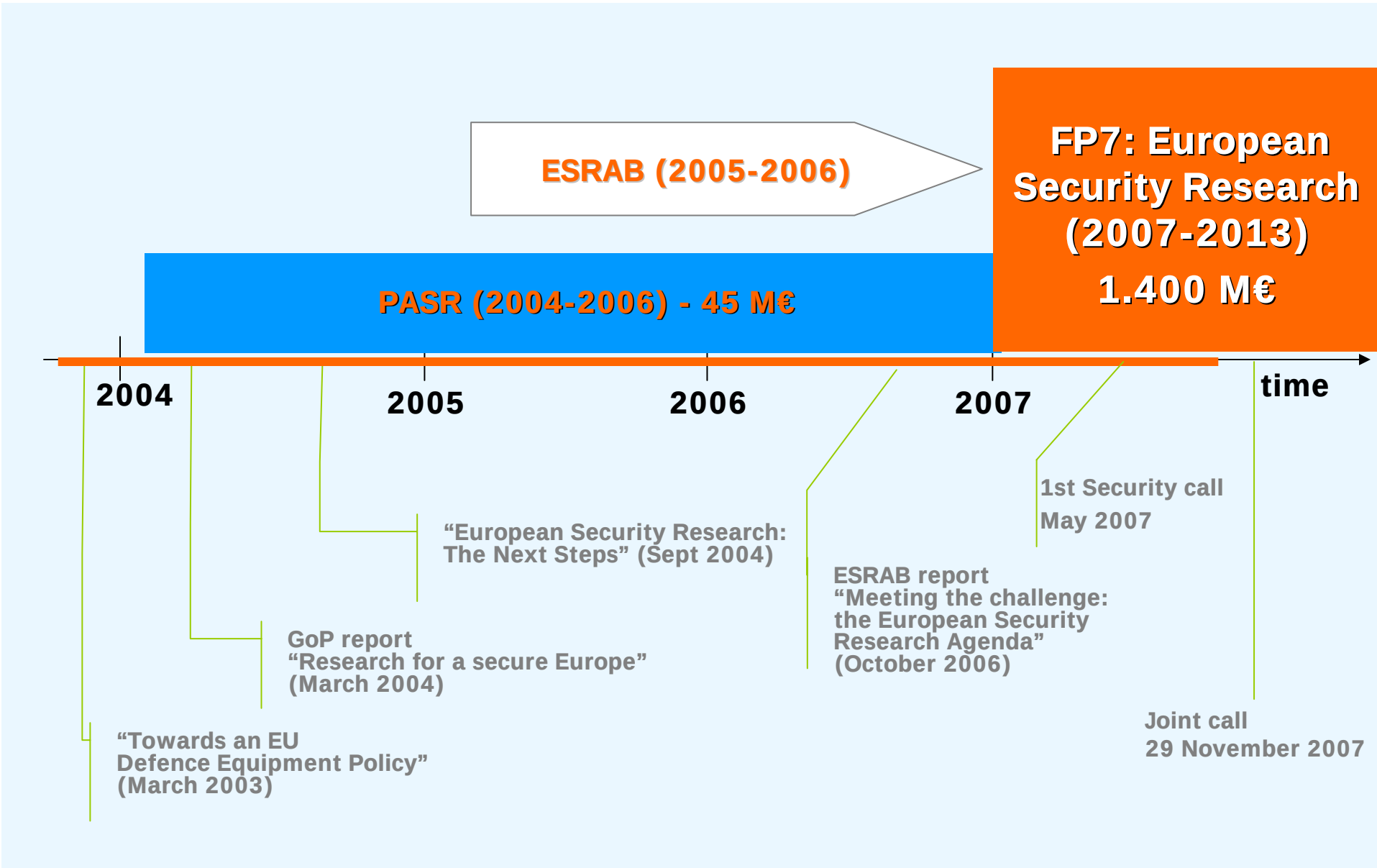
FP7
Joint Call between ICT and Security: Critical Infrastructure Protection

