European Commission

South African Interest

FP7-SEC-2013-1 call

FP7 Security Research Theme

From Calls to Projects

Call1 (2007-2008)	*156 million €*	*48 projects*
Joint Call SEC-INFSO	*20 million €*	*9 projects*
Call 2 (2009)	*117 million €*	*32 projects*
Call 3 (2010)	*209 million €*	*40 projects*
Call 4 (2011)	*221 million €*	*54 projects*
Call 5 (2012)	*241 million €*	*~ 56 projects*
Call 6 (2013)	*± 300 million €*	

Projects' description available on:

http://cordis.europa.eu/fp7/security/projects_en.html

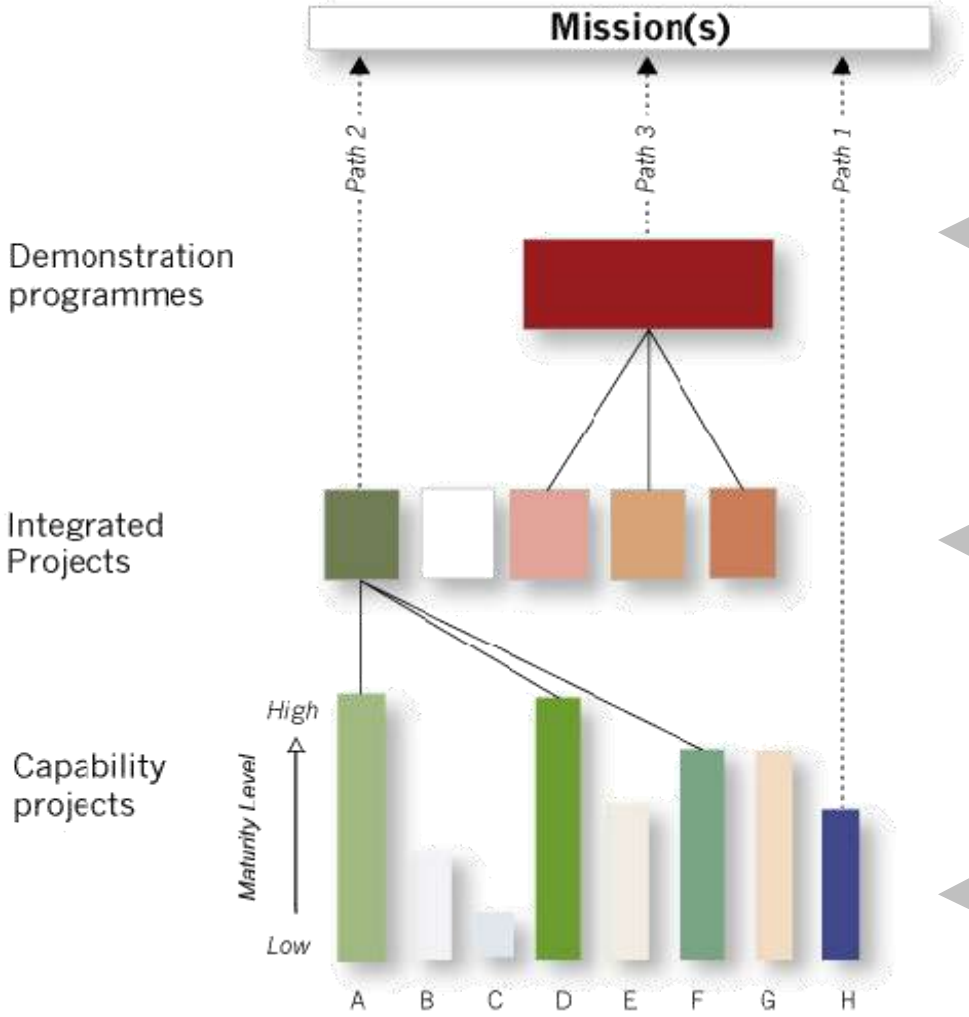
ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/securityresearch_catalogue2010_2_en.pdf

http://cordis.europa.eu/fp7/security/fp7-project-leaflets_en.html

Theme 10
Security Objectives

- To develop the **technologies and knowledge** for building capabilities needed to ensure the **security of citizens** from threats such as acts of **terrorist acts** and (organised) **crime**, **natural disasters** and **industrial accidents** 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 the cooperation of **providers and users** for civil security solutions;
- To improve the **competitiveness of the European security industry** and
- To deliver mission-oriented results to **reduce security gaps**.

