interoperability of existing detection and scanning devices available on the market. Part of PASR research looked at ways in which cutting edge technologies could transform the reliability and sensitivity of detectors (e.g. Watersafe developed nanotechnologies to provide early warning of toxicity in the water supply). While a number of FP7 projects focused on improving standoff detection capacity, including the LOTUS project which enables moving vehicles to detect airborne chemical and biological agents, time and location stamp the source and alert relevant security agencies through a secure communication structure.

Responding to CBRN attacks requires strong coordination among first responders in order to mitigate the worst affects to society and critical public infrastructure. Emergency services need durable personal protective equipment that is flexible enough for close inspection units to attend to casualties and carry out monitoring and remediation activities. This requires both long term research into nanomaterials and the creation of guidelines for manufactures to ensure first responders remain protected during the decontamination stage. There is also a need to consider the societal impacts of CBRN events in terms of analysing how people respond and react in crisis situations.
Evaluation results

A number of projects addressed such issues. For example, the **TIARA project** provided training to doctors in procedures for dealing with the aftermath of a radiological dispersal device (‘Dirty Bomb’), which included triage conditions for victims of radiological exposure. The role of human psychology was addressed by the **BeSeCu project**, which tested emergency evacuations in a wide range of Member States and third countries to assess whether individuals behave differently depending on their particular cultural backgrounds. Many of the project results achieved under PASR have been followed up on in FP7, especially for research with high potential of commercialisation (e.g. terahertz screening technology under the TERASEC project).

In terms of achievements in the CBRN field, some projects contributed towards fostering state of the art, for example, the **COCAE project** has developed cutting-edge technology using Cd(zn)te crystals to improve the reliability of handheld radiological detection devices with deployment potential at land borders. Another example was the FRESP project which utilised advances in the design of nanoporous adsorbent materials to develop a respiratory system for first responders. The product can protect against both chemical warfare agents and toxic industrial chemicals without losing capacity.

Other important steps forward include the setting up of a network of CBRN testing laboratories to promote the development of common testing and certification processes and a mapping exercise to account for existing procedures, equipment standards and certification processes in the civilian and military sphere. The **CREATIF project** identified the lack of recognised testing and certification facilities in the civil security sector as a major barrier to the commercialisation of SME products. The project made an important contribution towards the competitiveness of EU security markets, by demonstrating the viability of a European security label for detection products.

CBRN projects provided research coverage for areas in which national security programmes have not fully penetrated. Equally, some of the technologies developed to detect, monitor and assess CBRN materials were advanced by the emphasis certain projects placed on interoperability and building networking capacity. It is also likely that regulatory actions to standardise procurement and security evaluation procedures will lead to greater take up of CBRN results and outcomes.

Soft outcomes include the development of cross-border cooperation structures between end-users such as intelligence agencies and emergency services as well as civilian and military end-users. A significant soft outcome was the improved efficiency among first responders as a result of increased joint training exercises. Some projects were able to build higher levels of trust among key stakeholders which led to greater information sharing in areas where strong limitations were previously applied (e.g. CBRN detection device testing and certification facilities).

**Aviation security**

The case study showed that a number of projects have been supported in the area of **aviation security**. Research has been undertaken in the following areas: protection of critical infrastructure (airports), improved detection systems, surveillance and monitoring of people and luggage in airports, and the protection of airborne aircraft. A number of projects were examined in the case study including EFFISEC, PATIN, iDetecT4ALL, TERASEC, ISOTREX, Samurai, SUBITO, ISCAPS, PALMA.

A key aim of aviation security systems relating to the protection of airport infrastructure is to control people moving in or out of protected areas, such as physical buildings, sensitive areas within airport terminals and information systems through the use of surveillance and monitoring systems. Surveillance is central to airport security management and takes place through a number of means,
Evaluation results

from video surveillance to the use of biometric tools to check the identity of airport workers with secure access rights.

**PATIN** developed a system for protecting air transportation systems against terrorist attacks, including airport concourses, aircraft, critical ground infrastructure and ICT installations. Other projects such as **EFFISEC** made use of biometric technologies to allow faster and more accurate identification of personal documents at borders and checkpoints. Biometrics includes technologies that can be used to verify identity by analysing individual characteristics and personal attributes. The main types of biometric data include fingerprints, face recognition, iris recognition, and vascular recognition.

Some PASR and FP7 Security projects have focused on the development of new technologies to strengthen the effectiveness of screening and detection equipment. Such equipment is used to search persons and luggage in order to detect the presence of unauthorised persons, goods, explosives and CBRN. Luggage is currently checked by X-ray machines, but X-ray is difficult to apply when scanning people due to radiation safety issues, which are covered by specific regulations. Furthermore, current procedures rely on a visual identification of suspicious material on the part of staff operating the X-ray machines. The **TERASEC project** (also see CBRN) demonstrated that terahertz frequency radio waves can be developed as an alternative to existing scanner technology.

Terrorists carrying or wearing hidden explosives can be identified through the detection of chemical precursors in the form of airborne particles or minute traces dispersed on packing surfaces or attached to clothing. The problem is that there is a wide of scope for improvement in discriminating between substances, in detecting low-level traces and in the facility with which the detection mechanisms can be deployed. The **ISOTREX project** developed fast screening sensors using advanced laser technology to carry out rapid stand-off detection at airports.

In light of terrorist threats at airports, there is heightened awareness about the need for high quality video surveillance to monitor people and luggage in airports. Presently airports deploy 24 hour static, networked Pan-Tilt-Zoom (PTZ) CCTV. Most CCTV systems are controlled manually by operators on an ad-hoc basis rather than by automated systems that allow for ‘on-the-fly’ decision-making, which is needed to reduce false alarms. **SAMURAI** (Suspicious and abnormal behaviour monitoring using a network) has developed a sophisticated algorithm to identify, monitor and track people with luggage between different locations in airports and other public infrastructure. The project raises issues around the ethical and societal dimension in that there is a need to reassure the public about the way in which suspicious behaviour will be defined.

There is a threat in some parts of the world from attacks by MANPADs (Man-Portable Air Defence Systems). While in Europe, there have not to date been any recorded MANPADs attacks, the possibility of such attacks in future cannot be discounted. While MANPAD’s have not been a major priority in FP7 SEC, during PASR, the **PALMA** and **PATIN projects** identified functional and operational requirements, provided technological analysis, conducted experimental investigations and made recommendations for future research in this area.

With regard to achievements, these include the development of state of the art in the area of detection equipment, and the development of prototypes for new generation surveillance technologies to protect airport infrastructure using intelligent video-surveillance software. Such technology has strong deployment potential, since it is capable of identifying and tracking individuals that act suspiciously in crowded public spaces using algorithms to profile people's behaviour.
Evaluation results

The case study research on maritime security examined a number of projects. These included under PASR SOBCAH (Surveillance of Border Coastlines and Harbours) and SECCONDD (Secure Container Data Service Standardisation). A number of further projects in the maritime field supported during FP7 SEC were also examined. These include: Sectronic (Security System for Maritime Infrastructure, Ports and Coastal Zones), UNCOSS (Underwater Coastal Sea Surveillance), b (Interoperable Approach to the EU’s maritime security management) and WIMAAS (Wide Maritime Area Airborne Surveillance).

Among the priorities in the area of maritime security in the PASR calls in 2004, 2005 and 2006 were the demonstration of concepts and technologies in general border surveillance and relating to the tracking and tracing of persons, goods and assets. The PASR calls promoted the development of sensor technology. Furthermore, in 2006, PASR encouraged projects involving the development and demonstrations of novel concepts and technologies for locating illegal immigrants at EU borders.

As far as key achievements are concerned, PASR provided support for the SOBCAH project to improve the Surveillance of Border Coastlines and Harbors. The project was seen as successful in identifying gaps in systems capabilities to carry out effective surveillance and in mapping the range of possible technological solutions to address those gaps. The project also sought to test the use of sensors and data fusion to improve situation awareness for users. From a user perspective, the SOBCAH project promoted the integration of data and the interoperability of systems and raised awareness about the need for improved coordination in sea-based surveillance. Users of different technologies have been encouraged to pool their operational know-how so as to improve the overall standards of surveillance systems.

FP7 2007 also promoted the development of port area security systems with the aim of creating an integrated port area (i.e. land, sub-surface, water). improving situation awareness in maritime areas this time through the development of integrated novel surveillance technologies (i.e. covering land, sea, air and space) combining tracking and tracing sensor devices with sophisticated data management and data fusion processes.

A key finding was that compared with other areas within FP7 SEC, there will be a considerable time lag before many of the planned research outcomes can be operationalised by users. The reason for this is that in the maritime security field, the intention is to develop large-scale demonstrators in areas such as wide area maritime surveillance (which requires linking up networks of sea-based sensors with GMES and spatial technologies). To make progress in this area will therefore demand long-term commitment to research funding, given that many of the technologies and systems integration expertise required are new and will require considerable time to research, develop and operationalise.

Another positive finding was that many projects have been working closely with users, including coastguards, port authorities and customs and excise. Examples of projects interviewed that are actively involving users include the AMASS project (Autonomous Maritime Surveillance System). AMASS is seeking to develop the technology to find new algorithms able to detect abnormal vessel behavior from the common intelligent operational traffic picture. The project has two users, AFM (the Maltese Armed Forces) and ICCM (Instituto Canario de Ciencias Marinas). Tests at the end of the project will be carried out under realistic conditions in the territorial waters of both Malta and the Canary Islands in Spain. Both countries have been highly affected by illegal immigration and there is a need to improve surveillance in order to improve early detection of illegal boat entry to the EU.

The UNCOSS project (Underwater Coastal Sea Surveyor) has also succeeded in attracting the attention of users, such as the Vukovar Port Authority in Croatia which has helped to test the prototype.
Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research

Evaluation results

However, this project, in common with others in the area of maritime security, will only see the research outcomes fully realized over a longer timeframe. The project requires considerable technological input which is being led by research bodies with wide expertise in maritime security. The introduction of the technology to end-users for operational purposes is likely to take quite some time.

Overall, while progress has been made, there is a need for long-term investment going forwards to help realise the integration of maritime border control systems, and to address the need for greater interoperability between space-based surveillance of maritime traffic and the application of sea-based sensor technologies as part of a wide-area based approach to maritime surveillance. The technological challenges are such that the real achievements will be manifested over a 10-15 year period.

Crisis management

The crisis management case study focuses on ways in which Security Research has helped to improve technological capabilities to address the needs of first responders and civil protection authorities responding to crises. Among the projects examined through PASR included Geocrew, a study on geo-data and crisis early warning situation awareness. A number of FP7 SEC projects in the area of CM were also analysed. These include the BeSeCu, CrisComScore, COPE, NMFR Disaster and SICMA projects.

The projects focused on different aspects of crisis management, such as: interaction between the public and first responders; the development of early warning systems to alert relevant authorities to crises, and the use of technologies, for example, to improve situation awareness and common operational picture and to develop second generation locators in Urban Search and Rescue operations.

Two projects tackled aspects of Crisis Management relating to the interaction between the public and first responders. The BeSeCu project focused on modelling Human Behaviour in Crisis Situations. Research was undertaken through the project to improve safety and evacuation procedures, especially with regards cross-cultural and ethnic differences in crisis situations. The second project, CrisComScore tackles the communication of the situation to the public so as to ensure that the public is better able help themselves and others, without harming the efforts being made by first responders.

Among the technological-oriented projects examined include the COPE (Common Operational Picture Exploitation) project. As part of a technology solutions work package, COPE is performing systems integration, together with tasks to address other areas of command and control, which include improvement in sensors, communication, decision support and first responder solutions. The project provides a good example of how military and civilian legacy technologies can be leveraged and adapted to meet civil security research needs. There are demonstration aspects to the project and the improved interface and technology for CM command and control centres will be tested and validated by end users in a realistic scenario modelling exercise.

The SGL for USAR project, another project with strong technological innovation elements involves a pan-European multidisciplinary team of 21 partners including rescue teams, researchers and SMEs. Among the outcomes expected to be delivered include a prototype of a standalone first responder device that integrates five different location methods (FIRST), proof of concept for a networked rapid casualty location system (REDS) equipped with wireless sensor probes; a tested and calibrated advanced environmental simulator for training and testing search and rescue units, including canine teams and a fully developed mobile operational command and control platform ready for commercial
use. Additionally, methods and guidelines for the operation of rescue teams are being developed. The project is also expected to produce 5-6 publications (scientific and other) each year (5 so far).

The new first responder device has the potential to save lives. According to the team leader, ‘It will enable air quality in the pockets or voids found in collapsed buildings to be continually monitored. Entrapped people and these void spaces have characteristic visual, aural and chemical profiles that can be detected using such a combination of techniques.’

The project has also been successful in getting user organisations on board. There is active interest – currently expressed in the form of letter of intent – for the use of project outcomes from 12 national and local rescue services teams across Europe and from the Joint Research Centre. Users have also been involved through the organisation of a number of workshops (2 so far) which have brought together national authorities and rescue units, technical experts and the general public.

Other CM projects have sought to strengthen capabilities in particular areas. The NMFR Disaster was especially interesting in that it involved a number of civil protection agencies and first responders, and is also a good example of how the Security Research Programme is helping to strengthen cooperation internationally through the active participation of associated countries (Israeli and Palestinian first responders and academic institutions were also involved). The project work modules on different aspects of disaster response including: Training methodology and technology, the Human Impact of disasters, Legal and ethical aspects, Personal Protective equipment and Legal and ethical aspects. For each and every module, a workshop leader was assigned to lead the work package.

Users involved in the project stated that they had found participation to have been useful, and the opportunity to exchange and share experiences between countries was highly valued. One user provided detailed feedback on the most useful areas that FP7 SEC could support in the CM area. This is worth summarising here since it illustrates how useful feedback directly from users can be in defining user requirements at the project level, and also in defining programme level priorities.

Table 3.8: The user perspective – SAMUR civil protection, Madrid (NMFR Disaster)

<table>
<thead>
<tr>
<th>How FP7 SEC can assist civil protection agencies and first responders in the crisis management field</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improve the interoperability of communications equipment (internally and between organisations) and in ensuring greater versatility in communication systems</td>
</tr>
<tr>
<td>• Establish standards in respect of operational procedures to improve incident response</td>
</tr>
<tr>
<td>• Create a network of experts to ensure that good practices on incident response can be exchanged between and among different EU countries, and with international partners</td>
</tr>
<tr>
<td>• Develop scenario modelling on some of the main risks identified.</td>
</tr>
<tr>
<td>• Establish a fast and secure cross-border information sharing system between national civil protection agencies with common criteria, to identify and ensure better preparation for significant risk events.</td>
</tr>
<tr>
<td>• Produce common guidelines and procedures as to how to respond to different situations, develop procedures for working with other emergency services and Technical Guidelines for specific threats: CRBN, fire, etc.</td>
</tr>
<tr>
<td>• Wider dissemination of the experiences and results of projects to raise the level of knowledge about effective practice in crisis management and emergency support.</td>
</tr>
</tbody>
</table>

Overall, projects in the area of crisis management have made various steps forwards. Among the main research results include: improved Common Operational Picture Exploitation with potential to make command and control performance more effective and the development of a prototype for a
Evaluation results

standalone first responder device, which once deployed, has the potential to save lives by improving response times to identifying trapped victims. Several projects have also promoted improvements in crisis communication systems, both methodological and technological.

In crisis management, the largest demonstrator project supported in the first 2 calls was the ESS project (Emergency support system) which aims to develop an integrated and scalable crisis management system capable of providing situational awareness to decision-makers. The project will provide a demonstration of a technologically advanced portable command and control system with plug and play capabilities. ESS should provide real-time information sharing, multimedia information gathered from multiple sources. This will be vital in real crisis situations when communications infrastructure may be down. The project is also an excellent example of how use will be made of both GPS positioning and GMES data to better monitor and coordinate the efforts of first responders. This could be used for example to identify the coordinates of collapsed buildings and to provide much more accurate data on weather conditions. This project has strong potential to attract strong interest from users, providing the technology can be deployed at reasonable cost for public authorities.

Soft outcomes in the crisis management field include the exchange of knowledge, experiences and good practices between relevant stakeholders, greater cooperation between relevant actors, and the development of a better understanding of the human element in crisis management, and how cultural factors may influence how people respond in a crisis.

3.5 Cross-cutting missions in EU Security Research

In this sub-section, various cross-cutting issues are analysed. FP7 SEC defines 3 Cross-cutting missions. These include:

1. Security systems integration, interconnectivity and interoperability - information gathering for civil security, protection of confidentiality and traceability of transactions;
2. Security and society - socio-economic, political and cultural aspects of security, ethics and values, acceptance of security solutions, social environment and perceptions of security;
3. Security research coordination and structuring - coordination between European and international security research efforts in the areas of civil, security and defence research.

Additionally, other areas within FP7 SEC that are horizontal in nature have been examined in this sub-section. Examples include work to promote harmonisation and standardisation.

3.5.1 Security systems integration, interconnectivity and interoperability

End-users increasingly need to be able to share and gather information from different sources, and also to interact with other users at national, regional and international levels on security matters. There is also a need for greater interconnectivity and interoperability and data sharing between public authorities in particular areas of security, such as CBRN, maritime security and crisis management. Among the main challenges include: improving secure information sharing between users across Member States, addressing capability gaps that prevent interoperability between different countries and systems, and strengthening the ability to integrate data from many different sources.

Interoperability extends well beyond the challenges of integrating and networking IT systems and also relates to the need for more harmonised processes, procedures, equipment and technologies. Correspondingly, there has been a strong focus within the security research programme on networked systems and interoperability.
Evaluation results

While the development of net-centric systems means greater interconnectivity, which is essential to promote the efficiency and effectiveness of agencies involved in civil security, there are associated new vulnerabilities and risks at a systemic level. A networked environment raises new security concerns, about the potential vulnerabilities to networked systems and systems of systems, since these could potentially be exploited by criminal or terrorist organisations. Problems such as online financial fraud and cyber-crime demand a cross-border, interconnected response from law enforcement agencies. The ESRP has therefore also invested in projects that seek to tackle new and emerging threats, such as cyber crime which is evolving rapidly.

In order to facilitate secure information sharing and to promote greater technical interoperability, PASR and FP7 SEC have funded a number of projects that seek to network different user organisations and to integrate systems of systems to promote greater interoperability.

Examples of ESRP themes in which there is a need for investment in interoperable systems has been identified include:

- **Critical infrastructure protection** - Infrastructure Resilience, ensuring continuity of services in the event of a malevolent attack of accidental breakdown of CIs, combating cyber attacks
- **Maritime security** - investment in implementing networks of sea-based sensors to improve interconnectivity and interoperability. Also integration and fusion of information and data gathered by sea-based sensors with those of space-based data produced through GMES
- **Aviation security** – ensuring that secure communications networks can connect different public agencies with airport operators and airlines. For example, passenger information such as no-fly lists needs to be communicated between different public agencies
- **Combating terrorism and organised crime** - improving the traceability of financial transactions to prevent the financing of organised crime, money laundering and terrorism

In the 3rd and 4th calls within FP7 SEC in particular, there has been funding support for large-scale ‘flagship’ demonstrator projects, and these have included new ‘systems of systems’ solutions that are expected to go significantly beyond current ‘state of the art’ in promoting interoperability.

In the area of CBRN, there is an increasing need for networked analysis tools to prevent transfers of CBRN and other illicit materials. In order to achieve synergy among complex computerised information systems, capacities are being developed that should reduce the risk of information loss, while enhancing synchronisation across organisational, institutional and component boundaries. This would help address the lack of integration and coordination procedures between Member States who often do not collaborate effectively when forming operational requirements.

Several projects supported in both PASR and FP7 SEC addressed systems integration, interconnectivity and interoperability issues. For example, under PASR, the SUPHICE project promoted the development of secure networks. It addressed the need for an accepted algorithm suitable for EU use in a SECRET environment. The project also demonstrated that the same cryptographic product may be used without contravening EU or national law. A key outcome was to make communications consistent with national and international policies for a range of European and National agencies (e.g. Civil protection, Intelligence Agencies). The SUPHICE project ensured that the algorithm was interoperable with a number of different networks and systems.
Evaluation results

The HiTS/ISAC project under PASR aimed to prevent terrorism and organised crime by enhancing cross-border interoperability and situation awareness as key enablers of new technical and operational methods for work, training and co-operation across Europe. The project enabled information analysis and fusion of a range of sources, through secure cross-border cooperation between security authorities. HiTS/ISAC also focused on the electronic detection, tagging and tracking of suspicious individuals such as communication between suspected criminals, or anomalous movement of persons, goods and money.

The SGL for USaR project in the area of crisis management (specifically in urban search and rescue) has provided a demonstration of how different types of signals could be used to improve sensor technologies and to make these interoperable for the purpose of assisting in accelerating the location of victims in urban search and rescue operations.

In the maritime security domain, Operamar provides a good example of how innovative research can lead to breakthroughs in interoperability and networked systems capabilities. The project was able to improve the compatibility of all interfaces for data exchanges within the project, while also developing a strategic roadmap to encourage the evolution of an interoperable approach to maritime security from an organizational, institutional, and legislative basis.

Through the ODYSSEY project (Strategic pan-European ballistics intelligence platform for combating organised crime and terrorism), law enforcement agencies and technology providers established new patterns of cooperation which helped to develop good practices. Through the development of structural cooperation mechanisms, the project demonstrated how specialised groups from different areas of the security industry can share information and strategic planning tools in a secure environment. Underpinning the project’s success was a commitment to the development of common formats to facilitate data exchange between systems. These human interfaces were also accessible to Ballistic technology providers who were able to use the technology to compete within the security market through greater functionality and quality.

In addition to projects supported through PASR and FP7 SEC, through the Joint Security Research and ICT call in 2007, a joint approach was adopted to implementing the ICT theme on critical infrastructure protection. This shows the level of maturity in terms of delivery capacity that the programme has been able to acquire. PASR played a key role in developing capacity and the seconding of Commission officials to assist in setting up REA has ensured continuity in terms of knowledge about security research (the REA senior management includes officials from both DG ENTR and DG INFSO that formerly were part of the Security Research Units of the two respective DGs).