Pieter De Smet

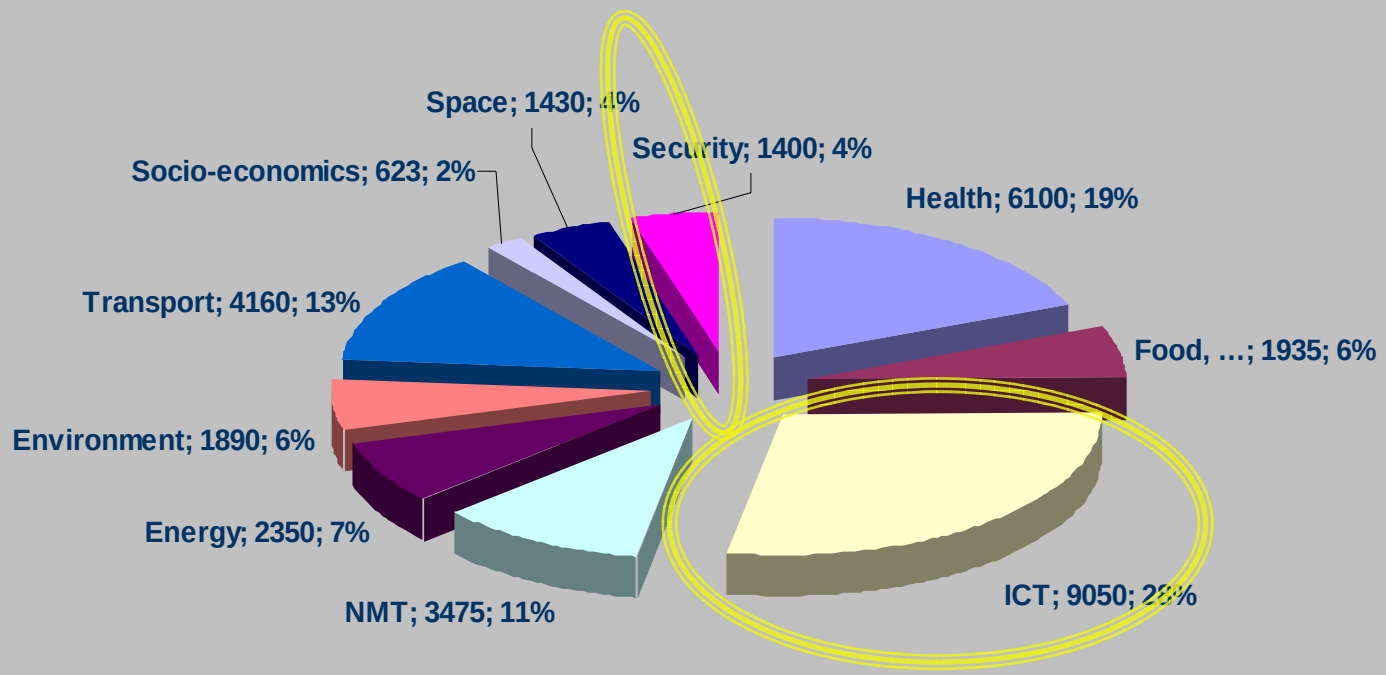
Project Officer, Unit "Security Research and Development "
DG ENTR, European Commission
Pieter.De-Smet@ec.europa.eu