Research routes to meet the Security theme objectives



Systems of systems demonstration
- *Combination of IP results*
- *Multi-mission*

System development and validation
- *Combination of capabilities*
- *Mission specific*

Capability development
- *Technology development*
- *Multi mission and mission specific*

Tentative Timeframe…

- **Call publication**: 10 July 2012
- **REA Info-day (Brussels): 11 September 2012**
- **Deadline for submissions**: 22 Nov 2012 at 17:00 Brussels time
- **Proposals evaluation**:
  - Remote: mid Dec 2012 / end Jan 2013
  - In house: end Jan 2013 / mid Feb 2013
  - Panel meeting: mid Feb 2013
  - Ethics screening: Mar 2013 / mid Apr 2013
  - Security Scrutiny: end Feb 2013 / mid May 2013
- Indicative **start of negotiations** of short listed proposals: mid-2013
- Indicative **projects starting** date: end 2013 / beginning 2014

Funding schemes (1)

Collaborative projects:

- **Small and medium-scale focused research projects** (CP-FP):
  - Capability Projects
  - indicative EU funding ~3.5M€ (No eligibility criteria)

- **Large-scale integrating projects** (CP–IP):
  - Demo Projects II & Integration projects
  - indicative EU funding >3.5M€ (No eligibility criteria)

➡ *CPs to be as small and simple as possible and as large as necessary*

Who can participate?

- Any **undertaking**, **university**, **research centre** or other existing **legal entity** established in:
  - ✓EU **Member States** (27 MS)
  - ✓**Associated Countries** to FP7 (14 AC) = Iceland, Liechtenstein, Norway, Croatia, Serbia, Turkey, FYROM, Switzerland, Israel, Albania, Montenegro, Bosnia & Herzegovina, Faroe Islands and Moldova
- If the conditions for participation are met (Minimum number):
  - ✓ **at least 3 independent participants from 3 MS/AC** (JRC as if established in another MS/AC);
  - ✓ except for Support Action: 1 legal entity.
- International organisations and participants from third countries can participate only in addition to the minima
  - ✓ **International Cooperation Partner Countries** (ICPCs): eligible for funding.
  - ✓ **High-income countries**: exceptionally might be funded (conditions)

Some related Institutions in South Africa

Department of Science and Technology

- ✓ ESASTAP (Euro SA Science & Tech Advancement Pgm)

Science Councils (experts, test facilities, access to applications/users):

- Council for Scientific and Industrial Research

- ✓ Defence, Peace, Safety & Security
  - ✓Radar, electronics, sensors, cyber defence, command & control, air/land/sea ops
- ✓ Meraka Institute (ICT) – Human Language, Ontologies, identity
- ✓ Modelling and Digital Science – biometrics, smart cards

- Medical Research Council – mortality, health and safety

Universities of Pretoria, Rhodes, UNISA, Johannesburg, Cape Town, KwaZulu Natal, …

- ✓ Computer Security, Crime Prevent, Risk Management, Criminology

Industry: Defence, Security, Guarding, SMEs, dual-use, financial

End-Users: Police, disaster management centres, border control (customs, immigration), security companies

WP Specific issues (2)

Multidisciplinary and mission-oriented

Active involvement of end users is considered of utmost importance:

- Direct participation of user organisations implementing research actions
- Other forms of indirect participation might also be followed

Networks of security research stakeholders are **key in disseminating results** to end users, national public authorities and citizens