The Joint ICT Call had a budget of €40m of which €20m was funded through the ICT Theme and €20m through the Security Theme. Some of the activities should promote interoperability. Following the Joint ICT and Security Call, there has subsequently been follow up in a number of calls for proposals on research topics to build on initial progress in promoting the strengthening of ICT networks to withstand cyber-attacks, such as the Sec-2011-1 Security Research call (Topic: 2.5-1: Cyber attacks against critical infrastructures).

Capability-driven standardisation is of vital importance to the security of critical infrastructures which are operating by means of ever more complex technologies. Many technologies have dual-use character, including civilian and COTS (commercial off-the-shelf) products. As globalisation disseminates these products more widely it is likely that new systemic vulnerabilities emerge.
Evaluation results

Interoperability, therefore, cuts both ways: It is a distinct functional advantage, but care needs to be taken to prevent negative cascading or chain effects if a part or an area of critical infrastructure suffers from attack, accident or disaster.

The INSPIRE project (Increasing Security and Protection through Infrastructure), financed through the joint ICT and Security call aims at enhancing European potential in the field of security of critical infrastructures (CI) by assuring the protection of critical information infrastructures through the identification and modelling of vulnerabilities and the development of innovative techniques for securing networked process control systems.

In order to increase the resilience of such systems, INSPIRE is developing traffic engineering algorithms, self-reconfigurable architectures and diagnosis and recovery techniques. The idea is to protect critical information infrastructures by appropriately configuring, managing, and securing the communication networks which interconnect distributed control systems. With regard to standardisation, INSPIRE will contribute to standardisation by fostering the interoperability of CI equipment and multiple CI operators and coordinated strategies for securing networked process control systems.

Given that many projects are still underway, it is not possible to provide a full assessment of results. However, it is clear that progress has been made in improving the security dependability and resilience of Critical Infrastructure (CIs). With regard to softer outcomes, some projects have created new knowledge about the organisational, human, societal and legal aspects of CIs. Technologies for the protection of critical infrastructures have also been improved. For example, trusted computing infrastructures to promote interoperability and end-to-end security of data and services are being developed and show considerable promise.

3.5.2 Security and society

The annual work programmes in respect of FP7 Security Research include a commitment to comply with the European Charter of Fundamental Rights, including privacy considerations. It is important that the balance between the risk of a security threat and any risk to Europeans’ human rights and freedoms coming out of the deployment of technologies to counter that threat are assessed.

Issues of security almost inevitably involve questions of ethics and human rights and several projects have been supported that explore issues relating to the ethical and societal dimension in FP7 Security. The perception of security threats in Europe has changed dramatically since September 11th, 2001 and the lessons have been brought home by the events in Madrid and London. Risk and uncertainty have become important factors in the organisation and mobilisation of responses to perceived security threats and with them ethical issues of greater complexity. The focus of these issues in the current context is the ethics of new technologies that are being supported under FP Security and their potential impact on human dignity and integrity but also with their implications for future generations.

The Security area, however, is not unique in facing such questions. The rapid pace of scientific and technological progress in general has given rise to a range of ethical questions. These questions are most acute for the European Commission in relation to European support for research and development through the Framework Programmes. Especially since the Commission’s Science and Society Action Plan was launched in 2001, a systematic approach has been adopted to ethical issues in the EU’s scientific and technological activities. The European Group on Ethics has also had an important role in guiding EU policy on culturally sensitive ethical questions in science.
Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research

Evaluation results

The fundamental principles providing ethical guidance are enshrined in the EU’s Charter of Fundamental Rights, especially in the current context, with its references to the integrity of the person, the protection of personal data and the right to a private life. The FP7 Decision states that research must comply with fundamental rights principles. A requirement was also included in FP7 to review any project applications raising ethical questions. As well as checking compliance with standards set under the European Charter of Fundamental Rights, the ethical review also seeks to check the balance between the research objectives and the means to be used (e.g. privacy considerations in respect of surveillance technologies).

In relation to Security, the issues revolve around the question of how to ensure the security of EU citizens in the face of threats such as terrorism and crime but also natural disasters and industrial accidents while respecting the right to individual security and civil liberties. The Security & Society axis under FP7 takes integrates societal and ethical considerations into programme planning, delivery and projects. Regarding the project level, the ethical screening review presents the primary vehicle to ensure that projects do not raise ethical concerns. The societal and ethical issues addressed include personal data protection, communication between authorities and citizens in crisis situations, public awareness about security threats, and societal acceptance of the deployment of security technologies.

Among the ethical aspects of security research include the need to monitor ‘dual use’ potential. In other words, technologies developed for civilian purposes can sometimes be adapted for defence purposes and dual use issues associated with particular technologies being developed through FP7 SEC need to take this into consideration.

At the project level, ethical and societal issues arise at a number of levels. A contrast can be made between i) projects that focus directly on these issues and ii) projects that raise ethical or privacy issues and address these as a horizontal theme during project implementation, through work packages on ethical aspects of technology deployment, the use of an external ethical advisory committee, etc.

Among the examples of projects that include an explicit focus on societal and cultural aspects of security was the BeSeCu project. The project has examined the role played by national cultural differences in determining how people and authorities respond when faced with a disaster situation. The project examined behavioural reactions to crisis situations in different EU Member States and identified possible similarities and differences in response to disasters and emergencies. The research results are already being used in niche software which is used by architects in designing buildings that take into account differences in cultural behaviour in crisis situations.

The DETECTOR project examines how policy-making institutions and law enforcement bodies respond to the ethical challenges posed by the development of counter-terrorism technologies. A major review of the human rights’ consequences of countering terrorism is being undertaken, including a survey of data mining technologies and electronic surveillance of the internet and other counter-terrorism techniques. Safeguards will be proposed. With regard to achievements, projects contributed to promoting pan-European and international awareness on ethical aspects of security technologies, while contributing to deepening and enlarging transnational and international dialogue, for example, through contributions to international conferences on ethics and biometrics organised by the DG Research.

Project level research has focused on socio-economic analyses, scenario building and activities related to cultural, social, political and economic dimensions of security. The role of human values in policy
Evaluation results

making as well as citizens' perception of security in different countries have been addressed in projects both to achieve a European ethical framework in the field of security and to enhance the trust of European citizens in research activities. Projects have fostered open debates between different stakeholders (i.e. researchers, end-users, civil organizations) on the place of culture in security research. Technology-oriented projects are refining detection and protection methods in order to better safeguard privacy and liberties, while addressing vulnerabilities and foreseeing new threats.

The CPSI project aims to analyse the influence of factors such as technological progress and media coverage on public opinion in general but also on specific groups of individuals to try and identify both similarities and differences in the way certain groups of people perceive themselves to be safe in society. Research is also conducted on the role of the media in the area of security and civil protection. The activities of CPSI have yielded a system to register and monitor security-related data down to the neighbourhood level, and have provided end-users with a theoretical insight into (perceived) security so that they can formulate better policy.

Surveillance and detection methods, ranging from CCTV camera-surveillance of suspicious behaviour in public places to secret internet monitoring and data-mining are among the areas of technological development that pose major ethical and legal questions. The trend towards interoperability between EU-operated databases has to be accompanied by a comprehensive, specific and legally binding data protection framework with adequate safeguards to cover risks related to the large scale storage and use of personal data. The ethical framework for all security projects is being developed in a consistent fashion. An ongoing challenge is how to promote greater cross-fertilisation between projects and greater take-up of results after projects have been completed.

3.5.3 Security research coordination and structuring

Security research coordination and structuring is one of three cross-cutting missions in the FP7 SEC programme. Support for activities to help structure the ESRP can be 100% EU financed through Coordination and Support Actions (CSAs). Among the types of activities supported to date include:

- **Staccato** – supply chain mapping and development of an industrial taxonomy of the security industry, methodology on Technology Watch
- **SecureSME** – facilitating SME's access to supply chains in the security industry
- **STRAW** - Technology Watch to monitor available technologies for potential adaptation and deployment by users
- **CREATIF network** - establishment of a network of facilities for testing and certification in areas of CBRN
- **PETRANET** - establishing a ‘user network for the take-up of security research’;
- **SEREN and SEREN II** – promoting co-operation between NCP’s involved in FP7 SEC (e.g. SEREN coordination action and the recently awarded SEREN II project)

Support for supporting activities, such as the various project examples identified above was built into calls for proposals in both PASR and FP7 SEC. The Commission wished to provide support for the strategic development of the ESRP, and to promote structuring and coordination between the supply and the demand side, and to encourage the participation of SME.s
Evaluation results

As an example of the attention devoted to such activities, in the 2006 PASR call, there was support for “Coordination networks between security technology stakeholders including research activities supported at the national and/or regional level” and for the setting up of “Coordination networks integrating security technology supply chains including small and medium enterprises (SME).

There were some links between coordination and structuring projects. For example, the Staccato project funded through PASR 2006 liaised with Secure SME in order to ensure that potential synergies between projects were continued. Staccato (Stakeholders Platform for Supply chain Mapping, Market Condition Analysis and Technologies Opportunities), provides an interesting example of how CSA projects have helped to promote the structuring of the future ESRP. STACCATO was a 16 month project, and the project followed up on the earlier SeNTRE (Security Network for Technological Research in Europe) project, a supporting activity funded under PASR 2004. The main aim was to propose methods and solutions for the creation of a security market and a more structured supply chain in Europe.

The project led to sustainable outcomes. Some project results have been used by other projects and by wider security research actors. For example, an industrial taxonomy was developed which mapped out an industrial classification system for the civil security industry. Linked to the taxonomy, the project was also helpful in developing a framework for structuring the security supply chain. The taxonomy has been subsequently been used and referred to by other projects, such as STRAW. This provides a useful illustration of continuity between PASR and FP7 SEC, with the knowledge gained through the implementation of individual CSA projects being gradually built on through follow-up projects. Some aspects of Staccato, such as the development of a Technology Watch methodology, have been followed up. The recommendation to establish a European Technology Watch has been implemented. The study also helped to prompt a debate among relevant stakeholders on how to best further the European Security Market.

The STRAW project involved proof of concept testing in relation to the establishment of Security Technology Active Watch. The aim was to actively monitor the development of new technologies of potential relevance to public user organisations through the development of a secure access database. The project was successful in attracting users to attend a workshop, but experienced some difficulties in obtaining sufficient time inputs from users during the project.

CSAs have played an important role in stimulating cooperation between relevant actors in particular fields, such as the CREATIF network in the field of CBRN. Creatif provides a dedicated communication platform for technology users and decision makers, providers and testers to discuss the future development of testing and to support user decisions and industry product/service development. The project has successfully developed a networking strategy to strengthen cooperation and knowledge exchange within Europe between CBRNE testing and certification facilities.

With regard to the promotion of cooperation between security actors, through the PASR 2005 call, the PETRANET project was supported. PETRANET established a network linking the security research community with users such as the police, fire brigades, ambulance services and civil defence. The network promoted the transfer of research results into the operational environment using secure dissemination mechanisms. PETRANET supported the cross-fertilisation of emerging research results between PASR activities. The project provided support to individuals, organisations and agencies seeking information on PASR projects by putting them in contact with each other. This communication was consolidated through the establishment of a virtual helpdesk that offers networking activities and information brokerage services as well as through access to experts involved in the PASR programme.
Evaluation results

During FP7 SEC, there has been continued support for cooperation and networking between users. For example, the EUSEC II project (described in detail in 4.3 on user participation in Security Research), provides a good example of how the EU Security Research programme can promote interaction, cooperation and the sharing of good practices between projects. The project, which focuses on Security Planning for Major Events, has strengthened cooperation between Ministries of Interior, national police academies and police forces. A key recommendation from the project is to set up a European House of Security Planning for Major Events, which would serve as a knowledge repository and mechanism for promoting ongoing cooperation.

CSA projects have also promoted networking between NCPs, the SEREN project and the follow-up project - SEREN II. SEREN sought to promote improved coordination between the network of NCPs by linking them up through an intranet. The aim was to improve the quality of service provided by NCPs and to strengthen cooperation between NCPs so as to improve the network’s overall effectiveness. While the project achieved some successes in promoting networking and coordination, some NCPs felt that more could be done to strengthen coordination activities between NCPs. Some NCPs taking part were more positive, however. ‘SEREN has been effective in improving the quality of services provided by NCPs throughout Europe through training and networking activities. Customised training sessions were organised and this was useful because some organisations fulfilling the NCP role are new’.

In conclusion, CSA projects have made a positive contribution to promoting coordination and structuring. Among the achievements include: improving SME access to technology and research supply chains; promoting cooperation between suppliers and users of security research; improving cooperation, coordination and networking between users on internal security issues; prompting debate among relevant stakeholders about how to structure the security industry; competence mapping in particular areas; and developing a more strategic approach to structuring the security industry. There is a need to ensure that the various networks set up are sustainable, since there is a question mark as to whether these could continue to operate without ongoing EU funding.

3.6 SMEs in PASR and FP7 Security Research

Given the significance of Small and Medium-sized Enterprises (SMEs) in the European economy and their important role in promoting innovation, successive Framework Programmes have encouraged SME participation in European research. Changes were introduced in FP7 as part of a concerted effort to encourage the active engagement of SMEs in research activity. Funding problems were addressed by increasing the funding rate for R&D activities by SMEs to 75%. Furthermore, a target has been established of at least 15% of the available funding going to SMEs under the Cooperation Programme.

Challenges for SMEs in the Security market

The Study on the Competitiveness of the EU Security Industry pointed out that the security industry is still in the process of structuring. High investment costs in technology development and the high costs

33 The latest figures from Eurostat show that independent firms with less than 250 employees employ two thirds of the workforce (67.4 %) and generate 57.7 % of total value added

34 Ecorys et al, Study on the Competitiveness of the EU security industry, November 2009
Evaluation results

associated with securing access to markets mean that there are high barriers to market entry. Public authorities are the main purchasers of the industry’s outputs and these operate through public procurement regimes which add to the costs of securing markets, especially when there is a need to ‘educate’ clients on technological possibilities and choices. One of the consequences is that although there are several EU companies among the global leaders in their fields, the depth of the industrial base in Europe is relatively shallow and supply chain relationships are underdeveloped.

The ESRIF final report (December 2009) proposed a strategic approach to the development of innovation in the security sector and highlighted ‘untapped potential’ in terms of the innovative capabilities of SMEs, including those that would not normally operate in the security arena. Opportunities do exist, particularly in high-tech niche security markets where greater SME participation could improve the competitiveness of large European enterprises.

FP7 Security Projects, SME participation and financial aspects

Security research has contributed a relatively high proportion of funds to SMEs, especially when considering that although calls for proposals have explicitly encouraged SME participation, there have been no dedicated SME calls. However, in contracts signed by 31 March 2010, 20.2% of the Security budget allocated at that stage had been assigned to SMEs in contrast to 14.0% for FP7 as a whole and 18.7% of participants are SMEs as opposed to 16% for FP7 overall. At that stage, some 135 SMEs had been involved in 52 signed grant agreements in the Security area; France, the UK, Italy, Germany and Spain all had a relatively significant presence. Only 7 projects were led by SMEs (11% of the total number of Security projects) and 14 projects had no SMEs involved at all.

In the 2010 Call, some question marks have been raised in relation to whether all SMEs really meet the criteria in the official definition of an SME. This is important not only because there is a need to establish the ongoing performance of FP7 SEC versus other areas within FP7 Cooperation, but also because it affects the co-financing rate at which different participants can take part. Some of the largest consumers of EU funds categorised as SMEs in the 2010 call appear to be research institutes. CSES’ evaluation scope was PASR and the first two calls in FP7 SEC, and given the breadth of issues covered in this report, it is not possible to explore this in detail. However, a check was carried out of earlier calls using data from the CORDA database and the SME statistics were found to be accurate.

There is strong competition among SME’s for funding. Only 15% of applications from SMEs were successful in FP7 Security, compared with 18% of all applications in Security and 20% of all applications across all FP7 themes. The characteristics of SME participation in FP7 Security raise some interesting questions:

- Why has Security been relatively successful in encouraging SME participation?
- How should this be seen in the context of a fragmented security market and relatively high barriers to entry?
- Why do SMEs participating in FP7 request relatively high contributions
- Why is there relatively fierce competition for project funding under FP7?

One possible answer is that SMEs see participation in EU funding programmes as a way of entering the market and coping with high entry barriers. High barriers arise due to the cost of developing new

35 ESRIF final report
Evaluation results

technology to cope with new threats and also because of the procurement regime that governs much of the purchasing of the sector’s outputs. Participation in Security research projects can assist with both of these considerations. Market fragmentation underlines the need for co-ordination mechanisms that bring together teams with depth of experience to address emerging needs, especially in a context where procurement procedures dominate the route to market. This hypothesis is consistent with the relatively high participation rate and the relatively tough competition to obtain funding. It also possibly explains why the funding requested by SMEs is relatively high, since the technical barriers to entry could be perceived to need high expenditure in order to surmount them.

Questions were included in the survey of beneficiaries and checklists on the extent and nature of the involvement of SMEs in consortia and on extent to which SMEs have brought innovation to projects. Of those responding to the on-line survey, 19 out of 72 were SMEs. Other respondents were involved in projects that had SME participation. Of those who identified themselves as SMEs, the respondents split roughly equally between ‘micro’, ‘small’ and ‘medium’ enterprises. They have a variety of roles in the consortiums of which they are a member. Clearly some SMEs are central to structuring the project, while others have a more peripheral role. It is also known from interviews, that some SMEs were specifically engaged to handle the dissemination aspects of the project or to advise on project management processes. Overall, the involvement of SMEs appears to have generally been viewed positively by other partners in the consortium, with no negative attitudes being reported.

The relatively strong participation by SMEs seems to have been welcomed by other participants. When all participants were asked about ‘soft’ research outcomes linked to projects, just over half thought that ‘Improved networking and coordination between security research actors’ was significant and over a third (39%) specifically referred to ‘Strengthened cooperation between SMEs and large firms’ as a positive outcome.

Projects with SMEs as a lead partner

Among the relatively small number of Security projects where SMEs are the lead partner, there are some interesting cases where the lead position enables the SME to have its own clear technical and commercial objectives and also allows it to co-ordinate the other partners in the pursuit of them. If SMEs are able to initiate a project and assume the position of lead partner, there are a number of advantages. Since it is their own agenda that they are pursuing rather than one determined by others, they are able to make developments that are central to an active business strategy. As the representative of the project, they can achieve a higher profile in the market and be the natural point of contact for other market players. At the same time there are advantages of participation giving full rein to small firm innovation potential, resolving funding problems where high entry costs exist and helping to establish niche positions in the market in order to establish viable routes to market.

The iDetecT4ALL project shows that a strategy for SMEs in the Security Market, especially when they already have an established position, perhaps in a parallel market, is to make use of the assistance available through FP SEC to create a leading position in the supply of a particular range of products, or rather to create the technical and commercial conditions for establishing such a position. Research funding at the new higher level under FP7 is clearly having the effect of making this approach a more viable option and is seen by SMEs as a way of overcoming the high technical barriers to entry.36

Projects with SMEs participating as partners

36 The funding also appears to be at a higher level than that available in most cases at a national level.
Evaluation results

SMEs that do not initiate a project or take a leading role in their consortiums are in a somewhat different position from the previous category. Roles within a consortium can differ quite substantially. SMEs may be brought in to provide specific expertise and this may be technical, although, in a number of cases it may also be in the form of contributions to project management or dissemination and publicity. However, a common theme is that SMEs find participation in projects to be a way of networking, especially beyond national frontiers, and a potentially significant route to market.

However, this type of involvement has its own contribution to make. The relatively large number of FP7 SEC projects involving SMEs as participating partners rather than initiators or leaders of projects may be seen as making a distinctive contribution to the creation of a more diverse, but also more cohesive security sector across Europe. In this way, SMEs are helping to strengthen the industrial base of the sector in a variety of ways. Some participants in these projects do use them to further develop their position as niche suppliers in particular areas and also play that role within their consortiums.

However, there is some evidence that SMEs are useful in pushing their larger partners and research institutes in the direction of concrete applications. Projects in this category appear to be making contributions to building supply chain relationships and overcoming fragmentation.

The moves to simplify application procedures under FP7 and improve the funding arrangements for SMEs have definitely been welcomed. However, the job here has not been finished. Cases cited in the horizontal study refer to the need for firms new to FP processes to have professional assistance if they are to participate in successful proposals. There is a need to continue to assist SMEs both in terms of a continuing simplification of procedures and rules and at a practical level.

There is also a need to continue to examine the way that SMEs operate within projects, once they are under way and even after they have been completed. This will give rise to other improvements in the way that SMEs and the European Security industry benefit from projects. In terms of the mechanisms of SME participation, project requirements do not always take into account the day-to-day realities of small firms. Their management in particular needs to be very flexible to respond to unforeseen issues and difficulties in their business. Consequently, it is sometimes difficult to maintain a steady input into research processes and greater flexibility, for instance, by allowing outsourcing during the course of a project, might be more in line with the way that SMEs actually work.

Future challenges for SMEs

The main future challenge would appear to be to build on what is already being achieved. There is a relatively high SME participation rate in FP7 SEC, but the absolute numbers are still relatively small and the ESRIF Report talks of a target of 25% participation. Competition among proposals involving SMEs is relatively fierce, but there is scope for helping projects involving SMEs to improve their success rate. Above all though, moves to consolidate and build on the results of projects, even by simple measures to improve the information available on results, are important, particularly in a sector where the development of integration and interoperability are so important.

In conclusion, in spite of the fragmentation of the security market and high entry barriers, there are capable enterprises which can creatively use the opportunities presented by FP7 SEC to overcome the difficulties and find a viable position for themselves. The involvement of SMEs is generally welcomed by other participants in projects.

Although SME participation in FP7 SEC is higher than elsewhere within FP7 Co-operation, there is still room for further improvement, perhaps by dedicated SME calls, in order to boost the number of
projects led by SMEs. The new level of research funding for SMEs under FP7 is having an important effect in encouraging SMEs to enter a market with high barriers. Other simplification measures have also been appreciated. However, further improvements are possible, especially developments based on an appreciation of SME management processes and practices, such as more flexibility in allowing outsourcing and sub-contracting.