From PASR to the FP7 Theme "Security": A set of coherent initiatives



FP7: 2007-2013

Total 50,521 M€

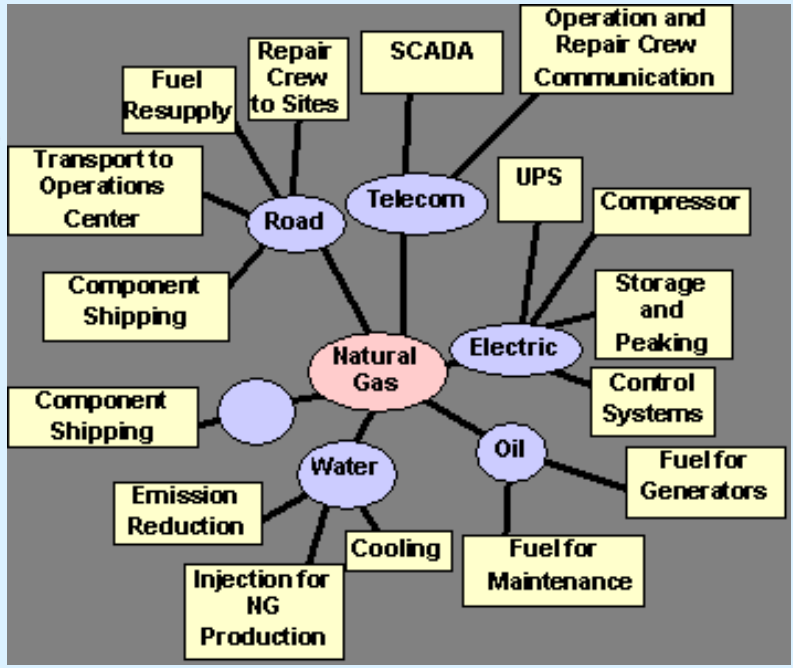


Strengthening Competitiveness through Co-operation

Protection of Critical Infrastructures

Challenges

- Liberalization, Deregulation
- Global, Cross border CI's
  - ➔ Different policy & regulatory frameworks
  - ➔ Different protection measures and technologies
- Openness & Interconnection
  - ➔ Interdependencies
  - ➔ Large scale, multi layer systems
  - ➔ Complexity, Chaotic Behavior
  - ➔ New Vulnerabilities, Cyber-threats
- Law enforcement, Crisis Management



Protection of Critical Infrastructures
The Context

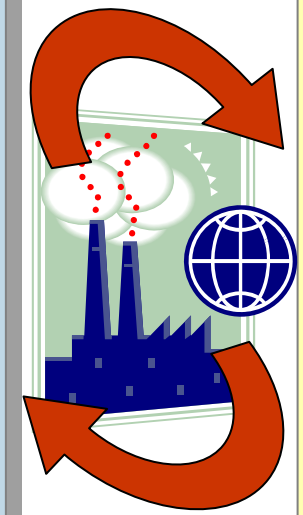
Policy

2004: EU program on CIP (EPCIP) and CI Warning Info Network (CIWIN) (DG JLS)

2006: Communication and Directive on EPCIP – sectoral approach (DG JLS)

2007: Communication on Protecting Europe's Critical Energy and Transport Infrastructure (DG TREN)

2007: INFSO consultation process for policy initiative in ICT sector (DG INFSO)



Research

IST-FP6 (2002-2006)
9 RTD projects, 36M€ EU funding

PASR (2004-2006)
5 projects for about 11,5M€ – total cost

FP7: Joint ICT-Security Research Initiative

Joint Call between Security and ICT Themes
Critical Infrastructure Protection (1)

Aims

- Create more secure and dependable Critical Infrastructures (CI's)
  - ➔ Protect CI's against deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour
- Develop new technical solutions that support and refine the policy options and legislative processes
- 'Coalition formation' and 'consensus building'

Joint Call between Security and ICT Themes
Critical Infrastructure Protection (2)

1 objective – 2 foci (ICT, Security) – 5 topics:

ICT

1. **ICT-SEC-2007.1.7**
   1. Understand and Manage complex interconnected and interdependent CI's — **CP**
   2. Build secure and resilient networked and distributed information and process control systems; Risk analysis, security configuration & management, forensics — **CP**
   3. Develop research roadmaps, metrics, benchmarks, International-Cooperation activities — **CSA**

Security

1. **ICT-SEC-2007-1.0-01** — **CP**
   Risk assessment and contingency planning for interconnected transport or energy networks — **CSA**
2. **ICT-SEC-2007-1.0-02**
   Modeling and simulation for training — **CP**
3. **ICT-SEC-2007-1.0-03**
   Optimized situational awareness through intelligent surveillance of interconnected transport or energy infrastructures — **CP**
4. **ICT-SEC-2007-1.0-04**
   ICT support for first responders in crisis occurring in critical infrastructures — **CP**

Joint Call between Security and ICT Themes
Critical Infrastructure Protection (3)