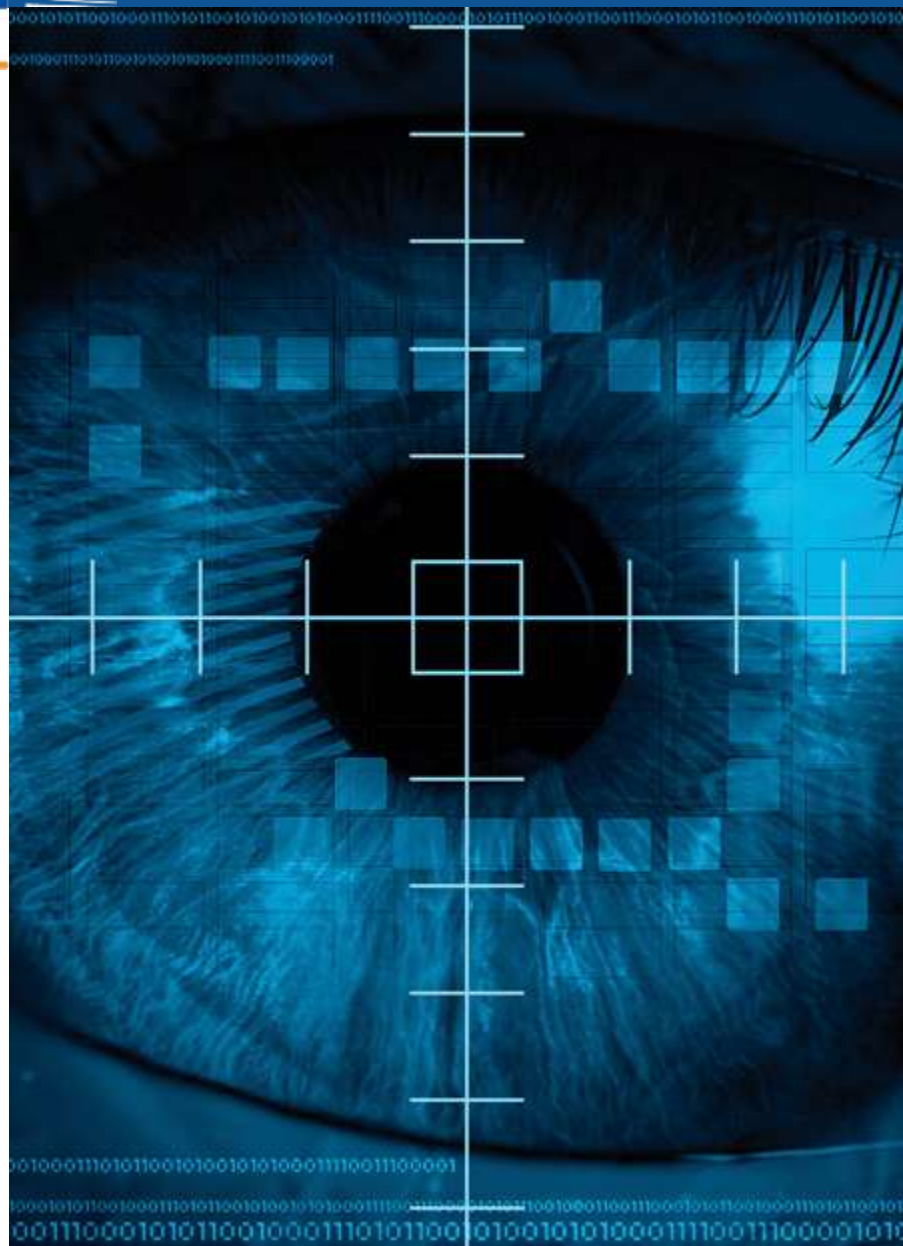
WP Specific issues (3)

The broad **involvement of SMEs** in consortia is highly encouraged

- explicitly mentioned in the description of the topics
- SMEs open topics
  - 7.2-1: Solutions for frequent petty crimes
  - 7.6-1: Serious gaming to improve intelligence analysis

Sensitive activities and information

- not in the proposal
- provisions must be foreseen for use of classified background or production of classified foreground if relevant



WP Specific issues (4)

Societal impact of the proposed technologies must be addressed

NEW: Societal checklist!!

Ensuring security research:

- ✓**meets the needs of society**
- ✓**benefits society**
- ✓**does not have negative impacts on society**

Dual use technologies (both civilian and defence applications) might be covered (EDA coord)

Standards are crucial for interoperability

Concrete achievements are strongly encouraged (expected impact)

Ethical issues are essential in the core of the project development

Ethics in Security research

European Commission

Privacy and data protection

- Health information
- Criminal justice
- Financial information
- Genetic information
- Location information
- Cultural information

Dual use

- Direct military use
- Research having a potential for terrorist abuse

Human data collection, tests

- Are humans part of test or demonstration?
- Are personal data stored and processed to avoid reconciliation of data with identity?
- Is there any tracking of people?
- Is informed consent mentioned?