It might also be appropriate to give more recognition to the learning function that can be important for some SMEs within an FP7 project. Consideration might be given, for instance, to an ‘apprentice’ status for some SMEs. This would recognise that they are not always in a position to contribute substantially to core developments in a project, but help them to develop their research capacity and contribute in other ways, such as representing the consortium in domestic markets. This could be especially relevant in the case of SMEs from the new member states.

A more fundamental recommendation relates to one of the major reasons that SMEs find the Security sector to be difficult terrain. Some of the significant barriers to entry that SMEs face arise because most purchasing of security goods and services is by public authorities through public procurement regimes. There is growing attention currently to ‘smarter’ public procurement and ESRIF37 called for the security sector to be included in the Lead Market Initiative37. It is clear that the Lead Market approach to procurement in the security area could potentially make a significant contribution to strengthening the whole sector. It should be investigated further.

3.7 National Security Research Programmes and the ESRP

As part of the evaluation research, CSES carried out a comparative analysis of those countries that presently have national civil security research programmes. The research suggests that only 8 out of the 27 EU Member States presently have such programmes, although some of the Associated countries taking part in FP7 SEC, such as Israel, also pursue such research programmes. The findings from the analysis are set out in Appendix G. The aims of the research were to:

- Make comparisons between national programmes and the ESRP and examine any differences (funding level and co-financing, application procedures, geographic eligibility);
- Establish the extent to which the ESRP adds value to existing national research programmes;
- Ascertain the extent to which national programmes are complementary, and whether there were any areas of overlap/duplication with the ESRP.

The main national programmes identified were:

<table>
<thead>
<tr>
<th>Table 3.9: National Security Research Programmes in the EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>● France: Research Programme  CSOSG - Concepts, Systèmes et Outils pour la Sécurité Globale (National Research Agency ANR)</td>
</tr>
<tr>
<td>● Netherlands - R&amp;D Programme on Security, Safety and Technology</td>
</tr>
<tr>
<td>● Sweden - National Security Technology Research and Innovation Programme</td>
</tr>
</tbody>
</table>

Evaluation results

- Finland - Technology Programme on Safety and Security
- UK – a number of programmes, including the UK CBRN Resilience Programme
- Austria - KIRAS – the Austrian Security Research Programme
- Germany - Research for Civil Security Programme
- Romania – National Programme for Research, Development and Innovation in Space and Security

Information on national programmes were undertaken with a sample of national security programme managers (AT, DE, FI, UK, RO). In some cases, there was a lack of literature on the planning and implementation of national security research (several programmes only recently got underway). The main findings from the comparative assessment are summarised below (detailed findings are presented in Appendix G):

Table 3.10: Key findings - comparative assessment national security research programmes and ESRP

- ESRP has a higher annual funding allocation than national security research programmes combined. It plays an important role in addressing a funding gap in response to identified needs;
- There are wide variations in funding levels for national programmes among the 8 Member States that presently run programmes. However, some countries have allocated a significant budget, such as DE, €129m (2007-09), and FI, €160m EUR (2007-13);
- The setting up of an EU Security Research Programme has been a catalyst for some MS in setting up their own national programmes. Other Member States are considering creating such programmes in future.
- There were common priorities in themes supported through national programmes and ESRP with a strong focus on topics such as: CBRNE, Crisis management, Critical infrastructure protection, Land border and maritime security, Networked systems and interconnectivity and interoperability
- The application process at national level was viewed as being easier and more user-friendly than FP7 SEC by beneficiaries in some countries (e.g. DE). There were also simplified rules for the participation of SMEs and users in some cases (again, DE);
- There were higher levels of co-financing for some types of participants in national programmes. For example, SMEs and research institutes were sometimes eligible for 100% financing (DE);
- Only 2 out of 8 EU countries made provision for a transnational element to research projects. DE and AT allowed scope for cross-border research, but there were language restrictions (i.e. German only);
- There is compulsory user involvement in some countries (e.g. FI);
- The ESRP has played a role in encouraging some national security research programmes to take greater account of the ethical and societal dimension in security research (e.g. FI, SE); and
- There is evidence of fragmentation in national civil security research and a general failure to respond to the need for a common European Research Area through support for transnational collaborative research. EU funding plays a role in providing appropriate scale.

There are variations in funding for national programmes between Member States. For example, the Finnish Funding Agency for Technology and Innovation (Tekes) has a budget of €160m in 2007-2013. Germany has allocated €129m (€43m per year) for the implementation of its Civil Security Research Programme 2008-2010.

The Austrian Security Research Programme has a budget of €110m for the period 2006-2009. Romania has allocated €3.5m (which accounts for 8% of total national research spending) to space
and security research in the period 2007-13. It was difficult to obtain data on funding in the UK, because a number of separate programmes have a security research orientation. Some data was obtained however. For example, the UK CBRN Resilience Programme has an annual budget of €12m, which forms part of the UK strategy on combating terrorism (CONTEST, €14m).

While some cross-border cooperation on security research has taken place between the German and Austrian programmes, the research found that most national security research programmes are domestically-orientated. In terms of research themes, there was strong complementarity between national and EU security research programmes.

There was a common focus in national programmes on measures to prevent, prepare, protect and respond to the threat of terrorism. It was interesting that some themes in national programmes received greater attention than others. For example, in Finland, there has been a focus on environmental security and on improving regional security, which has received less priority at EU level. Some Member States have dedicated substantial resources to the prevention, preparedness and response phases of CBRN threats as result of collaborative activities at EU level. While the UK, French and German programmes are largely focused on mitigating CBRN threats, there was a comparatively small focus on this theme in the Swedish and Austrian programmes.

The launch of the ESRP has played a key role in encouraging national authorities to set up national security research programmes. In Finland, Germany and Romania, the programmes appear to have been explicitly created to complement the EU programme in this area and to ensure that civil security actors (suppliers and users) strengthen their capacity to take part in the programme. In Lithuania, the government is considering setting up a national security programme to structure the domestic security market, and to create opportunities for national industries to participate in ESRP. In Romania, the programme was designed to provide a framework to support the development of the scientific and technological research base and industry to leverage further financial support through FP7 SEC.

ESRP played a vital role in Member States that lacked a domestic programme, who would otherwise lack the research capabilities to address growing security threats. National authorities in some New Member states viewed the creation of national security research programmes as a means of linking national priorities to the strategic goals of the ESRP. However, there is presently a lack of financial resources to establish their own programmes and the ESRP addresses an important funding gap. In some EU countries (EU12, smaller member states), a relatively small number of firms have the critical research mass to participate in large-scale R&D projects, therefore national subsidies through national security programmes have potential to build the capacity required for companies to participate in EU security research in future. There is scope to strengthen collaboration between national programmes among those Member States that do implement such programmes.
Beneficiary Feedback, Achievements and Research Results

Section 4 is divided into two parts. The first part focuses on feedback from beneficiaries on different aspects of the ESRP, such as levels of awareness, how consortia have been formulated, partnership working and the benefits of participation in PASR and FP7 Security Research. In the second part, the research results achieved through PASR and FP7 SEC respectively are reviewed, and the extent of take-up of research results at interim evaluation stage in programme implementation is considered.

Part 4.1 – Beneficiary feedback

4. Beneficiary feedback, achievements and research results

4.1 Awareness about FP7 SEC and consortium formulation

There already appears to be a high level of awareness about FP7 Security and about how to apply for funding. Many beneficiaries in FP7 SEC had previously participated in the RTD Framework Programmes. A good proportion had also taken part in PASR. The work of ESRIF has also served to heighten awareness about the programme and funding opportunities across different activity areas.

The fact that there is strong continuity in the research topics being supported between PASR and FP7 SEC means that previous beneficiaries typically keep a close eye on forthcoming calls and are aware about what topics will be supported (since the calls are included in the annual work programmes. Other information and awareness-raising activities undertaken by the Commission and the REA have also helped to promote awareness about funding opportunities among relevant security research actors.

For example, the REA has organised information days for applicants prior to the launch of SEC calls for proposals. This has played a useful role in promoting awareness about the programme and about specific activity areas and topics being supported in forthcoming calls.

The network of FP7 National Contact Points (NCPs) established in all EU MS and in FP7 associated countries has been important in promoting awareness on the ground in the Member States. Overall, there are high levels of awareness about the programme.

Another evaluation issue explored was how beneficiaries in FP7 SEC went about the formulation of consortia and process of partner identification prior to applying for funding. Related issues in terms of views of the optimal size of consortia were also examined.

Among the findings were that consortia are often formed through pre-established networks of people having worked together on EU funded research projects. In some cases, such as EU-SECII, partners in the consortium built on an earlier FP6 project, which had different objectives, and the number of partners working together was increased. Although FP7 Security is a new programme, many beneficiaries had previous experience of participating in RTD FPs, so there were not generally problems in applying for funding or in understanding guidance for applicants.

While many project consortia involved partners that had previously worked together, valuable new partnerships have also been created through the programme, such as TerraSec. A number of projects also stated that cooperation between partners in the consortium had been very fruitful and subsequently led to further bids for EU SEC funding and cooperation on new EU-funded research projects (COPE, SICMA, ASTRO+). The inter-disciplinary and international nature of consortia adds value to the work of security industry actors (COPE).
Beneficiary Feedback, Achievements and Research Results

Some beneficiaries interviewed did approach their NCP to assist with partner identification. In this regard, NCPs may play an especially helpful role in terms of suggesting end-users that may be interested in taking part in FP7 Security.

With regard to optimal consortium size, there can be a trade-off between ensuring good EU coverage in partners through the consortium and structuring the project in such a way so as to maximise the effectiveness of individual work packages and R&D. There was a perception that large consortia with too many partners may not be as effective as a leaner consortium arrangement. It may be difficult for lead coordinators to manage multiple WPs involving multi-disciplinary teams when there are too many partners, due to the risk of compromising research quality. The structure and composition of the consortium has to be workable. Partners in large consortia may not feel as engaged or have as strong buy-in as those involved in smaller projects. There is moreover a concern on large projects that only the lead coordinator and key partners have a detailed understanding of what the project is trying to achieve overall and the detailed content of work packages (WPs).

4.2 The benefits of participation in PASR and FP7 Security Research

The benefits of participation in FP7 Security Research are now examined from the point of view of different beneficiaries – e.g. SMEs, large firms, research institutes and universities. The evaluation explored the main reasons for participating in FP7 SEC common to all beneficiaries. These included:

- Access to research funding;
- Strengthened cooperation and networking with transnational partners;
- The development of strategic relationships with users;
- A better understanding of and the opportunity to test functional user requirements.

There were also found to be different drivers of participation in FP7 SEC according to the organisation type. University departments and research institutes have an interest in participating in EU funded transnational security research and have participated in similar activities under earlier FPs. Gaining recognition for research excellence, and the opportunity to work with the private sector (which opens up scope for technology-transfer from research to industry) and networking are among the key drivers.

The availability of EU funding was important in bringing in private sector partners to take part in consortia, but was more important for SMEs than for large firms, which usually have their own in-house R&D programmes. For SMEs, various factors were mentioned including the possibility of carrying out original research leading to ‘state of the art’, strengthening links and the opportunity to demonstrate their capabilities to industry players with whom they wished to develop closer cooperation and supply chain relationships. Given that SMEs in some areas of security face barriers to market entry, access to EU research funding was a stronger driver. Other motivations were for SMEs to further develop their know-how and expertise and to strengthen their consultancy service offering. Another factor that influences SME participation was the opportunity to work together with networks of end-users, to open up new markets. SMEs appreciated the possibility of getting direct access to users in order to test and validate particular technologies and systems with end-users.

Large firms in the security industry have also been active in taking part. Among the main reasons they participate include: strengthening transnational cooperation with other large firms, harnessing the research and innovation potential of SMEs, enhancing their visibility in particular areas of civil security, leveraging know-how and adapting existing technologies for civil research / civil use purposes.
Given that multiple R&D projects influence produce development in large firms, not only ones funded through FP7 SEC, there may be some reluctance due to commercial sensitivities to share the very best technologies and research ideas. These require significant investment, carry risk in that early-stage research may not lead directly to commercialisation, and also in cases where particular technologies are to commercialised, that other firms may ultimately benefit from this, not only those that carried out the early-stage research. Examples of interviewee views were that, ‘long R&D lead times to operational products and services mean that really advanced technologies need to remain outside FP7’ and that ‘some of the most promising technologies may be developed in-house in order to avoid commercially-sensitive ideas being put in the public domain’.

In conclusion, among the main benefits for all types of beneficiaries of participation in FP7 were: strengthened cooperation with EU/ international partners; the development of strategic relationships (with other security research actors, end-users), the opportunity to develop a better understanding of user needs, enhanced visibility in the market and with users in particular, and strengthened knowledge and capabilities in particular areas of security research.

**Part 2 - Achievements and research results**

In this part of Section 4, CSES outlines a typology of outcomes and then reviews the main achievements through the implementation of PASR and FP7 Security respectively. A distinction between hard, soft and wider outcomes is made. The extent to which projects supported demonstrate research quality is also assessed.

**4.3 Typology of outcomes**

A key aim was to identify the research results to date through the implementation of Security Research projects in PASR and FP7 SEC. A typology of outcomes was drawn up in order to provide an analytical framework for this assessment. It was important to identify the most common types of research results and these varied considerably, reflecting the heterogeneity of projects types and themes. Examples of the qualitative research results that might be expected include:

**Table 4.1: Examples of research results in FP7 Security Research**

| • New knowledge and capabilities generated |
| • New technologies and innovation developed |
| • Contribution to development of standards/ harmonised approaches |
| • Development of common processes, procedures and written guidelines to promote interoperability |
| • Feasibility assessments completed |
| • Demonstration of proof of concept and prototypes |
| • Demonstration of technological solutions |
| • Development of secure networks |
| • Improvements in mobile and stand-off detection |
| • Improved strategic foresight and horizon scanning capabilities |
| • Strengthened Technology Watch capabilities |
| • Establishment of networks of security research suppliers and users. |

Another element of the framework was to distinguish between different types of outcomes associated with different types of security research projects. A basic differentiation can be made between projects depending whether they involve the following:
Table 4.2: Types of Security Research projects

| **Cooperation and coordination** | projects that bring together end-users or involve close cooperation between end-users themselves and/or between end-users and industry providers. These may involve the development of common approaches, methodologies and strategies |
| **Capability development** | development of new security capabilities and closing of gaps and vulnerabilities |
| **Foresight studies and the anticipation of emerging security threats** | projects that involve future scenario modelling to identify and address security issues likely to be a threat in future. Examples include bioterrorism, malevolent use of nanotechnologies and of synthetic biology |
| **Standardisation and harmonisation** | projects that involve identifying areas of security where there is scope for harmonisation, pre-harmonisation and standardisation activities leading to the development of minimum common standards, common certification and testing systems |
| **Interoperability and networked systems** | projects that promote greater interoperability of processes, procedures, equipment, technologies, IT networks and systems. Security solutions that provide secure network systems and help to combat cyber crime and to address ‘system of system’ vulnerabilities |
| **Social science research and analytical studies** | projects that lead to the development of knowledge about societal and human factors in strengthening the security of EU citizens, such as projects on the economics of security, risk-based assessments of security challenges |
| **Other knowledge-based activities** | examples include projects that pool together information and knowledge, involve data gathering and the development of databases in particular areas such as CBRN incidents and environmental security. Also the development of other knowledge tools such as web portals, taxonomies on industrial classification of different parts of the security industry |

Some projects may involve a combination of the characteristics of the project types set out above.

A further distinction can be drawn in analysing research outcomes depending on the extent to which projects are near to market, or closer to fundamental research:

- **Basic / fundamental research and development** – some projects have longer lead times such as maritime security. This impacts the sorts of research outcomes achieved
- **Applied research and development** - projects that involve the development of new technologies and innovation, harness legacy technologies or refine and improve existing technologies

There are then different types of outcomes, in particular a difference between **hard and soft outcomes** (and then over the medium-long term, **wider outcomes** achieved through projects collectively):

- **Hard outcomes** – new knowledge and capabilities, technologies, data, products and services, commercialisation of research results
- **Soft outcomes** – strengthened networking, partnership working and cooperation among end-users and wider security actors on security matters, greater sharing and dissemination of good practices, improved quality of research and information gathering
- **Wider outcomes** – improved access to research excellence for users, strengthened IP and technology transfer, feeding into policy development processes (e.g. CBRN counter-terrorism, drugs, crisis management, critical infrastructure protection)
Beneficiary Feedback, Achievements and Research Results

4.4 Research results and initial impacts – PASR and FP7 SEC

An overview of the findings in respect of the assessment of research results and initial impacts is provided in this sub-section. A number of elements are addressed:

- **Assessment framework** – key evaluation issues in assessing research results from the ESRP
- Key challenges in assessing research quality
- PASR results – hard, soft and wider outcomes
- FP7 SEC results – hard, soft and wider outcomes achieved to date (note: scope is 1st two calls)
- Assessment of research quality

Given the number of projects examined, their diversity and technical complexity, it was not possible to undertake a detailed technical review of the quality of all deliverables (projects have multiple deliverables). Rather, a sample of deliverables was reviewed and this, together with discussions with beneficiaries, and a review of achievements to date informed the assessment of the calibre of research being undertaken.

A more detailed thematic assessment of research results, including issues relating to the quality and effectiveness of the research carried out, is provided in the case studies. The case studies assessed research quality, but given the number of projects and the scope of a programme evaluation, it has not been possible to explore in great depth research quality across all projects.

4.4.1 Assessing the quality of research results in the ESRP

The evaluation sought to assess the **quality and effectiveness of research results** achieved through PASR and FP7 SEC, both at the project level and overall. In assessing research quality, a number of key issues were considered, and incorporated into the analytical framework:

<table>
<thead>
<tr>
<th>Criteria on which quality of ESRP projects can be assessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>- What was the quality of research outputs? (e.g. citation information, patents / IP developed and used, extent of take-up by users)</td>
</tr>
<tr>
<td>- Did the research projects funded through PASR and FP7 SEC attract leading-edge organisations engaged in security research from the private sector, universities and academia?</td>
</tr>
<tr>
<td>- Were the researchers involved in implementing projects world-class in their respective fields?</td>
</tr>
<tr>
<td>- What contribution was made to enhancing the knowledge base across different areas of Security Research?</td>
</tr>
<tr>
<td>- How far was innovation and technological excellence facilitated?</td>
</tr>
<tr>
<td>- Did the research produce recommendations likely to lead to influence the formulation of new policies and legislation/ Regulations?</td>
</tr>
<tr>
<td>- To what extent, overall, was research excellence achieved through PASR and FP7 SEC projects?</td>
</tr>
</tbody>
</table>

These questions are addressed at the end of this sub-section, following a presentation of selected achievements linked to the outputs of security research (PASR/ FP7 SEC). Where possible, research outcomes are also provided.
Beneficiary Feedback, Achievements and Research Results

4.4.2 Key challenges in assessing research excellence

Among the main challenges in assessing research excellence in respect of the ESRP are:

- The nature of an Interim Evaluation, where the expectation is that there will be more comment on process and delivery of outputs rather than on the assessment of outcomes (since it will be too premature to assess full impacts).
- There is considerable heterogeneity in projects supported, so it is difficult to compare research quality between projects;
- The relatively early stage in project implementation of those projects reviewed in FP7 SEC (especially projects selected under the 2nd Call);
- There is generally no benchmarking information in particular research areas as to what constitutes research excellence and how it should be measured (the exception is the use of citation information as an indicator of bibliographical excellence);
- It is furthermore difficult in a programme evaluation of this nature (which examines a very wide set of issues) to establish appropriate benchmarks for assessing the future potential value added of research in particular areas. For example, in aviation security, while progress had been made in developing improved detection technologies, such as the use of Terahertz rays, this research is at a relatively early stage and it is difficult to compare the effectiveness of technologies that could potentially be developed in future with existing detection technology products already available on the market.

There is an ongoing debate in the academic and research community and among funders of security research about how scientific and research excellence might best be assessed. In some countries, frameworks for assessing research quality have been developed. Consideration could be given to taking on board these principles in future assessments of the quality of research carried out through ESRP.

For example, in the UK, the Research Excellence Framework (REF) is the new system for assessing the quality of research in UK higher education institutions (HEIs). It is being used as a framework to provide benchmarking information and to promote greater accountability for public investment in research and development. However, the quality of research outputs is often assessed in terms of citation information, which although appropriate for assessing the achievements of some ESRP projects, is more suitable for assessing and comparing research quality of social science research and fundamental research within academic and research institutions than for research on ‘near to market’ applications being conducted by SMEs and industry.

There were challenges in the evaluation in comparing research quality between very different types of projects. However, an effort was made to cluster projects together in a particular thematic area through the case study research, which provides a more complete assessment of research outputs, and where possible, research outcomes.

4.4.3 PASR 2004-2006

The evaluation examined the research results achieved through the implementation of the PASR Preparatory Action. All PASR projects have now been implemented, so it has been possible to arrive at an evaluative judgement on what has been achieved through their implementation.

A constraint was that PASR activities were by definition of a preparatory nature, and concerned with laying the foundations for the future implementation of the ESRP. The assessment was qualitative and
Beneficiary Feedback, Achievements and Research Results

drew on survey research and interviews, since there is not as yet an indicator system to assess project outcomes quantitatively, although the existing periodic project monitoring reports to provide useful qualitative information (and at output level, quantitative), on project achievements.

Among the findings were that research results varied considerably, depending on the project type and theme in question. Examples of PASR achievements include:

- The completion of RTD roadmapping exercises;
- Carrying out feasibility assessments;
- Demonstration of proof of concept;
- Establishing the feasibility of new technologies; and
- Strategic development of the future ESRP.