Focus of the ICT Theme – Budget: 20 m€

Technology building blocks for creating secure, resilient, responsive and always available information infrastructures linking critical infrastructures (CI's)

a) mastering interactions and complexity of LCCI; preventing against cascading effects; providing recovery and continuity (self-adapted and self-healing); quantifying dependability and resilience of interdependencies

b) Designing and developing distributed information and process control systems; systemic risk analysis and security configuration; dynamic assurance frameworks; security forensics

c) Longer term visions and roadmaps; metrics and benchmarks -> certification and standardisation; international cooperation; coordination with other programmes or initiatives

Joint Call between Security and ICT Themes
Protection of Critical Infrastructures (4)

Focus of the Security Theme – Budget: 20 m€

Technology building blocks for secure, resilient and always available transport & energy infrastructures that survive malicious attacks or accidental failures and guarantee continuous provision of services

a) ICT-SEC-2007-1.0-01: Risk assessment and contingency planning for interconnected transport or energy networks

b) ICT-SEC-2007-1.0-02: Modelling and simulation for training

c) ICT-SEC-2007-1.0-03: Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures

d) ICT-SEC-2007-1.0-04: ICT support for first responders in crises occurring in critical Infrastructures

Joint FP7 Call between Security and ICT Themes
Critical Infrastructure Protection
Expected Impact

- Improving significantly the security, performance, dependability and resilience of CI's (while considering also organizational, human, societal and legal aspects)
- Reinforcing European industry's potential for leadership
- Increasing and preserving trust in the use of technologies for the protection of CI's
- More effective protection through enhanced co-operation, coordination and focus
- Contribution to the development and promotion of metrics, standards, evaluation & certification methods and best practice in security of CI's

Joint Call between Security and ICT Themes
Critical Infrastructure Protection (2)

1 objective – 2 foci (ICT, Security) – 5 topics:

ICT

1. **ICT-SEC-2007.1.7**
   1. Understand and Manage complex interconnected and interdependent CI's — **CP**
   2. Build secure and resilient networked and distributed information and process control systems; Risk analysis, security configuration & management, forensics — **CP**
   3. Develop research roadmaps, metrics, benchmarks, International-Cooperation activities — **CSA**

Security

1. **ICT-SEC-2007-1.0-01** — **CP**
   Risk assessment and contingency planning for interconnected transport or energy networks — **CSA**
2. **ICT-SEC-2007-1.0-02**
   Modeling and simulation for training — **CP**
3. **ICT-SEC-2007-1.0-03**
   Optimized situational awareness through intelligent surveillance of interconnected transport or energy infrastructures — **CP**
4. **ICT-SEC-2007-1.0-04**
   ICT support for first responders in crisis occurring in critical infrastructures — **CP**

Joint ICT-SEC Call
The Funding Schemes: CPs

STREPs for ICT Theme, Capability projects for Security Theme

Aim

- Targeting a specific objective in a clearly defined project approach
- Fixed overall work plan with stable deliverables that do not change over the life-time of the project
- Two types of activity or combination of the two:
  - → RTD activity designed to generate new knowledge to improve competitiveness and/or address major societal needs /or
  - → A demonstration activity aiming to validate technologies offering potential economic advantages but which can not be commercialised directly (e. g. testing of product like prototypes)

  as well as:
  - Project management activities (including innovation related activities like protection of knowledge dissemination and exploitation
- Evaluated by 3 experts without hearings

CPs: Up to 36 M€
at least 3 legal entities from 3 MS or AC
Expected average project size: 2-5 m€ (total cost)
Expected average duration: 2-4 years

Joint ICT-SEC Call
The Evaluation Criteria: CPs

Evaluation criteria applicable to Collaborative project proposals focusing on the joint call of the ICT and the Security Themes		
S/T QUALITY **"Scientific and/or technological excellence (relevant to the topics addressed by the call)"**	**IMPLEMENTATION** **"Quality and efficiency of the implementation and the management"**	**IMPACT** **"Potential impact through the development, dissemination and use of project results"**
• Soundness of concept, and quality of objectives • Progress beyond the state-of-the-art and / or integration of existing solutions in innovative applications for security • Quality and effectiveness of the S/T methodology and associated work plan • Contribution to tangible and demonstrable improvements in security	• Appropriateness and efficiency of the management structure and procedures • Quality and relevant experience of the individual participants • Quality of the consortium as a whole (including complementarity, balance, participation of end-users) • Appropriateness of the allocation and justification of the resources to be committed (budget, staff, equipment)	• Contribution, at the European and/or international level to the expected impacts listed in the work programme under the relevant topic/activity • Appropriateness of measures for the dissemination and/or exploitation of project results notably by (public) end-users, and management of intellectual property