CP-CSA
Pre Operational Validation (POV)

- POV differs from and complement the other projects, by involving directly and supporting financially **end-user agencies** (national/European authorities)
- To support the **demand side of research**, rather than the supply side, in their direct quest for new security solutions.
- Funding purposes:

  (i) the coordination of relevant institutions or authorities, acting as certifiers of new technologies (**100% support**) implemented via CSA; and

  (ii) the actual implementation of the corresponding **calls for tenders** (**50% support**), for testing/validation of novel security solutions (implemented according to the own criteria and specifications of the participating institutions or authorities) implemented via CP.
- **Funding scheme**: a **combination of CSA** (for coordination of validation policies) **and CP** (for implementation of testing and validation)
- 2 topics:

  ✓ **Topic SEC-2013.3.2-1** Pre-Operational Validation (POV) on land borders

  ✓ **Topic SEC-2013.5.3-2** Testing the interoperability of maritime surveillance systems

Demonstration Phase II projects

Large Demonstrators

- ✓ **Maritime Border Security**
- ✓ **Security of Mass Transportation**
- ✓ **CBRNE**
- ✓ **Supply Chain & Logistics**
  - **Topic SEC-2013.2.4-1 Phase II demonstration programme on logistics and supply chain security**
- ✓ **Crisis management**
  - **Topic SEC-2013.4.1-1 Phase II demonstration programme on aftermath crisis management**

FP7-SEC-2013: Topics

Activity	N
1- Security of the Citizens	10
2- Security of infrastructures and utilities	13
3- Intelligent surveillance & border security	6
4- Restoring security and safety in crisis	9
5- Security systems integration, interconnectivity and interoperability	5
6- Security and society	7
7- Security research coordination and structuring	4

Orientation paper with topics published in the **participant portal** under

FP7_Documentation

Activity: 10.1 Increasing the Security of the Citizens

- SEC-2013.1.1-1 Serious organised economic crime
- SEC-2013.1.1-2 “Stronger Identity for EU citizens”
- SEC-2013.1.3-1 Inhibiting the use of explosives precursors
- SEC-2013.1.4-1 Smart and protective clothing for law enforcement and first responders
- SEC-2013.1.4-2 Development of a Common European Framework for the application of new technologies in the collection and use of evidence
- SEC-2013.1.5-1 European toolbox, focusing on procedures, practices and guidelines for CBRN forensic aspects
- SEC-2013.1.6-1 Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes
- SEC-2013.1.6-2 Novel technologies and management solutions for protection of crowds
- SEC-2013-1.6-3 Surveillance of wide zones: from detection to alert
- SEC-2013-1.6-4 Information Exploitation

Activity: 10.2 Security of infrastructures and utilities

- SEC-2013.2.1-1 Evidence based and integral security concepts for government asset protection
- SEC-2013.2.1-2 Impact of extreme weather on critical infrastructure
- SEC-2013.2.2-1 A research agenda for security issues on land transport
- SEC-2013.2.2-2 Toolbox for pandemics or highly dangerous pathogens in transport hubs – Capability Project
- SEC-2013.2.2-3 Protection of smart energy grids against cyber attacks
- SEC-2013.2.2-4 Cost effectiveness of security measures applied to renewable/distributed energy production and distribution
- SEC-2013.2.2-5 Security of ground based infrastructure and assets operating space systems
- SEC-2013.2.4-1 Phase II demonstration programme on logistics and supply chain security
- SEC-2013.2.4-2 Non-military protection measures for merchant shipping against piracy
- SEC-2013.2.5-1 Developing a Cyber crime and cyber terrorism research agenda
- SEC-2013.2.5-2 Understanding the economic impacts of Cyber crime in non-ICT sectors across jurisdictions
- SEC-2013.2.5-3 Pan European detection and management of incidents/attacks on critical infrastructures in sectors other than the ICT sector (i.e. energy, transport, finance, etc)
- SEC-2013.2.5-4 Protection systems for utility networks