Progress was also made towards structuring civil security research i.e. influencing the strategic development of the future ESRP. A number of support activity projects focused on various areas, such as putting in place secure communications networks for security research (USE-IT and SUPHICE projects), encouraging SME participation in FP7 (SECURE SME) and promoting user engagement in Security Research through the setting up of a user network (PETRANET). Although positive outcomes were achieved through these projects, there was a concern about the sustainability of project results, and a need to strengthen follow-up activities in FP7.

The SeNTRE project (Security Network for Technological Research in Europe) played a useful role in strengthening cooperation and in structuring the ESRP through the establishment of a network of users and technology experts at national and European levels to support the work of ESRAB. Building on this framework, STACCATO (Stakeholders Platform for Supply chain Mapping, Market Condition Analysis and Technologies Opportunities) mapped competences across EU-27, highlighting the capacities of SMEs. R&D projects achieved various positive outcomes, including the development of preindustrial prototypes and the demonstration of proof of concept of technological solutions. For example, through GEOCREW, a virtual platform was developed to integrate different data sources such as geospatial and open sources as part of an early warning system. The ISCAPS project demonstrated a global multi-sensor integrated system for the detection of abnormal behaviour in a crowd.

PASR achieved some progress in promoting the development of pre-standards and common approaches to the testing and certification of equipment. Among the projects that focused in this area include STABORSEC (Standards for Border Security Enhancement) and SECONND (secure containers).

Furthermore, some PASR projects led to the creation of new knowledge tools. Examples include the creation of databases on particular security topics, modelling software, for example, to predict the dispersion paths of airborne micro-organisms, improvements in information management systems and the development of the first European taxonomy of the civil security industry, the development of communication and information exchange systems and improved command and control systems in the area of crisis management and new methodologies for Technology Watch.

Some PASR projects helped to identify capability gaps to be addressed in FP7 SEC. For example, the TRIPS project identified capability gaps in the protection of transport infrastructure. The main gaps identified were railway tracks, railway infrastructure surveillance, and detection of explosives inside carriage and coaches, as well as a communication and protection system architecture design. The AEROBACTICS project was designed to gaps in certain knowledge areas such as the numbers of, species,
Beneficiary Feedback, Achievements and Research Results

viability and pathogenicity of airborne micro-organisms. AEROBACTICS also developed capabilities to predict background fluctuations.

Interoperability was also strengthened through the implementation of PASR, for example, in the area of wireless communications. The SUPHICE project worked on the development of an encrypted algorithm to allow information classified as SECRET to be shared between European and national security agencies. The MARIUS project utilises advanced wireless technology to deploy its autonomous Command Post for crisis management response. The WINTSEC project explored a number of solutions to overcome the barriers to wireless interoperability across different security agencies, as well as potential legal restrictions.

While there was a strong focus in PASR on CSA projects to promote the structuring of the ESRP, some collaborative research projects were also supported and produced useful research results. For example, projects that led to the development of new and emerging technologies include the SECONND project (Secure Container Data Device Standardisation), which led to the development of a early prototype of a data device reader for shipping containers to allow port authorities to ensure better tracking of containers and to detect unauthorised tampering.

The BODE project focused on the development of Dry Detection Technologies and LIDAR (Light Detection and Ranging technologies), with an intelligent warning algorithm. These technologies were used to miniaturise and ruggedize detectors when integrated in networked systems. Emerging technologies were also supported under the HAMLeT project, which demonstrated new capabilities for early detection, localization, and continuous tracking of individuals and groups carrying hazardous material in crowded areas. Another example of a project leading to the development of an innovative prototype was the TRIPS project (Transport Infrastructure Protection System) which addresses security in mainline, subway and metro railways systems. The project involved the development of a small prototype robot capable of checking for explosives on rail networks. This was trialled on the SNCF high speed rail network and attracted strong interest from end-user organisations.

Soft outcomes - PASR

PASR achieved soft outcomes, such as the promotion of networking between security research actors, the creation of networks and strengthened coordination. Since a key aim was to promote security research coordination and structuring, a relatively high proportion of projects funded were support actions. Through networking, PASR helped to achieve progress towards the aim of building effective partnerships between users, industry and research establishments. For example the ASTRO+ set up networking mechanisms between space and security sectors, including users and wider stakeholders.

Some PASR projects improved understanding among relevant policy makers of security threats and challenges both within, and outside the EU. For example, the ESSTRT project (‘European Security, Threats, Responses and Relevant Technologies’) produced a high-level study on European security ‘New Approaches to Counter-Terrorism’. This focused both on counter-terrorism and on a wider range of internal security threats and challenges for the EU.

While some research results have already been taken up by user organisations, there was a perception that awareness about research results achieved through PASR needed to be improved, so as to maximise take-up by users. Among the types of research outcomes most likely to be taken up include
Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research

Section 4

Beneficiary Feedback, Achievements and Research Results

Knowledge tools, such as the web portals and public handbooks on state-of-the-art technologies, as demonstrated by the BIO3R project.

In addition to PASR, some security-related research projects were supported through FP6 (2002-2006) in areas such as ICT security and surveillance and detection technologies. However, these were not generally research into security technologies, but rather concerned with the application of existing technologies.

The research conducted was of high quality, with evidence that some research results have been utilised, especially in follow-up FP7 SEC projects that built directly on earlier research. Examples include the industrial taxonomy developed through STACCATO under PASR. This has been used by several follow-up projects in FP7 SEC, such as the STRAW project, which used the STACCATO classification in the development of a methodology and database for Technology Watch. Another example was the STABORSEC project (pre-standards standards for border security), which developed a framework that has been further built on through the CREATIF project (common testing and certification approaches for CBRNE detection equipment).

Overall, PASR played a central role in laying the basis for a full ESRP in FP7 SEC within the Cooperation Programme. It was an effective funding instrument in supporting pilot projects and in raising awareness about the possibility of obtaining funding through the future ESRP in FP7.

Research results – FP7 SEC

A methodological challenge in interim evaluation is to assess results and initial impacts at a relatively early stage in FP7 SEC’s implementation, focusing on the first two calls for proposals, since these projects are now in their first, second or third year of implementation and have not yet been completed.

Another difficulty in assessing outcomes is that in some thematic areas, such as maritime security, there is a focus on early-stage research with long R&D lead-times. This means that it will only be possible to carry out a full assessment of research outcomes over a 10-15 year time period. There is necessarily a medium-long term time horizon, and a need to track security research outcomes over time, given that progress in some areas is likely to be incremental, rather than involve dramatic step-changes.

The assessment of research results draws on a combination of desk research (for example, reviews of project websites and monitoring reports) and field work (interviews with beneficiaries and users and two online surveys). The survey included a number of questions addressed to beneficiaries in both PASR and FP7 SEC about project achievements. This yielded a lot of information about the types of outcomes likely to be produced. Furthermore, a review of annual call for proposals and of projects funded under particular topics was also undertaken. This provided useful information about further outcomes that have not yet materialised, but are likely to be produced through projects in future.

Hard outcomes

FP7 SEC projects identified concrete outcomes, such as the development of new data, products, services and technologies. However, many stressed that these were still under development and that it was too

38 There was also limited support for CBRN, for example, under the EURATOM Programme, the TMT Handbook project was prepared which provides a handbook for the monitoring and treatment of people exposed to radiation following malevolent acts.

39 STACCATO (Stakeholders Platform for Supply chain Mapping, Market Condition Analysis and Technologies Opportunities) was funded through PASR 2006 and was itself built on the earlier networking experiences gained, and the strategic research work of the SeENTRE project.
Beneficiary Feedback, Achievements and Research Results

early to assess whether they would be taken up by users. Beneficiaries were asked whether outcomes associated with their project could be quantified. The results are shown below:

Table 4.3: Please provide data for research results that can be quantified:

<table>
<thead>
<tr>
<th>Research Result</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of patents developed</td>
<td>6</td>
</tr>
<tr>
<td>No. of patents registered</td>
<td>3</td>
</tr>
<tr>
<td>No of other forms of Intellectual Property developed</td>
<td>14</td>
</tr>
<tr>
<td>No. of data sources</td>
<td>60</td>
</tr>
<tr>
<td>No of products developed</td>
<td>33</td>
</tr>
<tr>
<td>No. of new services developed</td>
<td>10</td>
</tr>
<tr>
<td>No. of new technologies developed</td>
<td>40</td>
</tr>
<tr>
<td>No. of knowledge tools (e.g. databases)</td>
<td>16</td>
</tr>
<tr>
<td>No. of good practice tools</td>
<td>15</td>
</tr>
<tr>
<td>No. of research papers</td>
<td>154</td>
</tr>
<tr>
<td>No. of citations</td>
<td>141</td>
</tr>
<tr>
<td>No. of end-users (organisations making use of research project outcomes)</td>
<td>21</td>
</tr>
</tbody>
</table>

A number of beneficiaries developed and registered new patents. It is also noteworthy that 14 respondents identified other forms of IP. Among the other types of outcomes identified include new technologies developed (40), the development of knowledge tools such as industrial taxonomies, online databases on particular security themes and good practice guides. With regard to scientific excellence in written materials, a large number of research papers (154) have been produced across a range of security topics such as the economics of security, environmental aspects of security, etc. These have received a good number of research citations (141), a key measure of bibliometric excellence. Another finding was that 21 user organisations have already made use of research results.

Beneficiaries were also asked to identify research outcomes achieved. In the following table, examples of new technologies already developed, or under development, include:

Table 4.4: What types of new technologies have been developed through your project?

<table>
<thead>
<tr>
<th>New technologies (1)</th>
<th>New technologies (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method of producing Ni/CdTe/Ni Schottky diode structures with low leakage current</td>
<td>Development of behavioural analysis technology</td>
</tr>
<tr>
<td>at high reverse bias voltage.</td>
<td></td>
</tr>
<tr>
<td>New technology for variable resolution rendering of compressed terrains</td>
<td>Improvement of the coupling between a Differential Mobility Analyzer (DMA) and a Mass Spectrometer</td>
</tr>
<tr>
<td>Miniaturized portable spectrometer</td>
<td>Implementation of a simulation test environment</td>
</tr>
<tr>
<td>Platform for Common Operational Picture capability/understanding for situational</td>
<td>New technology for large urban models visualizations to improve situation awareness</td>
</tr>
<tr>
<td>awareness</td>
<td>in urban areas</td>
</tr>
<tr>
<td>UV fluorescence lider built for demonstration</td>
<td>Development and understanding of change detection using cameras.</td>
</tr>
<tr>
<td>Development of a new technology for vapor ionization, based on ElectroSpray (SESI)</td>
<td>Mine detection on the seabed</td>
</tr>
<tr>
<td>Development of technical prototypes</td>
<td>Adaptation of existing technologies and military legacy</td>
</tr>
</tbody>
</table>
Benefits: Feedback, Achievements and Research Results

<table>
<thead>
<tr>
<th>Development of technical simulation models</th>
<th>Technologies for crisis management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improvements in sensor technologies</td>
<td>Laser method of solid phase doping of the surface region of semi-insulating Cd(Zn)Te crystals and formation of an ultra-shallow and sharp built-in p-n junction.</td>
</tr>
<tr>
<td>Development of new carbon-producing technologies</td>
<td>Developed a method of producing M-p-n structured In/CdTe/Au diode detectors for X-ray and γ-ray radiation/</td>
</tr>
<tr>
<td>Development of optical spectrometries for detection of explosives (Fundamental research)</td>
<td>Development of LIBS, RAMAN, IR (core technologies) and laser, spectrometry, optics and data fusion (enabling technologies)</td>
</tr>
</tbody>
</table>

The above examples demonstrate that many PASR and FP7 SEC projects have already led, or will in future lead to the development of new technologies. Of course, new technologies developed will commonly be at the pre-operational stage since FP7 mainly supports pre-operational research and rather than services.

In the following table, examples of the types of services and products, data, knowledge and good practice tools developed through FP7 SEC projects are provided:

Table 4.5: What types of services and products, data, knowledge and good practice tools were developed through your project?

<table>
<thead>
<tr>
<th>Services and products</th>
<th>Data</th>
<th>Knowledge and good practice tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of visualisation tools to improve situation awareness in crisis command control centres</td>
<td>Data on species and the numbers of microbes in the air</td>
<td>Disaster management trial experiments conducted leading to development of good practice manual</td>
</tr>
<tr>
<td>Deployable gas sensors</td>
<td>Data on the preparation of impregnated activated carbons</td>
<td>Identification and analysis of decision support needs to enhance humanitarian camp management</td>
</tr>
<tr>
<td>Implementation of new security technologies in hardware and silicon chips</td>
<td>Database of environmental disasters</td>
<td>Knowledge tool to reduce security manpower requirements and to improve cost-effectiveness</td>
</tr>
<tr>
<td>Development of next generation monitoring and surveillance systems for deployment in airports and in urban areas</td>
<td>Database of CBRN incidents (including relating to the disappearance of CBRN materials)</td>
<td>Database of environmental disasters</td>
</tr>
<tr>
<td>Development of more easily and quickly deployable crisis communication support tools.</td>
<td>Utilising surveillance data on abnormal behaviour</td>
<td>Database of CBRN incidents (including relating to the disappearance of CBRN materials)</td>
</tr>
<tr>
<td>Development of services for security planning at major events</td>
<td>Database on EU testing facilities/amenities</td>
<td>Production of multiple research papers on the economics of security</td>
</tr>
<tr>
<td>Improvement of quality of service for earth observation with applications in the field of wider-area maritime security and land border surveillance</td>
<td>Database of EU security curricula for the training of first responders</td>
<td>Production of research papers on security and the environment</td>
</tr>
<tr>
<td>Neutron sensor developed for underwater application (chemical analysis) and used with submarine.</td>
<td>Database of registered crimes and ballistics data</td>
<td>Analysis and development of good practice guide and methodology on the research into the human impact of</td>
</tr>
</tbody>
</table>
Beneficiary Feedback, Achievements and Research Results

The research identified achievements in the development of **products and services**. Examples of services include security planning advisory support to the police for major events and improvements in GMES services with downstream applications in the field of wider-area maritime security and land border surveillance. Examples of products include the development of next generation monitoring and surveillance systems, command and control systems offering better situational awareness, and the development of advanced sensor technologies.

Examples of new data include data on the numbers of species, variety of airborne pathogens, and improved data on environmental disasters as well as CBRN incidents (including the disappearance of CBRN materials). Among the **knowledge tools and good practice guidance** developed include: the development of the STACCATO taxonomy through PASR which provides a classification for the security industry, a good practice guide and methodology on the research into the human impact of disasters, a good practice guide on security planning for major events, the development of databases (e.g. on environmental security, CBRN incidents), and research papers on particular aspects of security, including the economics of security, environmental security etc.

**EUSECON - applying economic modelling to improve understanding and responses to security phenomenon**

The EUSECON project aimed to develop an analytical framework for complementary research in the discipline of security economics. This framework relates to human-induced insecurity (terrorism and organised crime) and other forms of insecurity (industrial accidents, natural disasters, geo-political insecurity) and security measures. The project focused on historical context, the societal perceptions of insecurity and on filling gaps in the data used to measure the impact of economics on social and political movements. Between 2009-2010 the project produced 24 working papers addressing security of economics issues with a strong emphasis on the relationship between terrorism and the socio-economic conditions of Muslim communities.

Some projects identified patents and other forms of Intellectual Property. Examples are provided below:

**Table 4.6: Patents and other forms of Intellectual Property**

<table>
<thead>
<tr>
<th>Patents and other forms of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of a patent relating to secure containers for container shipping industry (SECCOND)</td>
</tr>
<tr>
<td>Development of software applications built from main IT platform used in project (COPE)</td>
</tr>
<tr>
<td>Basic sensor technology was patented by the Lead coordinator before the project started (after earlier project funded by public sector in the UK). Expect to patent some subsidiary developments after the FP7 project (Idetect4all).</td>
</tr>
<tr>
<td>Development of an IPR policy to assess the viability of a full scale production of nanoporous adsorbent materials (FRESP)</td>
</tr>
</tbody>
</table>

The development and registration of IP may not necessarily be seen as the primary project achievement, since often the development of knowledge and the basic building blocks to take research to the next stage towards operationalisation is as important as IP generation itself.
Beneficiary Feedback, Achievements and Research Results

<table>
<thead>
<tr>
<th>IPR challenges within ESRP projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>The TERASEC project developed a new type of screening and detection technology using state-of-the-art terahertz (THz) rays. The project partners were confident that, given a longer timeframe, the research results could be exploited commercially through leveraging IP e.g. licensing. However only one partner organisation, an SME (Teraview), has successfully patented a prototype product based on research carried out under TERASEC. This was due to the relatively high costs of maintaining IPR while the new technology was at an early stage of development and considered to be far from the market.</td>
</tr>
</tbody>
</table>

While general guidance has been produced in FP7 overall on IP issues for project consortia, reaching an agreement on IP sharing arrangements including licensing can be complicated. For example, one partner may bring a patented platform or system into the consortium and then subsequently other partners may through the project develop subsidiary software or products using the basic platform and license these. The extent of use of IP in carrying out the research is therefore a viable indicator.

Examples of projects that developed patents include SECCOND (Secure Container Data Device Standardisation) which developed a patent relating to secure containers for container shipping. Another example was COPE (Common Operational Picture Exploitation), where IP has been registered for software applications by one partner, which were based on the patented IT platform provided by another consortium partner. The generation of derivative technologies through projects was a common theme. For example, the Idetect4all lead coordinator patented the basic sensor technology before they started the project, after an earlier project funded in the UK. The lead coordinator expects to patent further subsidiary developments. While there will be quite some time before any commercial leverage is achieved in both these projects, since the research was at a relatively early stage, this examples shows the potential of some of the PASR and FP7 SEC projects funded to date.

In the next table, examples of progress are provided in the following areas: systems integration and networks, interoperability, standardisation, harmonisation and the development of common testing and certification systems.

Table 4.7: Systems integration and networks, interoperability, standardisation and harmonisation.

<table>
<thead>
<tr>
<th>Systems integration and networks</th>
<th>Interoperability</th>
<th>Standardisation and harmonisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large scale net-based integration of defined subsystems across different parts of EU</td>
<td>Interoperability / compatibility of civil and military applications relating to crisis response</td>
<td>Development of a common strategy towards standardisation for industrial sectors and companies.</td>
</tr>
<tr>
<td>System of systems integration in sea-based sensors</td>
<td>Public Safety Network Interoperability issues</td>
<td>Mapping exercise for pre-standardisation in the area of CBRN (Créatif)</td>
</tr>
<tr>
<td>Decision support applications for web based command and control systems.</td>
<td>Interoperability of police information services (HITS/ISAC)</td>
<td></td>
</tr>
</tbody>
</table>

A number of projects promoted systems integration, including systems of systems and networks. In the area of maritime surveillance, for example, while still at a very early stage, sea-based sensor stations using heterogeneous sensors should become interoperable and networked, and in the area of crisis management, there has been work to develop integrated communication systems with common interfaces. Some research results can already be discerned in promoting harmonisation and standardisation through FP7 SEC, but further work is needed. These are examined in Appendix I.
**Beneficiary Feedback, Achievements and Research Results**

**Soft outcomes**

Soft outcomes are less tangible, but nevertheless appreciated by beneficiaries and users. Examples include: improved networking and coordination, the sharing of information and good practice exchange between the security industry and users; progress towards research excellence and the greater ability to predict future threats and challenges in different areas of security.

Table 4.8: What other types of research outcomes can be identified linked to your project to date?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress towards 'state of the art'</td>
<td>43</td>
<td>59.7</td>
</tr>
<tr>
<td>Fostering research excellence</td>
<td>22</td>
<td>30.6</td>
</tr>
<tr>
<td>Improved networking and coordination between security research actors</td>
<td>38</td>
<td>52.8</td>
</tr>
<tr>
<td>Improved information sharing and good practice exchange between security research actors</td>
<td>25</td>
<td>34.7</td>
</tr>
<tr>
<td>Strengthened cooperation between SMEs and large firms</td>
<td>28</td>
<td>38.9</td>
</tr>
<tr>
<td>Strengthened innovation transfer between industry and publicly funded research</td>
<td>17</td>
<td>23.6</td>
</tr>
<tr>
<td>Increased visibility of new and emerging areas of security research (e.g. the economics of security, the environmental aspects of security etc.)</td>
<td>20</td>
<td>27.8</td>
</tr>
<tr>
<td>Greater ability to predict future challenges, threats and developments in different areas of security field</td>
<td>25</td>
<td>34.7</td>
</tr>
<tr>
<td>Promotion of standards, harmonisation and interoperability</td>
<td>14</td>
<td>19.4</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>4.2</td>
</tr>
</tbody>
</table>

*Note: multiple responses were possible*

Almost six in ten projects stated that they had made progress towards the achievement of 'state of the art'. Among the most common soft outcomes identified include (in order of the frequency that they were mentioned) (1) Progress towards 'state of the art' (2) improved networking and coordination between security research actors (3) Strengthened cooperation between SMEs and large firms (4) Improved information and good practice sharing between security research actors (5) Greater ability to predict future challenges, threats and developments in different areas of security field (6) Fostering research excellence and (7) Increased visibility of new and emerging areas of security research (e.g. the economics of security, the environmental aspects of security etc.). Other benefits mentioned through the field research include strengthened partnership working and cooperation between regional, national, EU and international actors on internal and external security matters.

Some interviewees viewed soft outcomes as being as important as hard outcomes in terms of the perceived benefits of taking part in FP7 SEC projects. Being part of a transnational consortium meant an opportunity to exchange information and network with relevant providers and users, to obtain feedback directly from users with regard to their functional requirements, and the opportunity to get to know other firms in their industry at European level.