Joint ICT-SEC Call
The Funding Schemes: CAs

Aim

- Designed to promote and support the ad hoc networking and co-ordination of research and innovation activities at national, regional and European level over a fixed period for a specific purpose
  - by establishing in a coherent way coordinated initiatives of a range of research and innovation operators, in order to achieve improved cooperation of the European research
- May combine the following two types of activities:
  - Co-ordination activities;
  - Consortium management activities
  - (Coordination actions do not conduct S&T research !)
- Evaluated by 3 experts without hearings

CAs: up to 4 M€

at least 3 legal entities from 3 MS or AC

→ Expected average project size: around 0.5 m€

→ Expected average duration: 6 months to 3 years

→ Grant to budget; 100% contribution; fixed overhead of 7%

Activities

- Each Coordination Action shall propose a work plan, incorporating all or some of the following types of mid/long term collaborative activities:
  - Organisation of events (conferences, meetings); Performance of studies, analysis; Exchanges of personnel; Exchange and dissemination of good practice; Setting up of common information systems; Setting up of expert groups; Definition, organisation, management of joint or common initiatives; Management of the action

Joint ICT-SEC Call
The Evaluation Criteria: CAs

Evaluation criteria applicable to Co-ordination actions focusing on the joint call of the ICT and the Security Themes		
S/T QUALITY **"Scientific and/or technological excellence (relevant to the topics addressed by the call)"**	**IMPLEMENTATION** **"Quality and efficiency of the implementation and the management"**	**IMPACT** **"Potential impact through the development, dissemination and use of project results"**
• Soundness of concept, and quality of objectives • Quality and effectiveness of the co-ordination mechanisms, and associated work plan • Contribution to the coordination of high quality research	• Appropriateness and efficiency of the management structure and procedures • Quality and relevant experience of the individual participants • Quality of the consortium as a whole (including complementarity, balance) • Appropriateness of the allocation and justification of the resources to be committed (budget, staff, equipment)	• Contribution, at the European and/or international level to the expected impacts listed in the work programme under the relevant topic/activity • Appropriateness of measures for spreading excellence, exploiting results and disseminating knowledge through engagement with stakeholders and the public at large

Joint ICT-SEC Call
The Funding Schemes: SAs

Aim

- Designed to
  - underpin the implementation of the programme
  - complement the other FP7 funding schemes,
  - help in preparations for future Community RTD policy activities and
  - stimulate, encourage and facilitate the participation of SMEs, civil society organisations, small research teams, newly developed and remote research centres, as well as setting up research clusters across Europe
  - Cover one off events or single purpose activities
- May combine the following two types of activities:
  - Support activities,
  - Consortium management activities
  - (Coordination actions do not conduct S&T research !)
- Evaluated by 3 experts without hearings

SAs: up to 4 M€

→SA proposal may be presented by a consortium or a single organisation, from any country or countries

→Expected average project size: around 0.5 m€

→ Expected average duration: 6 months to 3 years

→ Grant to budget; 100% contribution; fixed overhead of 7%

Activities

- Each Support Action (SA) shall have a work plan, which may consist of one or more (as appropriate on a case by case basis) of the following activities:
  - Conferences, seminars, working groups and expert groups; Studies, analysis; Fact findings and monitoring; Preparatory technical work, including feasibility studies; Development of research or innovation strategies; High level scientific awards and competitions; Operational support, data access and dissemination, information and communication activities

Joint ICT-SEC Call
The Evaluation Criteria: SAs

Evaluation criteria applicable to Support actions focusing on the joint call of the ICT and the Security Themes		
S/T QUALITY **"Scientific and/or technological excellence (relevant to the topics addressed by the call)"**	**IMPLEMENTATION** **"Quality and efficiency of the implementation and the management"**	**IMPACT** **"Potential impact through the development, dissemination and use of project results"**
• Soundness of concept and quality of objectives • Quality and effectiveness of the support mechanisms and associated work plan	• Appropriateness and efficiency of the management structure and procedures • Quality and relevant experience of the individual participants • Quality of the consortium as a whole (including complementarity, balance) [only if relevant] • Appropriateness of the allocation and justification of the resources to be committed (budget, staff, equipment)	• Contribution, at the European and/or international level to the expected impacts listed in the work programme under the relevant topic/activity • Appropriateness of measures for spreading excellence, exploiting results and disseminating knowledge through engagement with stakeholders and the public at large

Handling "Sensitive" Projects
What is a sensitive project?