Activity: 10.3 Intelligent surveillance and border security

- SEC-2013.3.2-1 Pre-Operational Validation (POV) on land borders
- SEC-2013.3.2-2 Sensor technology for under foliage detection
- SEC-2013.3.2-3 Mobile equipment at the land border crossing points
- SEC-2013.3.4-1 Border checkpoints - hidden human detection
- SEC-2013.3.4-2 Extended border security - passport breeder document security
- SEC-2013.3.4-3 Security checks versus risk at borders

Activity: 10.4 Restoring security and safety in case of crisis

- SEC-2013.4.1-1 Phase II demonstration programme on aftermath crisis management
- SEC-2013.4.1-2 Better understanding of the cascading effect in crisis situations in order to improve future response and preparedness and contribute to lower damages and other unfortunate consequences
- SEC-2013.4.1-3 Development of simulation models and tools for optimising the pre-deployment and deployment of resources and the supply chain in external emergency situations
- SEC-2013.4.1-4 Development of decision support tools for improving preparedness and response of Health Services involved in emergency situations
- SEC-2013.4.1-5 Preparing societies to cope with large scale and/or cross border crisis and disasters
- SEC-2013.4.1-6 Preparedness for and management of large scale forest fires
- SEC-2013.4.2-1 Fast rescue of disaster surviving victims: Simulation of and situation awareness during structural collapses including detection of survivors and survival spaces
- SEC-2013.4.3-1 Shaping immediate relief action in line with the goals of development co-operation in post crisis / post conflict societies to maintain stability
- SEC-2013.4.4-1 Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination

Activity: 10.5 Security systems integration, interconnectivity and interoperability

- SEC-2013.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities
- SEC-2013.5.1-2 Audio and voice analysis, speaker identification for security applications
- SEC-2013.5.3-1 Definition of interoperability specifications for information and meta-data exchange amongst sensors and control systems
- SEC-2013.5.3-2 Testing the interoperability of maritime surveillance systems
- SEC-2013.5.4-1 Evaluation and certification schemes for security products

Activity: 10.6 Security and society

- SEC-2013.6.1-1 The impact of social media in emergencies
- SEC-2013.6.1-2 Varying forms of terrorism
- SEC-2013.6.1-3 Trafficking in Human Beings: analysis of criminal networks for more effective counter-trafficking
- SEC-2013.6.2-1 Facilitators for assistance among EU Member States in emergencies at home and abroad
- SEC-2013.6.3-1 Horizon scanning and foresight for security research and innovation
- SEC-2013.6.3-2 The evolving concept of security
- SEC-2013.6.5-1 Synthesis of results and reviewing of ethics, legal and justice activities in Security research in FP7

Activity: 10.7 Security Research coordination and structuring

- SEC-2013.7.2-1 Open topic for Small and Medium Enterprises: "Solutions for frequent petty crimes that are of high impact to local communities and citizens"
- SEC-2013.7.3-1 Increasing the engagement of civil society in security research
- SEC-2013.7.4-1 Trans-national cooperation among public security research stakeholders
- SEC-2013.7.6-1 Open topic for Small and Medium Enterprises: "Use of serious gaming in order to improve intelligence analysis by law enforcement agents"

Two open topics for SME's (2)

Topic SEC-2013.7.2-1 Open topic for Small and Medium Enterprises: "**Solutions for frequent petty crimes that are of high impact to local communities and citizens**" – (CP-FP)

- Aim improve security in **local communities** and for **citizens**.
- Address insecurities towards local communities (Citizens & Business).
- **Identify** and then look into **solutions** for frequent but low-intensity sources of insecurity having high impact on C&C.
- **Innovative research** and **development work**, leading to **low cost technology based solutions**, meeting the needs and financial expectations of C&C. The **cost to benefit ratio** of the proposed solution should be analysed against the impact of the threats.
- Indicative **research areas** could be for instance:

1. to develop new technologies/methods to protect local business and/or citizens from theft and/or extortion and/or fraud;
2. to develop new technologies/methods for the general protection of citizens from physical violence;
3. to develop a technology method for the general protection of private and public properties against vandalism (e.g. train/subway stations, facades/walls, cars, etc.); and
4. any other field relevant for frequent in-security situations that are of high impact to local community businesses and citizens.