In some instances, especially among large firms, the benefits of taking part were difficult to quantify, but extended well beyond the purely monetary benefits of receiving an EC contribution towards the cost of research. Examples include: getting to know the market, increasing their visibility in particular markets and diversifying their client base, service and product offering, developing lasting relationships with SMEs and with users.
Beneficiary Feedback, Achievements and Research Results

Wider outcomes

Among the wider outcomes achieved through PASR and FP7 SEC projects include: technology transfer; improving foresight capabilities and addressing knowledge gaps and security vulnerabilities and capability enhancement. Although FP7 SEC funds pre-operational research, there is significant potential to promote technology transfer. There are two main aspects to this:

- Technology transfer between publicly funded research (e.g. carried out by universities and research institutes) to the private sector
- Harnessing legacy technologies and adapting these for civil security purposes e.g. in the field of crisis management

Given that many projects funded to date have involved a wide range of partners – SMEs, large firms, research institutes, universities, public agencies, NGOs etc. – there is ample scope through the programme for the promotion of technology transfer between publicly funded research and the private sector. A good example in this regard was the IMSK project (Integrated Mobile Security Kit (IMSK), which involves a wide-ranging consortium consisting of large enterprises, SMEs and public research institutions.

A number of projects have as part of their initial phases sought to identify gaps in security capabilities in particular areas. Examples in this regard include the STACCATO project (Stakeholders platform for supply Chain mapping, market Conditions Analysis and Technologies Opportunities) in PASR which defined methods and solutions integrating the overall security market and supply chain and mapped out a gap analysis in relation to the development of a European Security Technological Industrial Base (STIB).

4.4.5 Quality of research results

In this sub-section, an assessment of the evaluation issues raised in the terms of reference in respect of the quality of research results is provided.

What was the quality of research outputs achieved?

Overall, PASR and FP7 SEC projects supported to date have achieved high quality research outputs. There are inherent limitations in the analysis due to the time scope of an interim evaluation in that this focused only on the first two calls for proposals (and projects are ongoing).

The quality of research was assessed through the project level interviews, and supported by a review of desk research from a sample of deliverables produced by projects. Additional information that informed the review of the quality of the research included the survey work. This gathered some quantitative information on citations / bibliographical excellence, the number of patents / IP developed and used, and through the survey of users, information about the extent of take-up of project results by users.

There was evidence of innovation in some domains within civil security research (e.g. new generation CCTV cameras using complex algorithms (SAMURAI), scintillation crystals for high-resolution radiological detection (CoCAE) and the development of Common Operational Picture Exploitation (COPE) using legacy technologies to improve command and control performance for first responders and the use of ultra high frequency radio waves to improve visual detection (Terahertz). Further project examples of innovation and technological innovation are provided in the separately bound case studies.
Beneficiary Feedback, Achievements and Research Results

Among the findings were that:

- The research outputs produced reviewed by the evaluation team were of high quality;
- Some instances were identified of research outputs that represented ‘state of the art’;
- In some domains, such as maritime security, it will only be possible to assess research outcomes and their quality over a medium-long term timeframe, the same applies to projects that involve more fundamental research (e.g. Terahertz, CoCAE);
- There are examples of successful prototypes having been developed that strongly suggest research excellence such as a robot for use in standoff detection of explosives for use in the rail sector (TRIPS/ PASR) and the development of an integrated device for first responders with potential to significantly improve the early detection of victims of disasters (SgL for USAR);
- Only a small number of projects did not lead to research outputs that are relevant to the needs of end-users, although overall research quality could be further improved through the systematic involvement of users from the outset.

Did the research projects funded through PASR and FP7 SEC attract leading-edge organisations engaged in security research from the private sector, universities and academia? Likewise, were the researchers involved in implementing projects world-class in their respective fields?

The evaluation team carried out a large number of discussions as part of the evaluation mainly on a face to face basis. The collective view of the team was that the lead researchers involved in implementing projects were often world-class in their respective fields. Examples include a materials science institute in Spain that developed cutting-edge scintillation crystals technologies, and is one of only a small number of research institutes in the EU capable of competing with the US and China in this specialist field. Likewise, in the UK, Cambridge University is involved in the Terahertz project, and while this involves fundamental research, it appears likely to lead to some interesting spin-off effects in different sectors, such as pharmaceuticals, as well as have applicability in improving detection technologies over the medium-long term. The research was regarded as being cutting-edge.

With regard to participation by industry, many of the best-known companies from the defence and civil security research industries are represented in the FP7 SEC programme, such as BAE, EADS, SAAB, SELEX-Galileo and Thalys. Since these are leading players in security research (both civil and military), this suggests that the ESRP has been successful in attracting leading-edge private sector research expertise.

With regard to SME participation, as noted in Section 3.6, FP7 SEC has performed strongly compared with other areas of FP7 Cooperation in terms of involvement by SMEs. CSES interviewed a number of SMEs as part of the discussion programme and these were found to be of high calibre and be producing high quality research. A number of SMEs were involved in delivering technical / R&D focused WPs and it was clear from the discussions with large firms that their main value added was in bringing state of the art R&D expertise in particular areas to project consortia.

What contribution has been made through PASR and FP7 SEC projects to enhancing the knowledge base of different areas of Security Research?

Research outputs were found to be of high quality in emerging areas of Security Research, such as the environmental aspects of security (SECURENV) and the economics of security (SECON). The knowledge base has also been strengthened in different areas of Security Research. For example, a number of
Beneficiary Feedback, Achievements and Research Results

Projects have developed databases in particular areas that can be used by end-user organisations. For example, through the EUSECII project, a database of security planning in major events has been developed, which is already being used by national police services in helping them to learn from previous major events how to develop methodologies and strategies to improve planning and coordination of forthcoming major events. Through the FESTOS project, a database has been developed on risks from emerging technologies, which has attracted the interest of intelligence agencies and law enforcement agencies in strengthening horizon scanning capabilities. SECURENV has analysed major industrial and environmental accidents from a security perspective using foresight methods and scenario-building techniques to give end-users a better understanding of future risks. It has also developed a database mapping out previous incidents in order to strengthen risk management approaches and to enhance knowledge about environmental security threats among user organisations.

Less positively, not all projects achieved all their objectives in enhancing knowledge, such is the nature of the RTD Framework Programmes in which innovation and risk taking in funding projects means that not all projects will be as successful as hoped. For example, the STRAW project (European Service of Technology Watch on Security Technologies) achieved some successful outcomes, such as the holding of workshops bringing together relevant stakeholders. However, the database developed to provide a Technology Watch for public sector organisations has not been as widely used as had been hoped.

Did the research produce recommendations likely to lead to influence the formulation of new policies and legislation/ Regulations?

PASR and FP7 SEC have not yet directly led to the development of new policies and legislation/Regulations but through recommendations made through projects, and through research activities funded, they do have strong potential to influence the formulation of new policies and legislation/Regulations.

The coordination of drugs policy at EU level falls under the responsibility of DG Justice. The Commission official responsible was positive about the potential of several projects to improve detection technologies to find illicit drugs (at land borders) and in the use of improved surveillance and monitoring in the area of maritime surveillance to combat illegal drugs shipments. This was viewed as broadly supportive of the European Drugs Strategy. The intention in future is to publicise such projects through the DG Justice website and to draw them to the attention of relevant stakeholders that participate in a working groups on drugs led by the Directorate-General, such as Ministries of Interior and Justice.

In the CBRN field, cooperation has taken place between the Security Research Unit and the Unit dealing combating terrorism (including CBRN) within DG Justice, for example, the preparation of the CBRN Action Plan. There was a direct link in the views of the Commission officials working on counter-terrorism policy that FP7 SEC would make a direct contribution to the achievement of the aims in the CBRN Action Plan. The CBRN Task Force prepared a list of 120 measures that could be undertaken at EU level and in the Member States in order to lower the risks of terrorist acts using CBRN materials. A mapping exercise was undertaken of ways in which FP7 SEC might contribute and it was found that of the 120 measures, FP7 SEC research topics have potential to strengthen 40 of these capabilities.

Officials from DG Justice viewed the potential contribution of FP7 SEC in developing new and innovative technologies and in strengthening cooperation and capabilities to tackle terrorism positively. It was pointed out that the Directorate-General only has a limited budget to conduct soft projects such as studies and analyses on particular issues relating to terrorism. FP7 SEC fills a funding gap and ensures
that research to support the work of the policy unit is available. The programme should therefore contribute towards achieving the aims of the EU Counter-Terrorism Strategy.

In crisis management, FP7 SEC projects are making a positive contribution to strengthening cooperation and promoting interoperability between relevant first responders and civil protection agencies. It was also noted that among the main areas of value added in respect of FP7 SEC are the opportunity for crisis management agencies to cooperate together more closely through transnational projects, to share information and experiences and for knowledge exchange. Since the main basis for learning is experience and absorbing the lessons learned from previous crises, cooperation ensures that new knowledge gathered from crises is disseminated.

Overall, FP7 SEC is beginning to transfer research results to users through dissemination activities. It is also making a positive contribution in producing policy-relevant outcomes and in developing state of the art technologies, which while not yet operational, has strong potential in future to be used by users, and/or to be commercialised.

**Conclusions – quality of research**

Overall, PASR and FP7 SEC projects have promoted research excellence and the strengthening of cooperation between relevant actors with an interest in similar specialised fields. Over time, transnational collaborative research between these actors has potential to strengthen the competitiveness of the European security industry and to promote the achievement of state of the art in civil security research.

The fact that leading-edge research institutions and universities are well represented among the beneficiaries in FP7 SEC strongly suggests that the programme is already attracting scientific excellence. Likewise, participation by the most renowned firms in the sector, many of which while historically focusing on the defence sector are refocusing some of their research activities on civil security research. Their involvement brings significant scope to leverage knowledge and adapt and apply this for civil purposes to the benefit of EU citizens.

Increased competition for funding in each call also suggests that research quality will be progressively strengthened over time.

**4.5 Dissemination and exploitation of research results**

A key consideration is the extent to which, and how, PASR and FP7 Security research results have been disseminated (e.g. websites, conferences and workshops). This in turn will impact on the extent to which results have been taken up by users and the overall effectiveness of the programme.

**PASR**

In relation to the dissemination and exploitation of PASR research results, while some promotional and communication activities have already been undertaken, such as inviting PASR beneficiaries to present their results at security stakeholder conferences, more could be done in this area to promote their wider dissemination and uptake by users.

Very few PASR projects appear to have set up and maintained a project website, and performance in FP7 SEC is markedly improved in this area. While some research results are available online, overall, it does not appear to be that easy for the user community to obtain detailed information about these projects, with some exceptions, such as the Staccato taxonomy, the PRISE project on the ethical and societal dimension of security, among others.
Beneficiary Feedback, Achievements and Research Results

There is a need to develop a web portal which provides a single point of access and document repository with information about PASR projects and research outcomes. Practical examples of how results could be made use of by users and illustrations of how users have already utilised security research could also be provided. The promotion of research activities (and preliminary results) by beneficiaries themselves is stronger in FP7 SEC than in PASR. The majority of projects have developed websites so as to provide information about projects to users and the wider public. It is important that the programme ensures transparency about what projects are trying to achieve.

**FP7 Security Research**

The organisation of a series of 5 thematic workshops in 2010, together with the holding of an annual security conference are among the examples of ways in which the Commission is seeking to improve its communication activities, to engage with users and to foster a security research community at EU level. Such events need to become a reasonably regular feature of the Commission’s activities, to ensure that research results are disseminated to their intended target audience.

Project beneficiaries are already required to produce a publishable summary of their project’s achievements and potential impact in future. While this is useful, sometimes, the approach adopted to describing project achievements is not always clear, with information sometimes rather vague and relating to generic threats and applications of technologies under development, rather than detailing the specific ways in which new technologies will make a difference to the security of EU citizens, or could be attractive to users. The presentation could also be further standardised. There is a need to disseminate these ‘achievement summaries’ more widely.

NCP websites are another vehicle through which project results could be highlighted. Indeed, some interviewees pointed to the fact that project information is not currently available on FP7 SEC at national level. While the Cordis website contains a wealth of information including individual project records, some stakeholders commented that it is not that easy to navigate.

Among the improvements that could be made include the idea of having a central online repository to help disseminate research outcomes, many of which are non-classified.
End-users in EU Security Research

5. End-users in FP7 Security Research

In this section, CSES examines the role of users in EU Security Research (PASR, FP7 SEC). A strong emphasis has been placed by the Commission on the importance of involvement of ‘end-users’ and the European Security Research Programme was conceived as a user-driven, application-based research programme. The importance of involving users directly in projects was therefore stressed in the annual work programme and in guidance for applicants relating to Calls for Proposals.

5.1 Typology of end-users

End-users represent the demand-side of security research and are mainly public agencies, such as the emergency services, law enforcement agencies (e.g. first responders, police, anti-terrorism bodies, intelligence agencies, customs and border control), and public agencies responsible for safety and security. The user community includes national and EU policy makers responsible for different policy areas that have a security dimension, such as counter-terrorism, tackling organised crime, counteracting malevolent use of CBRN, etc. EU agencies are also among the users. The most relevant include FRONTEX (land / maritime border security), EMSA (maritime safety), EUROPOL (Law Enforcement) and international organisations, such as the UN (cooperation in the crisis management field) and organisations involved in international cooperation (e.g. discussions with the Transportation Security Administration (TSA) on possible standards.

A typology of users was developed by CSES in order to structure the analysis of how users have been involved in the programme, and the extent to which research outcomes are likely to be useful to users:

Table 5.1: Typology of users

<table>
<thead>
<tr>
<th>User type</th>
<th>Types of users within category</th>
</tr>
</thead>
</table>
| Emergency services               | • First responders  
|                                  | • Ambulance services                                                                         |
| Security services                | • Intelligence agencies                                                                       |
| Law enforcement agencies         | • Police  
|                                  | • Counter-terrorism bodies  
|                                  | • Forensic laboratories and ballistics agencies  
|                                  | • EU and international organisations, such as EUROPOL INTERPOL                                |
| Customs and border control       | Authorities responsible for:  
|                                  | • Land border security  
|                                  | • Maritime security  
|                                  | • Aviation security  
|                                  | Examples of EU organisations include FRONTEX (border control) and EMSA (European Maritime Safety Agency) |
| Public agencies responsible for safety and security | • Nuclear safety agencies  
|                                  | • Atomic Energy Authorities  
|                                  | • Radiation agencies  
|                                  | • Critical National Infrastructure Protection agencies                                         |
| Policy making and co-ordination  | • European Commission  
|                                  | • National authorities (some countries also have Security Tsars – an individual or body responsible for overall co-ordination of ‘homeland security’)  
|                                  | • Regional authorities                                                                         |
End-users in EU Security Research

- Local authorities – responsibility for co-ordinating local responses.

| Enterprises and industry | • SMEs and large firms active in the security industry
|                          | • Industry more widely e.g. aviation sector, maritime sector, energy and utilities
| NGOs                     | • NGOs are especially active in some areas such as crisis management and disaster response
| International organisations | • UN
| Organisations that run facilities | • Airport operators
|                          | • Port authorities
|                          | • Managers of critical infrastructure
|                          | • Managers of public buildings
| Procurement bodies | • European Commission and national authorities
|                          | • Regional and local authorities
| EU citizens | • General public
|                          | • Media
| Standards organisations | • European Standards Organisations
|                          | • National Standards Organisations
|                          | • Organisations that have responsibility for some areas of standards through international cooperation

The starting point for the typology was that it may be useful to distinguish between different types of end-users in order to better understand the intended target audience of security research results.

While the primary users of security research are public sector organisations, the typology illustrates that there are also wider end-users that may make use of research results, such as the security industry, SMEs and academic and research institutions. For example, knowledge-based projects and R&D oriented research outcomes may be of strong interest to firms since it enables them to strengthen their own expertise in specialised areas, but also to provide an opportunity to take stock of progress in state of the art in particular areas with a view to strengthening their competitive offering and developing new project ideas for future calls that build on earlier results.

Wider industry also benefits from investment in security research. For example, if common minimum standards are developed in the aviation industry in respect of testing and certification for particular types of detection equipment as a result of FP7 Sec, then there is a clear potential commercial benefit for airlines in terms of cost reductions linked to efficiency savings (not having to test equipment to meet 27 different national standards).

The wider security research community, including academic and educational institutions, are also among the wider users. For example, socio-economic analyses, such as research papers on the economics of security, may help to promote the development of different aspects of security research within academia. Some NGOs have also been directly involved in the programme as users providing feedback to other members of consortia, for example, those working in field of crisis management and disaster response, such as the Danish Red Cross.

With regard to procurement agencies, it is important that more is done to promote the development of pre-procurement to stimulate demand for early stage security research. This is common in the US and serves as a strong incentive for firms to invest in R&D. Sometimes procurement is organised by centralised or common agencies that act on behalf of final users, but impose their own procedures that may either help or hinder the take-up of new technology.
End-users in EU Security Research

Some stakeholders in ESRP may be both beneficiaries and users of research outcomes. For example, water companies fall into the category of users since they are service providers and could benefit from projects, for example, in the area of critical infrastructure protection. However, they are also sometimes directly involved in R&D activities, for example, to protect against accidental or deliberate contamination, and are therefore also taking part in FP7 SEC as beneficiaries.

5.2 Involvement, role and contribution of end-users in projects

In the first part of the sub-section, the survey findings in respect of the extent and nature of end-user involvement in projects are outlined. In subsequent parts, feedback is provided on the main challenges identified through the research in securing the engagement of end-users. Detailed project examples are then provided of ways in which users have been involved during project implementation, and the role and contribution that they have made to enhancing research results.

5.2.1 Survey feedback on end-user involvement

Feedback on the role and value added of users in projects was sought through two surveys: (i) general survey targeted at all project beneficiaries in PASR and FP7 Security and (ii) survey of users – divided into two parts, a section for users having participated in PASR and FP7 Security, and a section for prospective users not involved in the programme. The purpose was to ensure that the sample provided balanced feedback, not only from those directly benefiting financially from participation.

The evaluation explored the extent to which (and how) users have been involved in projects, both directly and indirectly. While some projects did not include any users, approximately three-quarters of projects involved end-users directly in the project consortium. End-users have also been involved indirectly, for example, through their participation in an external advisory forum of users.

Among the findings from the beneficiaries’ survey were that users were involved directly in more than two-thirds of projects (69.4%) (this was reflected in the review of project fiches and the CORDA database, which identified user organisations).

Table 5.2: Were users directly included in the project consortium?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>50</td>
<td>69.4</td>
</tr>
<tr>
<td>No</td>
<td>18</td>
<td>25.0</td>
</tr>
<tr>
<td>No response</td>
<td>4</td>
<td>5.6</td>
</tr>
<tr>
<td>Total</td>
<td>72</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Survey respondents in respect of projects in which users had been involved were asked about the role played by users during the implementation of projects activities. Among projects that did involve users, most were found to have involved them directly. There was variation in the extent of their involvement between those ‘significantly involved’ (50%) and those with ‘limited involvement’ (40%).

Table 5.3: If yes, were end-users directly involved in project activities?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, they have been significantly involved in the project consortium and in project activities</td>
<td>25</td>
<td>50.0</td>
</tr>
<tr>
<td>Yes, but their involvement has been limited</td>
<td>20</td>
<td>40.0</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
<td>10.0</td>
</tr>
</tbody>
</table>
End-users in EU Security Research

It appears to be quite common to set up a formal advisory panel of users. Among survey respondents, almost four out of ten (38.9%) had set up an advisory panel.

Table 5.4: Was a formal advisory panel of users set up?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>28</td>
<td>38.9</td>
</tr>
<tr>
<td>No</td>
<td>37</td>
<td>51.4</td>
</tr>
<tr>
<td>No response</td>
<td>7</td>
<td>9.7</td>
</tr>
<tr>
<td>Total</td>
<td>72</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Users had played a valuable role in inputting to projects at particular stages during implementation, such as defining user requirements, taking part in scenario modelling, responding to surveys, inputting into the development of knowledge databases and advising on ethical considerations, for example, in relation to dual use technologies.

The survey found a mixed picture in terms of the nature and extent of the role that end-users have played during project implementation. While about a third of users played a major role, most played a relatively minor (but important) role in influencing overall project implementation. This finding was confirmed through the interview programme.

Table 5.5: If yes, what role has the advisory panel played during the project’s implementation?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major role</td>
<td>9</td>
<td>32.1</td>
</tr>
<tr>
<td>Minor role</td>
<td>17</td>
<td>60.7</td>
</tr>
<tr>
<td>Minimal role</td>
<td>2</td>
<td>7.1</td>
</tr>
<tr>
<td>Total</td>
<td>28</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Some interviewees stated that the main value added of users was in providing validation and feedback on deliverables from a usability perspective. This was confirmed in the survey, which sought information on how users had been involved to date.

Table 5.6: Which aspects of project implementation have users been involved in to date?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member of (internal) advisory group of end-users</td>
<td>23</td>
<td>31.9</td>
</tr>
<tr>
<td>The project design process</td>
<td>18</td>
<td>25.0</td>
</tr>
<tr>
<td>Contributing to operational knowledge or procedures</td>
<td>43</td>
<td>59.7</td>
</tr>
<tr>
<td>The testing phase</td>
<td>30</td>
<td>41.7</td>
</tr>
<tr>
<td>The definition of future scenarios</td>
<td>36</td>
<td>50.0</td>
</tr>
</tbody>
</table>

Multiple responses possible.

The discussions with beneficiaries through the interview programme confirmed that the role of users during project implementation was typically to:
End-users in EU Security Research

- Advise during the early structuring stage on project design and Work Package configuration
- Participate in advisory groups both internal and external to the consortium
- Provide feedback to the rest of the consortium during key junctures of project implementation
- Provide input on user requirements. Users were also often asked to take part in workshops, scenario modelling and foresight exercises.
- Test and validate prototypes and demonstrators, for example, by attending field trials

5.2.2 Key challenges in securing end-user participation

The evaluation also explored issues around what factors encourage, or conversely hinder, the participation of end-user organisations in projects.

The research identified difficulties in attracting users to take part in some projects. In some projects, users were reluctant to take part because of lack of time and human resources. Uncertainty with regard to how much time commitment would be required and the trade-off between time spent and future benefits were barriers to participation.

An example in this regard was the IMSK project. Although some users are directly involved and have played a key role in defining systems and operational requirements, one interviewee stated that despite their attempt to secure the wider involvement of end-users, several prospective users from law enforcement agencies approached had declined to take part. This was despite the fact that the project itself could be very helpful to users involved in planning for and policing large-scale events.