- **A "Sensitive" Project is handling:**
  - Data or information requiring protection against unauthorised disclosure: classified information
  - Information or materials subject to security restrictions
  - Material subject to export- or transfer-control

- **No "Sensitive" Proposals are allowed in the call**
  (no classified information in a proposal)
- **BUT: a Proposal could lead to a "Sensitive" Project**
  (project that could use classified/sensitive background and/or produce classified/sensitive foreground)

Legal basis for classified Grant agreements
2001/844/EC amended by 2006/548/EC – OJ L215, 5.8.2006

Handling “Sensitive” Projects
Sensitive proposals with non-EU participants

- **EU classification is limited to EU Member States**
- **Sensitive projects can include participants from associated or third countries**
- **Countries having a security agreement with the EU (Council level) could refer to that security agreement for handling sensitive information and material**
- **Special MoU (Memorandum of Understanding) could be agreed between the countries involved in the handling of sensitive information/material of a project limited to that project**

No restriction for the participation to sensitive projects for associated countries and from third countries if no access foreseen to sensitive information/material

Information to Proposers: Use of sensitive information

- No classified information to be used in the proposal
- However, the project could use classified/sensitive background and/or produce classified/sensitive foreground
- In that case,
  - The proposal should be flagged on page 1 of the part B of the proposal as security sensitive
  - The table of deliverables must specify the level of classification for each deliverable
  - A Security Aspect Letter (SAL) must be attached to the proposal

Handling “Sensitive” Projects
Scrutiny Procedure

For each sensitive project proposal of the selection list:

- → **The concerned ICT / Security Committee Members or ICT / Security Committee Observers will be requested (via their national security authority representative) to verify that all security aspects are properly addressed and to reach an agreement among themselves**
- → **the scrutiny procedure is done, in a 2 months period, following the evaluation and before the start of the negotiation of the flagged projects**

The results of the scrutiny could be:

- → **go ahead with negotiation;**
- → **recommendations for the negotiation;**
- → **Recommendation not to finance the proposal**

Proposers receive report with the conclusions of the scrutiny procedure

Handling “Sensitive” Projects
Some recommendations

- Be serious about the sensitivity declaration
- Consider carefully the requirements for accessing sensitive information/material in a project (limit it as far as possible)
- Get reference of all applicable EU and national legislation
- Contact your National Contact Point (NCP) – see CORDIS
- Contact your NSA for sensitive proposals (OJ L193 of 23.7.2005 p.31-36)
- For non-EU countries find out if there are some security agreement between your country and EU

Timing of the Joint Call

Call FP7-ICT-SEC-2007-1

40 M€

(20 M€ ICT, 20 M€ Security)

03 August 2007	Publication
29 November 2007	Deadline
3rd week January 2008	Evaluation
February – March 2008	Screening of Sensitive Proposals
March – April 2008	Inter-Services Consultation
March – April 2008	Meetings of Programme Committees (ICT & Security)
April - May 2008	Start of negotiations
2nd half 2008	1st set of grant agreements signed

Budget Call and Information

- **Indicative Call Budget: 40 m€**
  - Collaborative Projects: **Up to 36 m€**
  - Coordination and Support Actions: **Up to 4 m€**
- **Web Site on the Joint Call**

http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=70

Practical Guidelines for Proposers

- When submitting a proposal: indicate in which Theme your proposal fits best (ICT or Security)
- Proposals must not contain any classified information
- Special handling of proposals requiring classified inputs or producing classified outputs [Special Committee Procedure, SAL]
- All topics open for international cooperation
- Associated countries treated like Member States
- For the topics of the Security Theme only: All 4 topics are open for 75% EC funding
  → If 75% funding is requested, demonstrate in the proposal that the required conditions apply!
- Involve End users!
- Electronic submission of proposals