Recommendations (1)

- Follow the FP7 guides (definition of the funding schemes, scope of topics, eligibility rules, etc)
- Be aware of the 3 "evaluation criteria" and sub-criteria by funding scheme:
  - ✓**Scientific and technical quality**
  - ✓**Implementation**
  - ✓**Impact**
- Foresee the take up of the results of your research
  - **Describe the perspective of a wider and general use of expected results**

Recommendations (2)

- Address ethical, societal and sensitiveness issues within the proposal
- Justify the real innovative aspects (Incremental versus breakthrough)
- The size of projects and of consortia should be the result of the intended project objectives and not the other way round!
- Clearly explain/justify the project budget
- Within the partnership look for the right expertise needed for reaching the proposal objectives: end users, private and public, academia, industry, SMEs, etc:
  - ✓ **Avoid "sleeping" partners without real contribution,**
  - ✓ **Avoid redundant partnerships,**
  - ✓ **But … the involvement of SMEs and relevant End Users is encouraged!**

Recommendations (3)

- Present an overall vision of market deployment
- Check/link the project with relevant ongoing or finished EU/international research projects
- Clearly present the state of the art!
- Proof-read your proposal by a 'neutral' person
- Make the reading of an evaluator easy:
  - ✓**Use a simple and clear language**
  - ✓**Be short and concise**
  - ✓**Clearly define objectives, milestones and deliverables**
  - ✓**Use tables and graphs, etc**
- Respect the page limits: Applicants must ensure that proposals conform to the page limits and layout given in the GfA

… ***And do not leave the proposal submission to the last minute!***

Further information

Security Research Info-Day on 11 September 2012 in Brussels

Participants portal:

http://ec.europa.eu/research/participants/portal/

- Work Programme
- Call for proposals
- Guide for applicants etc.

REA: http://ec.europa.eu/research/rea/
REA-security-research@ec.europa.eu

DG ENTR: http://ec.europa.eu/enterprise/security/index_en.htm
entr-security-research@ec.europa.eu

Helpdesk Centralised FP7 Enquiries Service:
http://ec.europa.eu/research/enquiries

National Contact Points:
http://cordis.europa.eu/fp7/ncp_en.html
http://www.seren-project.eu

Security projects on CORDIS:
http://cordis.europa.eu/fp7/security/projects_en.html