The challenge in getting users on board was common to a number of projects interviewed. The main barrier was the perception that taking part, while interesting, was less urgent than day to day operational tasks. Users were much more interested in taking part when the research focused on adapting existing technologies, as opposed to developing new technology with a 10-15 year development timescale. Even projects with a 3-5 year deployment timeframe found it much more difficult to attract users to take part since users were reluctant to commit time until research results had been further developed. This is not to suggest that they were not interested in principle in the research itself and most users were either broadly or very supportive of what the programme is trying to achieve.

Users stressed that since there are pressing demands on their time in meeting day to day challenges and in responding to new and emerging threats, they are interested in taking part in research activities only when there is a strong possibility of the research being directly applied. A prospective user interviewed stated that they are ‘not interested in research for research’s sake’.

A misunderstanding on the part of some public sector organisations with regard to whether they could receive funding to help cover the costs of attending events was identified. It should be clearly communicated that users can have all their travel costs reimbursed, for example, to participate in workshops and other user events such as scenario modelling exercises. The underlying problem identified is however real – many users are not that well resourced, and issues such as cost reimbursement are seen as quite significant.

40 The project is developing an Integrated Mobile Security Kit (IMSK) project that will combine technologies for area surveillance; checkpoint control; CBRNE detection and support for VIP protection into a mobile system for rapid deployment at venues and sites (hotels, sport arenas) which temporarily need enhanced security.
End-users in EU Security Research

The possibility of covering both the costs of travel and the time input made by users involved directly in consortia should be stressed to all new beneficiaries at the introductory meeting in Brussels when projects commence and also to potential end-users in guidance for applicants.

5.2.3 Project examples - the role and contribution of end-users

The role and contribution of users in projects is now examined. Examples of projects that had strong user involvement are provided.

The EU-SECII project involved 22 user organisations from different Member States. There was strong interest among participants in developing common approaches, methodologies and strategies in the area of security planning for large-scale events. It was notable that projects with the buy-in of end-users were more likely to be seen as relevant because there was a real sense of ownership: ‘the project had been designed by and for end-users’. More information about EU-SEC II is provided below.

Table 5.7: EU-SEC II - example of user involvement

<table>
<thead>
<tr>
<th>Project name:</th>
<th>EU-SEC II - Coordinating National Research Programmes and Policies on Security at Major Events in Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project timeframe:</td>
<td>June 2008 – June 2011</td>
</tr>
<tr>
<td>Total Cost and EU Contribution::</td>
<td>€ 2.53 million euro / 2.53 million euro (100% EU financed)</td>
</tr>
<tr>
<td>Project type*:</td>
<td>Coordination Action</td>
</tr>
<tr>
<td>Project description (overview):</td>
<td>EU-SEC II aims to develop common approaches, methodologies and strategies for security planning for major events and to bring together national authorities from EU MS to ensure better coordination on security events, share experiences, exchange information and good practices.</td>
</tr>
</tbody>
</table>

Project detail: EU-SEC II involves 22 end-user organisations, including Ministries of Interior and Justice, police academies and the police. The project developed a common security strategy and methodology for planning major events. The main written deliverable to date has been the publication of EU SEC - Toward a European House of Security at Major Events - Best Practices for Research Coordination, UNICRI Turin, 2008.

Among the activities to date include: establishing Public-Private Partnerships for major events, media management strategy for security, and carrying out an appraisal of specific technologies that can be used at major events and the development of common standards for planning and consideration of ethical issues. The deliverables were informed by the knowledge and previous experience of end-users involved in the consortium.

Because users are project owners, there has been a strong commitment to make the research results as relevant and operational as possible. The project provides a forum for discussion and information exchange on the development of policies, strategies and methodologies between users with an interest in security planning for major events. There are elements of peer review, but the role is to develop common strategic approaches.

Success factors include the fact that users were the driver of the definition of priorities and needs. This increases the likelihood that knowledge exchanged through the project will be used by police forces and Ministries of Interior responsible for planning major events. Among the main benefits identified by users were the opportunity to cooperate with and get to know their counterparts in other EU countries, exchange of best practices at a technical level that can be adapted to planning future major events.
End-users in EU Security Research

Outcomes to date:

**Overall project achievements** - Common research standards were defined by the consortium partners. A common methodological and strategic approach was developed to security planning for major events. This has been adopted at national level by some partners as a training tool on which to base security planning both for major events and security planning more widely. Some have incorporated elements of the methodology into their national security strategies. Good practices were also disseminated.

**Research outputs**

**Data** - a survey was carried out on national research programmes on major event security. This mapped out specific major events (sporting, political) that had taken place and drawn up a security plan. An agreed common definition of 'major events' was established.

**Services** – technical assistance services were developed to provide advice to national police forces on topics linked to major event security (e.g. media management, the setting up of Public-Private Partnerships linked to specific events, and a database of available technologies).

**Enhanced capabilities** - a common approach was adopted to the development of security plans for major events, best practices in security management were developed, mechanisms for cross-border and international cooperation on security planning for major events have been strengthened.

**Soft outcomes** - greater coordination of activities between actors responsible for internal security, the exchange of information and networking, and improvements in the quality and availability of good practices.

**Follow-up / sustainability:** The project aims to encourage sustainable follow-up through a European House of Security at Major Events. This could serve as a good practice repository and provider of technical expertise on security events.

The **FESTOS project**, a foresight study that is seeking to identify the emerging threats posed by emerging technologies has involved users both directly and indirectly in its activities to date. End-user organisations have been closely involved in project activities, such as Delphi Survey of experts and through the participation of 5 experts in an external advisory panel.

**Table 5.8: FESTOS – example of the involvement of users in foresight projects**

<table>
<thead>
<tr>
<th>Project(s):</th>
<th>FESTOS - Foresight of Evolving Security Threats Posed by Emerging Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Coordinator:</td>
<td>Interdisciplinary Centre for Technology Analysis and Forecasting (ICTAF) Tel-Aviv University Israel</td>
</tr>
<tr>
<td><strong>Project overview:</strong></td>
<td>FESTOS is a foresight project that seeks to identify the emerging threats resulting from new technologies with a time horizon of 2030. The aim is to identify and assess the type, nature and extent of evolving and future threats to security posed by the abuse or inadequate use of emerging technologies.</td>
</tr>
<tr>
<td><strong>Project detail:</strong></td>
<td>Users are involved in the project in two main ways i) 5 experts with a user background are taking part in the advisory group and ii) a much wider group of users have taken part in a Delphi Survey carried out in 2010 with experts in nanotechnologies, converging technologies and biotechnology. The expert views from the Delphi survey will then be incorporated into a Report on the Security Climate which will be distributed to relevant security policy officials and any other interested stakeholders. Target users include technical experts in relevant security fields, counter-terrorism officers, decision makers, security research centres. The project coordinated its activities through an external advisory group of potential users in order to map threats more effectively.</td>
</tr>
</tbody>
</table>
End-users in EU Security Research

Users also play a role in scrutinising the project from an ethical point of view. There is a need to ensure that information about future emerging security threats from new technologies is reviewed prior to its dissemination and distribution. A concern is that hypothetical scenarios, vulnerabilities or concerns about the malevolent use of technologies or infrastructure weaknesses could give ideas to terrorists or organised crime. As a project that dealt with foresight and horizon scanning of ‘low probability, high impact’ events, there was considerable cross-over between the activities of FESTOS and the work of national intelligence organisations. Users working in counter-terrorism in Germany and Israel have contributed to the analysis of future scenarios and the mapping of threats. A list of 80 “potentially threatening technologies” has been produced following an initial ‘scanning exercise’.

The involvement of users across a number of other projects was also examined. An example of a user organisation that was involved in a PASR project in the field of aviation security is provided below. This illustrates the important role of users both in defining their requirements and also in taking part in the testing and validation phases of project implementation, which provided valuable feedback to other organisations in the consortium.

Table 5.9: PATIN Project (PASR): EUROCONTROL – a user perspective on aviation security

<table>
<thead>
<tr>
<th>The European Organisation for the Safety of Air Navigation (EUROCONTROL) aims to harmonise and integrate air navigation services in Europe aims to create a uniform air traffic management (ATM) system for civil and military users, in order to achieve the safe, secure, orderly, expeditious and economic flow of traffic throughout Europe, while minimising adverse environmental impacts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUROCONTROL was involved in the PATIN (Protection of Air Transportation and Infrastructure) project as a user. The project was led by Diehl in Germany and had 21 organisations taking part, including 3 users: Munich Airport and the Czech Airport authorities.</td>
</tr>
<tr>
<td>Project activities included a mapping exercise to identify security measures to protect air transport systems. A threat assessment and risk analysis was also undertaken to examine various terrorist threats. A methodology was developed to assess whether future security requirements in the air transportation and ATM domains could be met through enhancements in operations, procedures, systems and technologies.</td>
</tr>
<tr>
<td>Three end-users were involved in defining user requirements and other activities, including a ‘live’ test cross-border flight to trial particular scenarios. This required cooperation across different national airspaces and authorities for security research purposes. At the end of the project, a conference for stakeholders was organised to test the practicability of a plan to improve aircraft self-protection and to install technologies to do so.</td>
</tr>
<tr>
<td>EUROCONTROL viewed participation in the project as having been useful. Prototype technologies were also developed to help protect aircraft from missiles, and valuable lessons were learned. The project was also successful in bringing together a range of relevant stakeholder organisations from both the demand and supply side that had not previously cooperated together. Gaining access to the technological know-how of different industrial partners, who had different functional expertise, was seen as helpful. The opportunity to exchange information on net-centric threats both to aircraft and systems of systems was also valuable, given the increased risk of intelligent and unconventional threats, including ATM cyber security breaches.</td>
</tr>
<tr>
<td>However, since the project was completed, ‘not much has happened’. Among the obstacles include the high implementation costs of some of the proposed aviation and aircraft security measures, along with a lack of political will and reluctance on the part of airlines, airports and ANSPs to make the necessary investments. In the absence of a regulatory framework to drive take-up, despite the threat of international terrorism, the technologies have not yet been deployed and ground-based systems could be more useful. Eurocontrol stated that there was a need for a clearer strategy on how the results would be used, and project follow-up in particular areas – e.g. net-centric threats, higher interconnectivity of airborne and ground systems, etc.</td>
</tr>
</tbody>
</table>
Users have played an important role in some maritime security projects, for example, in testing prototypes and in providing feedback on how these could be improved. A good example in this regard was the involvement of the Vukovar Port Authority in the UNCOSS project.

**Table 5.10: The Vukovar Port Authority— a user perspective on maritime security**

| Responsible for managing the Croatian section of the Danube river, port authority Vukovar, played a key role in trialling a prototype underwater coastal sea surveyor as a partner in the UNCOSS project. The underwater device will be used to scan coastal and river ports, although its main purpose is to lay the foundations for a specialised centre to run the device in cooperation with other agencies. The partners were convinced that river security personnel had received valuable knowledge and skills during the testing phase which placed them in a credible position with national authorities who invited the partners to participate in inter-agency training and exercises. The UNCOSS project addressed a clear need for greater increased security planning and technologies to prevent attacks on the physical infrastructure of river waterways. UNCOSS is the first project to raise awareness among public end-users in Croatia about emerging unconventional threats to the national waterways. However more support is needed to establish a permanent knowledge centre within the port authority to develop a genuine river safety system and a sustainable cooperation framework with law enforcement agencies. More broadly, maritime security end-users require new technologies such as GPS systems, vessel plating, scanning devices that can be easily integrated with the existing systems of port authorities and private shipping companies. |

The UK Police National CBRN Centre is not directly involved in the programme but has an active interest in the results achieved through the Security Research programmes. It has also participated in some of the thematic workshops organised by the Commission. The example below provides an interesting prospective end-user perspective, and makes suggestions as to how users might be more closely involved in ESRP projects and in the programme overall in the CBRN domain.

**Table 5.11: UK Police National CBRN Centre: Meeting the needs of users in the CBRN field**

| The UK Police National CBRN Centre leads the UK’s multi-agency preparations for responding to Chemical, Biological, Nuclear and Radiological attacks. It is responsible for improving the UK’s preparedness to respond to CBRN attacks and provides operational support to emergency services and crisis management agencies. This includes equipping operational advisors with secure communications and decision support systems. There is no single type of user in the CBRN field due to the different requirements for preventing, preparing and responding to CBRN threats. The main types of end-users, however, include the police, military, health protection agencies and centres for the Protection of Critical Public Infrastructure. There is high demand for trained individuals who are experienced in operating existing and new CBRN technologies (detection, communication ICT, scene assessment techniques and Personal Protection Equipment). Presently CBRN commanders respond to an average of three CBRN related incidents per year, therefore improved and more realistic training programmes would drastically improve scientific assessment and data management during live events. In addition, cost reductions in the manufacturing of low degradation personal protective clothing would allow first responders more flexibility to carry out response and remediation activities. Users should have closer involvement in projects during the planning and implementation stages, since users are often brought in to advise at a relatively late stage in project development. It is often the case that users are not asked to articulate the added value of project outcomes. An easily accessible forum could be set up with a focus on CBRN including a list of projects and users, to articulate problems more clearly. The selection of users could be improved to ensure relevance in terms of their ability to contribute valid operational skills and help develop operational CBRN capability. There is a need to leverage the unique expertise of military end-users while focusing on the civil security response to CBRN threats. This type of cooperation could be fostered by establishing a permanent platform for cooperation. |
5.2.4 Conclusions – end-user involvement

In conclusion, among the findings in relation to end-user involvement and the nature of the role that they have played in projects were that:

- **In successive Calls for Proposals, greater attention appears to have been given by project beneficiaries to the close involvement of end-user organisations.** As funding has become more competitive over successive Calls for Proposals, the imperative of including end-user organisations more closely has become better recognised by project applicants.

- **Approximately 3 in 4 projects involved users directly** - for example, through their participation in advisory panels, defining user requirements and specific activities and events to obtain user feedback (e.g. user workshops, scenario modeling and simulation, demonstration activities).

- **The extent of user involvement in FP7 SEC projects varies.** There is scope for the more systematic involvement of users in projects, especially during the early stages.

- **Users have also been involved in projects indirectly, for example, through participation in external advisory boards.** The role of users outside the consortium was to provide feedback on user needs, to define user requirements, strengthen knowledge about user target groups and to advise on societal and ethical aspects.

- **Some projects encountered difficulties in securing the engagement of end-users.** Among the main challenges include the perception among users that taking part in FP7 may be bureaucratic, a lack of interest in the research unless it was near to market and limited human resources. Users face many pressing demands on their time, and it is not always easy to get them to commit fully.

- **End-users were reluctant to participate in projects that involve long R&D lead times.** It was hard to convince users of the benefits of taking part in projects with a 10-15 year time horizon until the results can be made operational for users, even when this involved state of the art technologies.

- **Some national authorities expressed a reluctance to engage with projects in domestically sensitive areas of security.** Intelligence agencies may be unwilling to participate because of information sharing concerns in some areas, e.g. deadly pathogens. Such concerns may be allayed over time, given the focus through FP7 SEC on secure networks.

- **A success factor in increasing the likelihood of the take up of research results was the involvement of end-users as early as possible during project implementation.** This was felt to be especially critical in defining user requirements, testing and validation, interface development.

- **Large security industry firms identified added value in being able to engage directly with users through ESRP projects.** Taking part in FP7 SEC provided them with the opportunity to strengthen their visibility among users, and to validate and test user requirements directly.

- **Good practice identified to strengthen user take-up of research results include the development of end-user engagement strategies (e.g. FESTOS) while others have developed mechanisms for the regular dissemination of research results, such as the creation of an End Users Club [ISCAPS].**
5.3 Take-up of research results by end-users

5.3.1 Take-up by end-users

A key aim of FP7 Security is to encourage the take-up of research results by users through the effective dissemination of results. Through the survey work, issues were explored about the extent to which users perceive the types of projects supported and research results that have materialised to date through their implementation as relevant. The extent to which users are likely to take up results was analysed.

With regard to the field research, a key priority during September and October 2010 was to carry out interviews with users, both those involved in projects, as well as prospective users from the wider community not having been involved in the programme. It was important that both types of users were interviewed given the need to ensure that bias in the research results is avoided.

Beneficiaries were first asked the extent to which users were likely to make use of research outcomes produced through the project in which they have been directly involved. Encouragingly, almost a quarter of beneficiaries thought that end-users were ‘highly likely’ to take up the research results, 45.7% were ‘quite likely’ to use the results and 9.7% stated that it was difficult to say at this stage in project implementation. Only 4.2% said that users were unlikely to use the results. Although the sample is small, this suggests that beneficiaries are keenly aware of the need to ensure that their deliverables and results are fit for purpose and meet the needs and expectations of users.

Table 5.12: To what extent are users likely to use research outcomes produced through your project?

<table>
<thead>
<tr>
<th>Options</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly likely</td>
<td>17</td>
<td>23.6</td>
</tr>
<tr>
<td>Somewhat likely</td>
<td>33</td>
<td>45.8</td>
</tr>
<tr>
<td>Not likely at all</td>
<td>3</td>
<td>4.2</td>
</tr>
<tr>
<td>Difficult to say at this stage</td>
<td>7</td>
<td>9.7</td>
</tr>
<tr>
<td>No response</td>
<td>12</td>
<td>16.7</td>
</tr>
<tr>
<td>Total</td>
<td>72</td>
<td>100.0</td>
</tr>
</tbody>
</table>

With regard to the types of users that beneficiaries felt were most likely to use the research results, in order of greatest likelihood to least likelihood the results were as follows: National authorities, Public agencies responsible for civil security, Regional or local authorities, Industry (other than SMEs), SMEs, Public research institutions and lastly, Universities or Higher Education Institutions. It is interesting that this confirms CSES’ finding that users should be interpreted as a wider set of stakeholders that public agencies alone. More than a third of respondents stated that industry would benefit from the research results.

Table 5.13: What types of users are likely to benefit from the results produced through your project?

<table>
<thead>
<tr>
<th>Options</th>
<th>No</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regional or local authorities</td>
<td>31</td>
<td>43.1</td>
</tr>
<tr>
<td>National authorities</td>
<td>51</td>
<td>70.8</td>
</tr>
<tr>
<td>Universities or Higher Education Institutions</td>
<td>10</td>
<td>13.9</td>
</tr>
<tr>
<td>Public research institutions</td>
<td>18</td>
<td>25.0</td>
</tr>
<tr>
<td>Small and Medium Sized Enterprises (SMEs)</td>
<td>20</td>
<td>27.8</td>
</tr>
<tr>
<td>Industry (other than SMEs)</td>
<td>26</td>
<td>36.1</td>
</tr>
</tbody>
</table>
End-users in EU Security Research

| Public agencies responsible for civil security | 48 | 66.7 |

*Multiple responses possible*

The types of end-user organizations that beneficiaries perceived were most likely to use their research results is now provided. The results in ranked order according to their frequency are: (1) Agencies responsible for public safety and civil security 2) Crisis management and emergency response, (3) Law enforcement agencies and equal 3rd (3) Agencies responsible for chemical, biological, radiological and nuclear safety/ detection (4) Maritime and aviation security agencies and (5) Intelligence services. This broadly reflects the type of projects being supported through FP7 SEC and also tallies with CSES’ review of project fiches to examine the composition of consortia in terms of end-user involvement.

**Table 5.14: If you ticked public agencies please specify what type:**

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law enforcement agency</td>
<td>22</td>
<td>45.8</td>
</tr>
<tr>
<td>Intelligence services</td>
<td>12</td>
<td>25.0</td>
</tr>
<tr>
<td>Crisis management and emergency response</td>
<td>32</td>
<td>66.7</td>
</tr>
<tr>
<td>Maritime and aviation security agencies</td>
<td>20</td>
<td>41.7</td>
</tr>
<tr>
<td>Agencies responsible for chemical, biological, radiological and nuclear safety/ detection</td>
<td>22</td>
<td>45.8</td>
</tr>
<tr>
<td>Agencies responsible for public safety and civil security</td>
<td>38</td>
<td>79.2</td>
</tr>
</tbody>
</table>

*Multiple responses possible*

As part of the assessment of the relevance of EU Security Research, the usefulness of the research from the point of view of EU and national policy makers has been analysed. These are among the intended users of the research.

A number of projects were identified leading to the development of policy-relevant outcomes that can be used by EU and national policy makers responsible for different aspects of security policy. The programme is designed to contribute to achieving key EU objectives across a range of policy areas, including justice, liberty and security, enterprise and competitiveness, research, innovation and technological development transport, the environment.

Examples of projects that appear to have strong potential to contribute to strengthening policy knowledge and promoting debate among academia and policy makers include **EUSECON (A New Agenda for European Security Economics)** a four-year research project that analyses the causes, dynamics, and long-term causes of insecurity. Human-induced drivers of insecurity are being explored through the research. This could be useful to policy makers, for example, in providing them with better insights into the causes of and how to prevent terrorism and conflicts. It is also an area where research has previously been fragmented and part of the added value of FP7 SEC is in supporting a project that will serve as a beacon for academic research in a particular area and encourage the organisation of conferences and the production and dissemination of research papers on emerging areas.

Various examples were identified of ways in which users have either expressed strong interest in, or already made use of research results. In the area of maritime security, an example of a project which attracted strong interest from port authorities (and also from wider stakeholders interested in the standardisation aspects of the project) was the SECONDD project.
Table 5.15: Take up of project results: Maritime security

Some users stated that they had utilised some results from the SECONDD project which complimented the project SMART-CM (which creates interaction between custom authorities and market players involved in the container transport chain management and administration business). While SECONDD produced a novel data management system that can be used at a variety of seaports, end-users have also expressed a strong interest in technologies such as mobile neutron scanners for vessels and containers, chemicals detecting systems, thermal imaging scanners that can be interconnected with IT systems at sea ports. Projects in other areas of the ESRP are focusing on these types of technologies, particularly in the area of radiological cargo screening (e.g. COCAE).

Wider examples of projects that appear to have strong potential to be taken up by users include those with a focus on state of the art technologies. Examples include the SUBITO and SAMURAI projects, which have strong potential to improve security in mass transport systems and also in the area of aviation security, where the threat of terrorist attack demands improved technological solutions to identify suspicious behaviour and to improve the deficiencies in the current generation of CCTV cameras (i.e. fixed versus mobile and dynamic capabilities).