- Evaluation Procedure
  - Single-step evaluation procedure (in January 2008)
  - Joint evaluation of submitted proposals by experts from supply and demand side
  - Evaluators could move transparently proposals from one Theme to the other, according to where it fits best (centre of gravity)

Further Information & Contact

Call information

→ **CORDIS call page and work programme, evaluation forms: http://cordis.europa.eu/fp7/calls/**

General sources of help:

- → **The Commission's FP7 Enquiry service** : **http://ec.europa.eu/research/enquiries**
- → **National Contact Points** : **http://cordis.europa.eu/fp7/ncp_en.html**

Specialised and technical assistance:

- → **CORDIS help desk : http://cordis.europa.eu/guidance/helpdesk/home_en.html**
- → **CORDIS FP7 service : cordis.europa.eu/fp7/participate_en.html**
- → **Risk sharing financing facility (European Investment Bank)**: **http://www.eib.org/rsff**
- → **EPSS Help desk** e-mail: **support@epss-fp7.org**
- → **IPR helpdesk http://www.ipr-helpdesk.org**
- → **ICT Information Desk** email: **ict@ec.europa.eu**
- → **Security Information Desk** e-mail: **entr-security-research@ec.europa.eu**

Contacts for the Joint Call:

- → [ICT Theme] Angelo.Marino AT ec.europa.eu,
- → [Security Theme] Laurent.Cabirol AT ec.europa.eu

Slides on ongoing R&D work under the 6th Community Framework Programme (2002-2006)

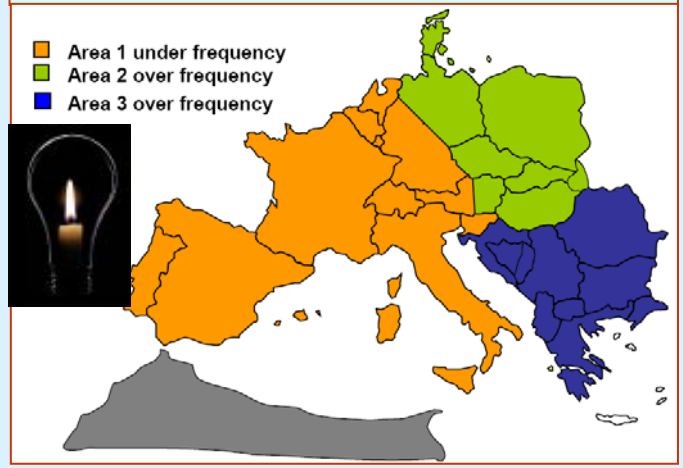
Protection of Critical Information Infrastructures
Ongoing IST-FP6 work

Areas of R&D work

- Understanding large complex Critical Infrastructures (CI's) and their interdependencies;
- Modelling & simulation environments
- Incident detection and decision support for CI's
- Resilience and survivability of future "ubiquitous computing systems"
- Fault-tolerant architectures
- Research coordination on Critical Information infrastructure Protection (CIIP)

Saturday 04 NOV 06 at 22:10

A system disturbance of the electricity grid originated in Germany led to disruptions of supply in many EU countries



Protection of Critical Information Infrastructures

Some ongoing IST-FP6 work

Projects found at:
http://cordis.europa.eu/ist/trust-security/projects.htm

Integrated Project - IRRIIS

- Novel and advanced model and simulation tools in synthetic environment
- MIT components for preventing & limiting cascading effects and support automated recovery and service continuity

STREP- CRUTIAL

- modelling approaches for understanding and mastering interdependencies
- fault-tolerant architectural configurations and models enabling dependable control and management

Coordination Action - GRID

- Methods to assess reliability, security and risks
- Management, control and protection schemes including architectures and devices

Critical Infrastructures Protection
Ongoing PASR Work

- Vital Infrastructures Threats and Assurance (VITA)
- Transport Infrastructures Protection System (TRIPS)
- Open Robust Infrastructures (ROBIN)
- Protection of Air Transportation and Infrastructure (PATIN)
- On-line monitoring of drinking water (WATERSAFE)