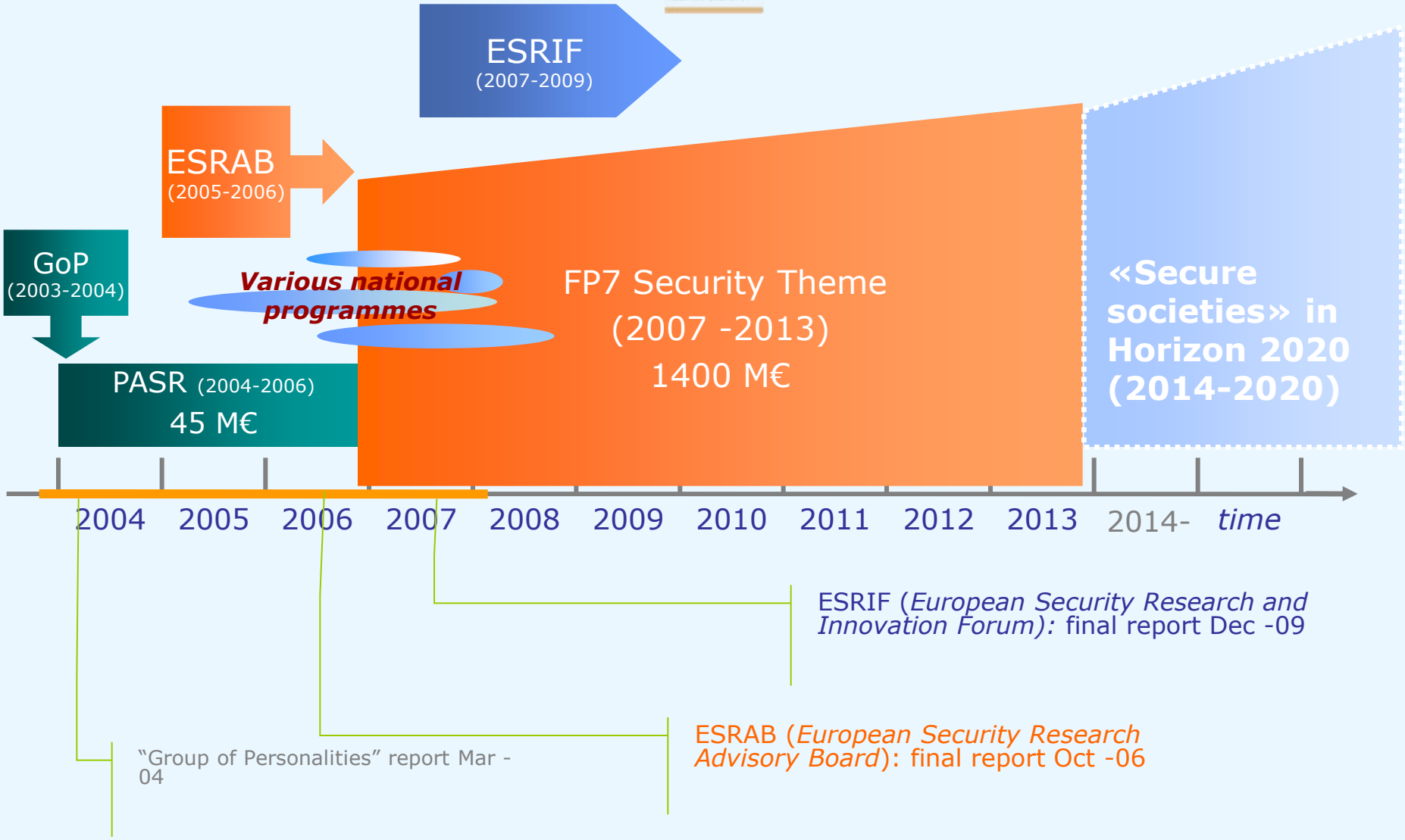
Success rate – Call 2012

Activity/area	*Total n° proposals*	*Total cost (€)*	*Average per proposal (€)*	*Requested EU contribution (€)*	*Average per proposal (€)*
Evaluated	***326***	***1.698.462.823***	***5.210.009***	***1.215.600.982***	***3.728.837***
Ranked List	***56***	***339.088.796***	***6.055.157***	***243.899.140***	***4.355.342***
%	*17,18%*	*19,96%*		*20,06%*	

- The total EU requested budget on the main and the reserve lists for the international cooperation partners falls under the limit of 3% (0.4%)

- The total EU requested budget for proposals within the POV topic 3.1-1 on the main list is 9.2 M€ and falls under the limit of 4% (3.8%)

EU security research: from PASR to Horizon 2020



What is new?

A single programme bringing together three separate programmes/initiatives*)

More innovation, from research to retail, all forms of innovation

Focus on societal challenges facing EU society, e.g. health, clean energy, transport, security

Simplified access, for all companies, universities, institutes in all EU countries and beyond.

**) 7th research Framework Programme (FP7), innovation aspects of Competitiveness and Innovation Framework Programme (CIP), EU contribution to European Institute of Innovation and Technology (EIT)*

Security Research in Horizon 2020

Reinforcing support to EUs internal and external security policies, notably the Internal Security Strategy

Improving the competitiveness of EU industries to address security gaps and prevent threats to security, incl. cyber-threats

Maintaining mission-oriented approach, integrating end-user needs

Further enhancing the societal dimension & coordination

"Secure Societies" - five specific objectives:

1. Fighting crime and terrorism

2. Strengthening security through border management

3. Providing cyber security

4. Increasing Europe’s resilience to crises and disasters

5. Ensuring privacy in the internet and enhancing the societal dimension

Thank you

Dr Barend Taute & Simon Nare (Assistant NCP)
FP7 Security NCP for South Africa
www.esastap.org.za
Security.ncp@esastap.org.za
+27 12 841 4063
http://www.seren-project.eu/ (NCP network)