Table 5.16: State of the art technologies to support counter-terrorism – strong user interest

Counter-terrorism operations often involve fast paced tracking and tracing of individuals and baggage to carry out surveillance and intelligence collection activities and prevent attacks taking place in crowded areas. End-users such as the intelligence community, providers of critical infrastructure and law enforcement agencies are particularly interested in applying project results from the SUBITO and SAMURAI projects to address evolving terrorist threats (i.e. suicide bombers, and trafficking in CBRN).

SUBITO offers automated solutions for the identification and tracking of suspicious individuals in crowded areas. Civil contingency agencies expressed a strong desire to make use of existing CCTV camera networks, especially for transportation hubs and at sensitive locations. The attacks on buses and subway trains in London and commuter trains in Madrid have accelerated the deployment of intelligent algorithms across a number of CCTV networks, the results of SUBITO are well placed to play an important part in providing the technology and system management tools.

SAMURAI is leveraging legacy technology to monitor people and vehicles at critical infrastructure locations. The technology has reached a critical stage in its developed and tests have been carried out with end-users in the aviation industry. Airport operator BAA oversaw the trialling process and would like to see the system rolled out in the near term provided that IPR issues can be overcome.

Environmental security is becoming an important issue for the future development of the European Union. New threats and the potential consequences of these are becoming more difficult to predict so that authorities can be well-prepared. SECURENV is part of the EU FP7 Security Research that aims to develop technologies and knowledge needed to ensure the security of citizens from threats from non-state actors, natural disasters and industrial accidents. A database of industrial accidents and environmental natural disasters has been developed and the knowledge base in respect of security and its relationship with the natural environment has been strengthened. The project has also used foresight methods and scenario-building techniques to give end-users a better understanding of future risks.

Discussions were held with EU officials across different Commission services with responsibility for different aspects of security policy, such as drugs, counter-terrorism and crisis management. A number of different DGs are responsible for security policy questions at the EU level in areas such as aviation and maritime security, counter-terrorism, CBRN, drugs, combating organised crime, etc.
End-users in EU Security Research

5.3.2 Barriers to the take up of research results by end-users

Barriers to the take-up of research results by users were also explored through the research. It is important to understand obstacles so that steps can be taken to address these and encourage greater take-up. In the survey, more than two-thirds of beneficiaries (66.7%) identified obstacles to users capitalising on projects’ research results.

Table 5.17: What barriers can be identified?

<table>
<thead>
<tr>
<th>Options</th>
<th>№</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>The results of the research will be useful to end-users, but only after further development</td>
<td>35</td>
<td>72.9</td>
</tr>
<tr>
<td>End-users would consider using the results but only if these can be exploited free-of-charge</td>
<td>13</td>
<td>27.1</td>
</tr>
<tr>
<td>There may be difficulties in negotiating licensing agreements</td>
<td>6</td>
<td>12.5</td>
</tr>
<tr>
<td>There would be prohibitive costs in using the research results</td>
<td>7</td>
<td>14.6</td>
</tr>
<tr>
<td>There is insufficient commitment among target users to implement standards</td>
<td>8</td>
<td>16.7</td>
</tr>
<tr>
<td>There is insufficient commitment among target users to harmonise technologies, processes and procedures to promote interoperability</td>
<td>18</td>
<td>37.5</td>
</tr>
<tr>
<td>Outcomes are unlikely to correspond sufficiently to end-user needs</td>
<td>5</td>
<td>10.4</td>
</tr>
</tbody>
</table>

The results suggest that while some results can already be identified, it is too early to assess the take-up of new technologies, systems, approaches and knowledge by users in the case of many FP7 Security Research projects. This was confirmed through fieldwork discussions e.g. TeraSec, IMSK, SECONND.

Another barrier was that users may not have adequate resources to take-up results. 27.1% of respondents stated that ‘end-users would consider using the results but only if these can be exploited free-of-charge’. It was also felt that there was insufficient commitment among target end-users to implement standards (16.7%). About 1 in 10 respondents felt that the outcomes were unlikely to correspond sufficiently to user needs. Given the innovative and experimental nature of research funded through the FPs, this ratio is perhaps not surprising – there will inevitably be risk-taking involved in funding some of the more technologically ambitious projects, for example, and it is common across FP7 therefore that not all projects will achieve intended outcomes successfully.

Secondly, the earlier in the developmental process a particular technology, innovation or other aspect involving R&D, the more difficult it is to anticipate the extent to which end-users are likely to be interested in the technology. Even with PASR projects, lead times from initial R&D to test the feasibility of projects and to carry out initial research through the various stages of development prior to research, innovation, new technologies, products and services often materialises over a 10 – 15 year timeframe.

Table 5.18: National authorities - prospective users

Among the prospective end-users interviewed were national authorities responsible for implementing security research and for applying new technologies to support counter-terrorism policy. There was a perception among some authorities of large administrative burdens being associated with taking part in the ESRP. Additional human resources would be needed to administer the programme, which is currently unfeasible under the current workload and budgetary constraints of many Member States.

It was highlighted that national authorities are already involved in networking activities directly with the European Commission across different DGs responsible for security policies. While this cooperation has been
End-users in EU Security Research

broadly supported for its positive impact on the development of national security research programmes, there is a wide scope for increasing participation through joint projects. This will require reassurances that deeper cooperation will bring advantages and not lead to extra time commitment.

Another factor likely to influence take-up is the extent of dissemination of research results by individual projects and by the Commission in relation to the programme overall. Given that FP7 is a new programme and that many projects are still underway, most project-related dissemination has been through projects themselves during implementation (this applies both to PASR and to FP7). While communication activities about the programme, such as the organization of thematic workshops, have begun to disseminate the research outcomes more widely, the programme is still at an early stage and as projects mature, it should become much clearer the extent to which users are taking up results.

In promoting wider take-up of security research products and services by users, there is a need to strike an appropriate balance between a ‘technology push’ and a ‘technology pull’ strategy. Under a push approach, publicly funded research and the private sector develops technologies for users and then seeks to market and promote their take-up. A pull strategy places more of a focus on better understanding user needs so that these may be integrated from the design state so as to enhance and improve the effectiveness of FP7 Security Research results from a user perspective.

Based on the survey research and wider discussions, a hypothesis developed through the evaluation relating to the take-up of research outcomes by users is that various factors influence the degree of take-up. Examples of these are provided below:

- Internal factors: the degree of participation in projects by end-users, the extent to which the project consortium has made an active effort to disseminate and promote research results.

- External factors: the presence (or absence) of ‘enabling conditions’

Examples of enabling and inhibiting factors are provided in the following table:

<table>
<thead>
<tr>
<th>Table 5.19: Enabling and inhibiting factors – external drivers of take-up of EU Security Research outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence of a (conducive) regulatory framework at EU level – take-up for security research in some areas has been driven by Regulation. For example, in the area of aviation security, the adoption of common EU standards has played a positive in promoting demand for new generation detection equipment</td>
</tr>
<tr>
<td>Extent of EU versus Member State competence - pre-procurement and procurement by national governments or at EU level may stimulate demand for security products and services. This may be necessary in particular areas of security wherever there is evidence of market failure</td>
</tr>
<tr>
<td>Extent of industry and / or user acceptance of the need for standardisation and harmonisation – in some areas of security research, there is wide acceptance of the need for common minimum EU standards, and testing and certification regimes. This is seen as a driver of cost-effectiveness. However, in other areas, such as critical infrastructure protection, there appears to be a reluctance to embrace interoperability either for reasons linked to cost-effectiveness or improved operational efficiency</td>
</tr>
</tbody>
</table>

In some thematic areas within FP7 SEC, there are positive drivers of user take-up of security products, services and technological solutions. Examples include aviation security, where since 2002 the EU has been responsible for drawing up a common EU regulatory framework setting out minimum standards on aviation security. This should serve as a future driver not only of take-up for security detection equipment but also in promoting common certification and testing approaches and driving standardisation processes. Conversely, in other areas, such as critical infrastructure protection, there is a lack of cross-border inter-operability, and sometimes even within the same Member State. Moreover,
there is currently an absence of political will to drive processes of standardisation, harmonisation and inter-operability in this domain.

The absence of a supportive regulatory environment can sometimes create a ‘chicken and egg’ situation in terms of the RTD investment cycle, whereby researchers, industry and manufacturers are reluctant to invest in R&D without the confidence that regulation will drive take up by end-users of particular technologies or innovations which are often costly and require significant time to develop.

**Cost factors may also serve as a deterrent to taking up research results.** An example is the technology to combat manpad attacks, which may impose a significant cost on the industry, and requires a risk-based assessment of the trade-off between maximising security and the probable threat level.

Other inhibiting factors identified in the ESRIF report influencing take up include: the lack of EU regulatory competence in some areas of security, with the Member States retaining competence in particular security domains. This may lead to difficulties in terms of the EU playing a stronger coordination role in promoting standards, harmonisation and interoperability. For example, in the aviation security arena, a variety of detection devices compete with one another but there is an absence of common standards, testing and certification at EU level which leads to operational inefficiencies for airport operators. Lastly, in many Member States and at EU level, there is as yet little pre-procurement to simulate demand for security research, technologies, products and services.

5.4 EU Citizens and Security Research

EU citizens are the ultimate beneficiaries of FP7 Security Research and as such, are in a sense the ultimate end-users of security research. It is difficult at this relatively early stage in programme implementation to assess the overall contribution of FP7 SEC to improving the Security of EU Citizens, one of its four ‘core Missions’. There are lead times in particular technologies becoming operational and in being taken up by user organisations that protect the general public.

Nevertheless, there are already some examples of research outcomes that have strong potential to improve citizens’ security. For example, through the PASR project TRIPS (Transport Infrastructures Protection System), a small prototype robot has been developed that is capable of checking for explosives on the rail network. This has been trialled with strong interest from user organisations. Since there have been at least two terrorist plots to target high-speed rail links in France and Germany, and terrorist attacks having already taken place in Russia, this is evidently highly relevant to addressing the concerns of the travelling public.

Likewise, confidence among EU citizens in aviation security in general, and airport and in-flight security in particular is vital from an economic perspective. Some of the research being funded through FP7 SEC, such as the SAMURAI project to develop new generation CCTV cameras in airports able to track luggage and people has potential to improve the detection of suspicious behaviour and to eliminate the gaps in security resulting from present-generation CCTV systems. Such research is very directly beneficial to improving the security of EU citizens.

Likewise, in the maritime security field, through projects such as AMASS (Autonomous Maritime Surveillance System) for example, is developing new technology to improve the early detection of illegal immigration by sea in southern Europe, in particular the identification of small targets within the maritime environment. This will help to directly address the security concerns of EU citizens in relation to illegal immigration and improving the speed of detection which will enable humanitarian assistance to be provided to victims of people trafficking.
End-users in EU Security Research

Some projects directly concerned EU citizens, for example, in the area of crisis management, the BeSeCu project carried out research to explore the different cultural reactions to emergency situations and disasters in different countries. The research results are being incorporated both into the design of buildings and into the development of appropriate operating procedures for buildings. There is evidently a direct link with the citizen, and such knowledge has the potential to save lives.

EU citizens will also benefit from research to develop improved technologies in emergency response situations to detect bodies and survivors in disasters such as earthquakes. The SGL for USAR (Second Generation Locator for Urban Search and Rescue operations) project, described earlier, has developed a prototype of a portable first responder device that integrates sensors, images, sound and chemical analysis for the early location of entrapped people and dead bodies. This again has strong potential to improve the speed and accuracy of the response provided by first responders, which should save lives if deployed.

In the CBRN domain, while EU citizens will benefit from measures supported, through enhanced prevention, preparedness and response mechanisms, it was noted in the interviews that there is further scope for projects to be supported that focus on the recovery phase of CBRN, particularly strengthening societal and psychological resilience to CBRN attacks.

The role of EU citizens has been considered through ESRP as part of PASR and FP7 SEC projects that focus on the ethical and societal aspects of security research. Issues of direct concern to citizens, such as privacy considerations in areas such as biometrics, data storage and airport security have been examined. Dual use issues have also been considered in some projects, with ethical advisory groups set up to monitor ethical and dual use issues. There have been both dedicated projects addressing the ethical and societal aspects of security research and these issues have also been integrated as a horizontal priority in projects. Further details are provided in Section 3.5 (cross-cutting missions).

In conclusion, while the direct involvement of EU citizens in FP7 SEC projects has been limited, it is evident that citizens will benefit from all projects to a greater or lesser degree, assuming that user organisations take up research results.

While FP7 SEC has made a positive contribution to improving citizens’ security, however, there is no easy way of developing an appropriate metrics framework to assess this. Perceptions of security could of course be assessed through a Eurobarometer survey or a similar mechanism, but the question of attribution (i.e. the extent to which improvements in security can be directly attributed to the programme) means that this approach has its limitations.

FP7 SEC benefits EU citizens both directly and indirectly, but citizens themselves will be unaware of the extent to which particular technologies, methods and procedures, being deployed by user organisations were developed through the programme. The examples show however that some of the research being undertaken has strong potential to better protect EU citizens from security threats and in some instances, to save lives directly.
6. Conclusions and recommendations

6.1 Conclusions

6.1.1 Overall conclusions

Ex-post Evaluation of PASR

1. The Preparatory Action on Security Research (“PASR”) played a central role in laying the basis for the fully fledged ESRP in FP7. Full financial absorption was achieved and 39 projects were supported in the 2004 - 2006 period over 3 annual calls for proposals.

2. PASR strengthened the Commission’s institutional capacity to implement EU Security Research and served as a useful testing ground to establish what types of projects and research topics would be effective in contributing to the strategic aims of the future ESRP.

3. PASR attracted project applications from high-quality, well-known organisations from the public and private sectors. Since each call was considerably over-subscribed, the Commission was able to focus on research excellence during the project selection and evaluation process.

4. The intervention logic was robust and linked to the identified needs of security research actors (industry suppliers and end-users). The approach to defining priorities was coherent with the prevailing policy framework at the time.

5. There is evidence of continuity in research topics between PASR and FP7 SEC calls. PASR projects therefore provided a strong platform for follow-up projects financed through FP7 SEC.

6. Cross-cutting missions such as promoting interoperability and strengthening security in networked systems were already visible in PASR, although a stronger emphasis could perhaps have been placed on the ethical and societal aspects of security (which is better integrated in FP7 SEC).

7. National authorities had some influence on the formulation of research topics in annual PASR Calls, which suggests that the Commission tried to be responsive to meeting the needs of users.

8. Time to grant was viewed as more reasonable in PASR than in FP7 SEC, although some projects still encountered delays, which hindered effective project implementation in a small number of cases.

9. Progress was made through PASR support actions in structuring the security research industry and in preparing the ground for the new programme in FP7 by promoting capacity development among beneficiaries to participate in collaborative transnational research. This was appropriate given evidence of industry fragmentation.

10. PASR produced valuable research outputs and some initial useful research outcomes, although often further work is needed before research results can be made operational and actually deployed by end-user organisations.

11. Progress has been made in the development of pre-standards and pre-industrial prototypes and in the demonstration of proof of concept of technological solutions. The interoperability of networks and ICT systems has been strengthened.

12. Furthermore, progress has been made in the development of pre-standards (e.g. secure containers, maritime security) and of common approaches to testing and certification (in the CBRN domain).
Conclusions & Recommendations

13. Some research results have already been utilised, especially through follow-up FP7 SEC projects that built directly on PASR research in accordance with the ‘building block’ approach to developing mission-oriented capabilities.

14. PASR also achieved soft outcomes, such as strengthened coordination at EU level on particular thematic research topics and the promotion of networking between relevant security research actors, for example, the creation of networks.

15. Most stakeholders were positive about their participation in PASR and saw it as having been a valuable ‘training ground’ in taking part in the fully-fledged ESRP in FP7. Many PASR participants subsequently applied for funding in FP7 SEC, with some successes.

16. Large firms in the security industry were well represented in PASR. While recognising the valuable role that large firms play (routes to market, state of the art research, etc.) the Commission has successfully promoted the diversification of partners in consortia with some success, especially through the emphasis on strengthening SME participation.

17. User involvement from the earliest stages of projects, especially in defining user requirements was a key success factor. However, users were not always sufficiently involved in projects.

18. Some PASR projects encountered difficulties in engaging with users. This was attributed to the fact that R&D / technological projects were often at quite an early stage in development.

19. The extent of eventual take up of research results by users is difficult to assess at this point in time in respect of PASR projects that involved basic research. Some concerns were expressed about the sustainability of PASR project outcomes without further follow-up research funding.

20. Although some projects maintained project websites beyond the lifetime of the project, more could be done to better exploit PASR research results both at the project level and across projects.

21. Overall, PASR has been an effective funding instrument and raised awareness among security research actors about the future ESRP in FP7.

6.1.2 FP7 Security Research

1. FP7 SEC demonstrates strong coherence with key EU policies, including strengthening industrial competitiveness, promoting research excellence, and reinforcing the European Research Area.

2. The intervention logic is appropriate, with clear links between the programming framework in calls for proposals, and identified needs. However, objectives could have been defined at different levels in order to establish a clearer distinction between global, general and specific objectives.

3. The logic would benefit from an indicator framework so that the outcomes and achievements (quantitative, qualitative) expected to materialise through the programme are clearer.

---

41 Examples include an industrial taxonomy, work on technology watch, and developments in the interoperability of secure data devices for secure containers.

42 A key aim of ESRP is to strengthen industrial competitiveness in civil security. It is beneficial that major EU firms are participating in FP7 SEC. Large firms commonly work together with SMEs in delivering R&D/ technology-oriented work packages (WPs), strengthening supply chain relationships. They are in a position to leverage their research capabilities and know-how and to make use of legacy technologies civil security research purposes.
Conclusions & Recommendations

4. The thematic focus of EU Security Research has been progressively strengthened over successive calls. This has been influenced by the emergence of a more coherent EU policy framework since FP7 SEC was adopted, with developments in various areas in which security research projects are being supported (e.g. CBRN, crisis management, aviation security).

5. FP7 SEC was allocated 1.4bn EUR over a 7 year funding period 2007-2013. The programme appears to be on track to achieve a high level of funding absorption. The financial weighting is geared towards the second half of the programming period.

6. The combined human resource level for implementing FP7 SEC between DG ENTR’s Security Unit and the REA’s Security Unit is modest. The programme has been implemented efficiently, with administrative costs for implementing FP7 SEC well below the 6% maximum threshold set in FP7.

7. The transition of responsibility from the Commission’s DG ENTR to the REA in 2009 was well managed. The Executive Agency has rapidly developed the capacity to implement the programme and to monitor projects efficiently and effectively.

8. The comparatively long lead times in Time to Grant in FP7 SEC – 530 days - is a source of ongoing concern. However, there are factors specific to the ESRP, notably the Security Scrutiny Procedure and some aspects of ethical review (e.g. dual use), that presently make it difficult to reduce TtG without changes in the rules and procedures for FP7 overall.

9. Since many Member States do not presently have their own national civil security research programme, there is a clear Community Added Value to FP7 SEC.

10. Higher participation by SMEs in FP7 SEC (>18.7% compared to 16% for overall FP7) by SMEs and a high SME share of funding are significant achievements. SMEs face high market entry barriers in some areas of the security industry. FP7 SEC represents an important route to market for SMEs, in the face of fragmented market conditions.

11. FP7 SEC has become a key source of funding for security research for SMEs in many EU countries. FP7 SEC is demonstrably addressing a funding gap since SMEs, unlike large firms, are usually not in a position to fund applied research using own-financing.

12. The emphasis in FP7 SEC on a multi-disciplinary approach has meant that a wide range of organisations have been involved in the programme ranging from SMEs, through to large firms, academic and research institutions, NGOs, and consulting organisations.

13. A small number of instances were identified of organisations that had initially benefited from a research grant under a national programme and had then been successful in applying for further research funding to take the research to the next stage through the ESRP. National programmes therefore have potential to develop the capacity of security actors to benefit from FP7 SEC.

14. Competition for funding is becoming increasingly intense. A downside of over-subscription is that increasing numbers of proposals are being received in each call, which risks exacerbating TtG times.

15. While optimal consortium size is difficult to determine (and depends on type of project / theme), there is a trade-off between ensuring effectiveness in carrying out research and showing good EU coverage within the consortium.

16. Among the main advantages of participating in FP7 Security include from a beneficiary perspective are: access to EU research funding, strengthened cooperation with transnational partners, improved
Conclusions & Recommendations

knowledge and capabilities, and the development of strategic relationships with users and a better understanding of their needs.

17. It is important to involve users at all stages in project implementation, from design and structuring, through to testing user requirements and the dissemination of research results. Applicants are growingly aware of the importance of incorporating users (and SMEs) into proposals.

18. The use of demonstrator projects as the flagship of the programme has strong potential to promote awareness about the research being conducted through FP7 Security, and to encourage take-up among users by showcasing ‘state of the art’. However, it is too early to evaluate their success.

19. The ethical and societal dimension of EU Security Research has been strengthened in FP7, and the ethical screening procedure has played an important role in this regard. Given the importance of ethical and privacy issues and the need to scrutinise dual use potential, this was necessary.

20. There has been a concerted effort by the Commission during 2010 to engage in dissemination activities. This should help to promote the wider use of research results by end-users over the medium term, and also strengthen the EU’s coordination role in bringing together relevant stakeholders in specific areas e.g. standardisation, interoperability.

21. However, further steps could be taken to strengthen the dissemination of PASR project achievements.

22. While project monitoring in respect of technical content appears to be rigorous, it would be useful to develop an indicator system as part of the overall monitoring framework to enable the Commission to report on key programme achievements.

6.2 Key evaluation issues

The evaluation was carried out using the key evaluation issues framework developed by the European Commission’s DG Budget. The relevance, efficiency, effectiveness, Community Added Value and the sustainability of interventions funded through the ESRP were analysed.

6.2.1 Relevance

Among the issues examined in relation to relevance were the extent to which the ESRP has addressed the identified needs of end-user organisations and European citizens in improving the EU’s internal security. The evaluation also considered the extent to which the intervention logic was pertinent at the time the programme was adopted, given the prevailing policy framework.

The different thematic areas of intervention supported through FP7 Security were found to be relevant to the needs of end-users, although it is premature at interim evaluation stage to fully assess the extent to which research outcomes are likely to meet real needs. A lesson in improving the pertinence of project activities, research outputs and research results was the importance of involving users from the outset to maximise relevance. The ESRP was also found to be relevant in addressing the security concerns of EU citizens (see Section 5.5), such as combating terrorism, protecting critical infrastructure from attack and natural disasters and improving border surveillance to combat illegal immigration.

The assessment of the intervention logic underpinning ESRP found that the logic was robust. There is a strong recognition among EU and national stakeholders of the need for closer coordination and cooperation between relevant security actors, such as law enforcement agencies, agencies responsible for the protection of critical infrastructure and intelligence agencies.
Conclusions & Recommendations

There was also found to be a strong rationale for supporting the industrial competitiveness of the European security sector given that the market remains fragmented. Without the support of FP7 and other investment drivers such as regulation and public procurement, there would be a risk of that the market would fail to operate in some areas. Without EU support, Europe may lag behind its international competitors in particular areas of security.

Looking ahead, the relevance of the intervention logic will need to be reviewed in planning for FP8 in light of the ongoing policy, regulatory and wider developments since the programme was adopted. For example, the Lisbon Treaty has strengthened Community competence in respect of EU external actions and this raises the possibility of introducing an external dimension to ESRP research activities, which in FP7 SEC must focus on internal EU security matters.

6.2.2 Efficiency

A ‘classical’ assessment of programme efficiency would assess the ratio between financial inputs, outputs and research results in order to measure the cost-effectiveness of EU Security Research.

However, there are methodological challenges in assessing programme efficiency at interim evaluation stage. Many FP7 SEC projects supported are in their first, second year or third year of implementation with activities ongoing. Therefore, while some research outcomes can already be identified, other projects involve fundamental research with a long R&D timeframe. The usefulness of research results, and the extent to which these can be made operational by end-users may only be apparent in some instances over a 10-15 year timescale.

Nevertheless, the research suggests that collectively, the achievements through projects supported in both PASR and FP7 SEC represent good value for money, with evidence of solid progress in a number of areas (Section 4.5 details the research results and initial impacts achieved through the programme and provides a review of research quality. Section 2.5 provides data on financial inputs).

Some stakeholders interviewed expressed the view that greater cost-effectiveness could be achieved if in areas of common interest there were closer cooperation between EU funded civil security and defence research projects. However, it should be recalled that FP7 SEC is a civil security research programme. Notwithstanding, through the existing Cooperation Framework Mechanism that the Commission has signed with ESA and the EDA, the scope for closer coordination (and any funding synergies in research already being undertaken) could be explored in areas of common interest such as maritime surveillance, crisis management and CBRN. Such cooperation must necessarily respect the civil security focus of the programme.

Another aspect of efficiency was to assess how well the programme has been managed by the European Commission and REA and whether it has been implemented in an efficient manner (Section 2.4 provided a review of human resources deployed and the costs of administering the ESRP). The evaluation found that the level of human and financial resources used to administer the programme was modest, when set against the large scale of funding - 1.4bn EUR. Moreover, the Commission (and since June 2009, the REA) were found to have managed the Calls for Proposals process, and contracting procedures effectively. There were however considerable concerns among beneficiaries and wider stakeholders with regard to the length of Time to Grant.
Conclusions & Recommendations

6.2.3 Effectiveness

Issues analysed in relation to the third key evaluation criterion include the extent to which progress has been made towards the achievement of key ESRP objectives, and the quality of research results to date both at the project and programme level.

Good progress has been made towards the achievement of key ESRP objectives. PASR and FP7 Security have both had a positive effect on structuring EU Security Research. They have for example supported the preparation of R&D and strategic roadmaps setting out pathways to the development of Europe’s strategic civil security research capabilities. FP7 SEC has played a useful role in strengthening the EU’s security capabilities and in the identification of capability gaps in particular thematic areas.

FP7 SEC has helped to promote the development of a more strategic approach to research efforts to underpin Europe’s internal security. This is of critical importance since the majority of Member States (17/25) do not presently fund national (civil) security research programmes.

PASR and FP7 SEC has strengthened cooperation between relevant actors and promoted the formation of sustainable partnership working arrangements between different actors ready to work together on transnational collaborative research projects. This has helped to address the fragmentation of research efforts and to strengthen critical mass among the security research ‘community’ (industry, academia and publicly funded research).

The ESRP has helped to strengthen the competitiveness of the European security industry. Large firms that have participated in FP7 SEC have been effective in capitalising on know-how, and in adapting ‘dual use’ technologies from defence for civil security research purposes. An interesting aspect of progress in this area is the ESRP’s comparative success in attracting SMEs to take part. SMEs have played an effective role in delivering research on technical Work Packages in some consortia, although there could be greater scope in future for SMEs to play the lead coordinator role. Scope for taking part in collaborative research has enabled the security industry to tap into the knowledge and expertise of world-class universities and research institutions. In this way, the ESRP has been effective in promoting technology transfer between industry and academia (and vice versa).

FP7 SEC has had a positive effect in bringing suppliers of security solutions, products and services closer to end-user organisations. In some projects, there has been strong initial interest among end-user organisations in research outputs and the preliminary research outcomes to date. This was especially the case in respect of projects that are in the process of developing technologies and industrial prototypes that are relatively ‘near to market’. However, projects that will require longer R&D lead times have sometimes encountered difficulties in engaging with end-users.

With regard to the quality of research undertaken (see Section 4.5), given the heterogeneity of projects being supported, there are challenges in assessing research quality achieved through ESRP. The development of an indicator system to improve performance monitoring would be an important step in improving mechanisms to assess research quality. A current shortcoming is the lack of appropriate benchmarking information against which research outcomes can be assessed, for example, to assess the comparative effectiveness of technologies under development through ESRP research activities, compared with technologies already available on the market.

Nevertheless, it can be concluded that ESRP has fostered research excellence and promoted ‘state of the art’ in particular areas, such as the development of Terahertz waves for use in CBRN detection and the development to use scintillated crystals to improve the quality and effectiveness of portable detection equipment used at land border checkpoints. The fact that some projects have not only...
Conclusions & Recommendations

developed their own patents but used the patents and IP of consortium members (for example, the use of a proprietary technology platform belonging to one partner with software and add-on applications subsequently developed by other partner organisations) suggests a relatively high degree of sophistication in some research projects.

A further important issue relating to effectiveness was the extent to which project results have been **effectively disseminated**. Among the findings were that there is further scope to improve the promotion and dissemination of research results achieved, especially through PASR. There has however more positively been good progress in strengthening communication and dissemination activities during FP7 SEC, especially during 2010, given that there was a need to delay dissemination activities until there was a reasonable critical mass of initial research outputs to promote. The organisation of a series of thematic workshops during 2010 has been a positive step in promoting cooperation and further structuring in particular areas of security, such as aviation security, CBRN, critical infrastructure protection etc.

While difficult to measure, FP7 SEC has made a positive contribution to **improving the security of EU citizens**, although there is no easy means of developing an appropriate metrics framework to assess this. In the case of most projects, end-users are only just starting to use research results and to adapt these for their operational needs, therefore at this stage in the programme’s development, the impact on citizens is mainly indirect. There are however already promising technologies under development that, if deployed, have strong potential to make a direct contribution to protecting citizens from terrorist attacks and other malevolent acts. Compared with PASR, FP7 SEC was found to have been more effective in tackling ethical and societal aspects of security research, such as privacy and data protection concerns, and in addressing ‘dual use’ issues, which are of direct concern to **EU citizens**.

Overall, the programme has been effective in making progress towards key aims at the mid-point in its implementation. However, the ESRP remains in its infancy, and a medium-long-term approach is needed in developing capabilities in particular areas. The building block approach advocated through the ESRAB and ESRIF stakeholder consultation exercises implies making incremental progress towards programme aims. This is especially the case in respect of areas such as maritime security, where a 10-15 year time horizon is envisaged before key aims are likely to be achieved.

### 6.2.4 Community added value

Considerations in relation to Community Added Value (CAV) include additionality (i.e. the extent to which the ESRP has brought additional national resources that would not otherwise have been available), spillover effects (the benefits of action at EU level in promoting actions at national level that would not otherwise have materialised) and the impact of adopting a European approach in the civil security research domain, and of setting corresponding objectives at Community level.

With regard to **financial additionality**, the analysis of national security research programmes (see Section 3.7) found that only 8 /27 EU Member States currently support a civil security research programme. Moreover, in the context of the global economic crisis, it is especially difficult for new Member States to fund a domestic programme. The setting up of a full ESRP under FP7 has therefore brought about additional funding opportunities, which is especially important in structuring the civil security industry, and is vital in securing stronger SME engagement in the sector, given market entry barriers (see Section 3.6 on the involvement of SMEs in ESRP).

The nature and extent of **spillover effects** was also examined. Among the findings from the research were that the setting up of a Security Research Programme at EU level has been instrumental in encouraging the creation of national security research programmes in a number of EU countries (e.g.
Conclusions & Recommendations

Austria, Finland, Germany, Romania). In other countries, such as Lithuania, while presently no national programmes operate, the very fact that FP7 SEC was set up has prompted a debate among stakeholders about how best to promote greater participation by innovative Lithuanian SMEs in the programme. The reflected a finding in several new member states that there were concerns about the need to raise the capacity of SMEs, universities and research institutions to take part in ESRP.

The ESRP was found to have had a galvanising effect in promoting greater attention to civil security research at national level. At the firm level, the research suggests that this is a two-way process i.e. some firms initially participated in a national programme and then applied to take part in FP7 SEC. In other instances, following the successful implementation of an ESRP project, follow-up funding for additional research activities was secured through national sources.

Most areas of security research demand a European-wide approach and necessitate strong cross-border cooperation if progress is to be made. The programme adds value by encouraging structuring to take place in areas that may previously have lacked impetus for common EU-wide action, or in which coordination was already taking place, but through less formal structures. ESRP has also had a positive impact on encouraging progress in certain thematic areas that are inherently cross-border in nature and require a pan-EU response, such as improving land and maritime border security, and under the cross-cutting themes, strengthening interoperability and networking, promoting the development of standards and common approaches to testing and certification.

A further issue was the extent to which any effects could be identified from setting shared Community objectives in the security research domain. Given that many fields in which research is being undertaken are highly specialised, the transnational dimension of the research is a critical factor in promoting research excellence. ESRP was found to demonstrate high CAV since the transnational, collaborative nature of the research being carried out helps to strengthen critical mass and to alleviate the fragmentation of research efforts, thereby contributing towards strengthening the competitiveness of the EU’s civil security research community (not only industry, but also the potential of universities and research institutions to engage in world class research).

There were however concerns that consortia that included partners from too wide a number of EU countries in carrying out R&D activities may be less effective from a research quality and manageability perspective than smaller, focused consortia. There was also a concern that consortia should not be required to include partner organisations from new member states simply to demonstrate that their geographic coverage was sufficiently inclusive. Research excellence was felt to be the only criterion on which consortium partners should be selected.

A number of further positive impacts were discerned in assessing the ESRP’s CAV, such as improved cooperation and networking between relevant actors and the transfer and exchange of experiences between suppliers and end-users (e.g. Petranet, EUSEC II). Additionally, a number of projects promoted the exchange of good practices, such as the development of common methodologies in security planning for major events (EUSEC II) and the transfer of experiences between countries in training methodologies for first responders (e.g. NMFR Disaster).

6.2.5 Sustainability

Key issues examined in relation to sustainability include: financial sustainability; whether recommendations made by projects for follow-up activities to ensure that research results are sustainable were realistic; the extent to which research results are being disseminated effectively and
whether cooperation mechanisms and partnership structures formed through the programme are likely to be durable.

With regard to financial sustainability, beneficiaries were asked in the survey whether they could have gone ahead with the project in the absence of EU funding. The majority of respondents and interviewees stated either that they could not have gone ahead with the project at all (‘full additionality’) or in the case of some private sector projects led by large industry, would only have gone ahead on a more limited basis (‘partial additionality’).

As far as alternative funding sources are concerned, the research found that the level of financing available through national programmes was typically lower than in ESRP, with the added restriction that most funding is for domestic projects, rather than transnational research. With regard to the possibility of using own financing, while some large firms were found to have multi-million Euro R&D budgets to carry out research in-house, they were reluctant to commit large-scale resources for transnational collaborative research without EU funding support, given the fact that working in the FP environment means being open to the sharing of ideas and IP with other consortium partners and to transparency in terms of publishing the research results (with attendant risks that once in the public domain, commercially sensitive ideas could be used by competitors).

Another aspect of sustainability was the availability of follow-up funding for beneficiaries to continue research activities and/or to ensure that results achieved had a sustainable impact. The main potential financing source for follow-up activities was ESRP, and examples were identified of consortia that had been successful in applying for further funding in subsequent calls. However, FP7 SEC Calls for Proposals are becoming increasingly competitive. Some beneficiaries stated that if they were unsuccessful in applying for funding through ESRP, they hoped to apply for national funding to ensure follow-up.

Another aspect of sustainability was the extent to which provision has been made to ensure that research results have a lasting benefit through project follow-up. Projects are required under the terms of Grant Agreements to make recommendations for follow-up to ensure that their project activities and research results are sustainable and the research assessed how practical these were. Many projects were found to have made sensible suggestions\(^43\) with regard to how research activities should be built upon through future research topics. Continuity was found in the topics being supported in accordance with the ‘building block’ approach through which incremental progress is made in developing security research capabilities. There is also evidence that in many instances, research results have a sustainable impact because future projects make use of the results of previous projects. Examples of PASR projects in which the research outcomes have been used by successor projects are provided in Section 4.5 (e.g. Staccato, Staborsec).

However, not all projects achieved sustainable results. For example, the European Technology Watch database set up through the STRAW project (FP7 SEC) has not been as successful as had been hoped and the GEOCREW project (PASR), despite a promising beginning in terms of political commitment to implement an early-warning system for disasters within the EU has not been followed up. While every

\(^{43}\) An example of a project that made recommendations on how its activities could be followed up was the EU-SECII project (Security Planning for Major Events). A Work Package focused on putting in place a mechanism for ensuring sustainable follow-up to ensure that cooperation between end-user organisations continues beyond the project lifetime. The project recommended the setting up of a House of Security Planning for Major Events.
effort needs to be made to ensure that research outcomes are used, all RTD programmes have an element of risk, given the innovative nature of research being undertaken, and not all will be successful.

Another aspect of sustainability is the visibility of research results, which impacts the extent to which they are likely to be taken up by end-users. There has been a definite improvement between PASR and FP7 SEC in terms of the quality of project websites. The lack of a central web portal as a repository for PASR research results is an obvious current deficiency, although DG ENTR’s Security website does publicise project results, for example, through the compilation of a brochure containing 45 project fiche overviews. However, the summaries are only about the activities undertaken and general project aims, no information on the results achieved is presently provided.

While a publishable project summary about project achievements is already required from beneficiaries in FP7 SEC, this could be improved by placing a greater focus on explaining the research results achieved and on the potential relevance of their application to prospective end-user organisations. Currently, fiches seen by the evaluators often contain general information.
Conclusions & Recommendations

6.3 Recommendations

Key learning points in relation to PASR have already largely been addressed in FP7 SEC. The recommendations mainly focus on the current programming period and on preparation for FP8 Security. It should be noted that some recommendations apply to FP7 Security, whereas others would require changes at the level of FP7 Cooperation overall (indicated in brackets).

6.3.1 PASR and FP7 Security Research

Programme management (negotiation and contracting phase, financial reporting)

1. Close the annual call for proposals earlier than December in order to avoid lengthening Time to Grant due to the summer period following call closure, which can delay the finalisation of the contract negotiation process (FP7 overall).
2. Further adapt IT systems to support staff in carrying out the negotiation and contracting phase in order to help reduce Time to Grant (FP7 overall).
3. Explore whether there are any additional ways to reduce bottlenecks (while at the same time respecting the EU Financial Regulation and the specific features of security research, notably the security scrutiny procedure).
4. Ensure that the administrative and financial validation process of project partners begins as early as possible following the initial finalisation of selected projects and the commencement of the negotiation process.
5. Expenditure data on programme administration costs should in future be made available in relation to FP7 Security on a disaggregated basis within the European Commission’s DG ENTR Directorate H to check the position in respect of the 6% maximum target more easily.

SME participation

6. Further encouragement should be provided to SMEs willing to lead project consortia. There is already a financial incentive in terms of increased co-financing, but explicit mention could be made in annual calls that ‘applications led by SMEs will be especially welcomed’.
7. Give consideration to the concept of an ‘apprentice’ status within projects for SMEs. The learning function can be important within FP7 projects (FP7 overall).

User involvement

8. Give consideration to simplifying application procedures for end-users (FP7 overall).
9. Require all project consortia to involve public end-users in project consortia and encourage projects to systematically involve end-users during project implementation from the outset.

Examples of changes made since PASR include stronger attention to promoting the participation of SMEs and end-users in projects, the need for a greater balance in the types of beneficiaries taking part in project consortia (to address the concern that PASR was too large-firm dominated), and the strengthening of the ethical and societal dimension of Security Research through the introduction of the ethical screening procedure.
Conclusions & Recommendations

Assessing research excellence / quality

10. An indicator system should be introduced in FP7 SEC in order to improve the basis for assessing research quality. This needs to go beyond conventional measurement of research excellence (e.g. citations and bibliographic excellence).

11. The expected outcomes from research projects should be benchmarked in so far as possible against existing security products, services and solutions already available on the market. Appropriate benchmarks should be developed against which research quality can be assessed.

12. Elements of peer review between projects could be encouraged in particular thematic areas of Security Research to provide an additional mechanism for assessing research quality. An alternative (or additional) option would be to subject clusters of projects to detailed cross-comparative review by external experts.

Definition of Missions

13. The Security of EU citizens is currently defined as a core Mission in FP7 SEC. However, the EU citizens dimension should also be taken into account as a cross-cutting priority in all projects.

Evaluation and monitoring

14. A performance monitoring system should be introduced, supported by quantitative and qualitative indicators. This should take into account the need to report both on project achievements (especially research outcomes) and for data to be collected in respect of a more limited set of indicators for management reporting purposes.

Cooperation between the Commission and national authorities

15. Strengthen cooperation between national authorities and the Commission so as to ensure more effective coordination in the implementation of ESRP and national security research programmes. This would reduce the danger of double funding similar projects.

Dissemination of research results and project monitoring

Since the REA now has responsibility for most project monitoring, DG ENTR should turn its attention to disseminating research results and to utilising these to feed into policy development processes in different EU Security Research fields. In particular, the Commission should:

16. Improve the dissemination of PASR research results through the development of a single web portal, and a project compendium outlining the achievements of PASR projects.

17. Consider the scope for standardising information presented in the publishable ‘fiche’ that projects are required to produce at the end of their term explaining what has been achieved and setting out more clearly the opportunities for end-users to make use of research results.

18. Ensure together with the REA that the publishable summaries of project achievements are disseminated more effectively.

19. The Commission should closely monitor the effectiveness, utility and results achieved through Phase 2 demonstrator projects, since these have strong potential to become ‘flagship’ projects which showcase the potential usefulness of research results to users and the wider public.

6.3.2 FP8 Security

Various relevant legal and policy developments at EU-level have taken place since the FP7 Programme Decision was adopted in 2006. The adoption of the Lisbon Treaty in particular has implications for
Conclusions & Recommendations

structuring FP8 since it opens up new possibilities, such as strengthening the external dimension of EU security research, the inclusion of humanitarian assistance and energy security as research topics, etc. A review of key policy and legal developments is provided in Appendix J (‘future perspectives’).

Programme planning (intervention logic, indicator system and thematic scope)

1. In preparing for FP8, a clearer distinction should be made in the definition of aims and objectives between global, general and specific (operational) objectives.

Consideration should be given to broadening the scope of ESRP activities to incorporate some of the new possibilities resulting from the adoption of the Lisbon Treaty in December 2009.

2. The external EU dimension of the Security Research Programme should be strengthened.

3. Project results should be integrated more effectively with the work of EU agencies operating in the context of EU external actions, especially in areas such as crisis management, humanitarian assistance, monitoring the impact of climate change and border surveillance.

4. Cooperation should be further promoted through the ESRP between the EU and international organisations, notably the UN.

The ESRIF report from December 2009 provides a strategic innovation agenda for EU Security Research and sets out a number of themes for reflection in the formulation of FP8. Steps should be taken to implement more of the recommendations in the ESRIF final report. In particular:

5. The role of pre-procurement and procurement in stimulating demand for security products and services should be strengthened in FP8. This will require close joint cooperation between the Commission and the Member States.

6. Demand-side initiatives should be supported that encourage end-users of security research to refine user definition requirements in a way that takes full account of currently available technologies and the need for interoperability.

7. A target should be set of increasing SME participation in FP8 Security to 25%.

While a diverse range of organisations are already represented in projects, many proposals received include the largest industry players, and there remains scope to further increase the participation of ‘knowledge-intensive SMEs in transnational cooperation’.

Communication activities and dissemination of research results

8. Consider giving the REA greater responsibility for communication activities in future, since over time, given their role in project monitoring, the REA should be in a position to accumulate knowledge about good practices and to identify examples of research excellence.

Cooperation with other EU bodies and international organisations

9. The ESRP should remain exclusively focused on civil security research. Notwithstanding, closer cooperation should be pursued with the ESA and the EDA through the existing Cooperation Framework Mechanism in areas where there is scope for research synergies e.g. CBRN, crisis management and humanitarian assistance, maritime and border surveillance.

10. Further efforts should be made to strengthen existing partnerships with national authorities in third countries (e.g. US’ Department of Homeland Security) to ensure that synergies from funding and cooperation (e.g. on standardisation, interoperability) are maximised.