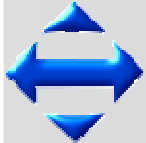


7. Rámcový program

priorita **BEZPEČNOST**

Informačný deň BA, 28.3.2007
Ing. Peter Beňo, APVV



7. Rámcový program



Základné novosti 7. RP

Trvanie 2007- 2013

Vyšší rozpočet

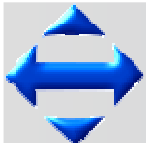
Administratívne zjednodušenie

Pridanie základného výskumu- riadený mimo EK

Väčšia podpora výskumnej infraštruktúry
a regionálneho rozvoja

Technologické platformy

Spoločné technologické iniciatívy



7. RP



Špecifické programy – základná schéma 7. RP

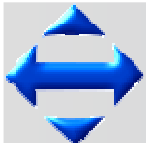
Spolupráca

Nápady

Ľudia

Kapacity

+ JRC + EURATOM



SPOLUPRÁCA **Tematické priority**

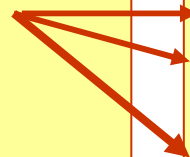


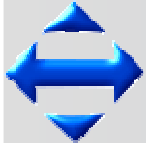
FP6

1. Vedy o živote
2. Informačné technológie
3. Nano., mat., procesy
4. Letectvo a kozmický priestor
5. Kvalita a bezpečnosť potravín
6. Udržateľný rozvoj
globálne zmeny a ekosystémy
7. Občania a spoločnosť

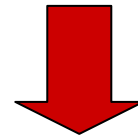
FP7

1. Zdravie
2. Potraviny, poľnohospodárstvo
a biotechnológie
3. Informačné a komunikačné tech.
4. Nano., mat., procesy
5. Energia
6. Životné prostredie a
klimatické zmeny
7. Doprava a letectvo
8. Socio-ekonomické vedy
9. Kozmický priestor
- 10. Bezpečnosť (nové)**



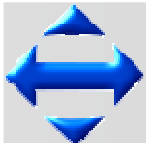


SPOLUPRÁCA



Návrhy spoločných projektov musia spĺňať nasledovné podmienky:

- **podielové financovanie**
- **vychádzať z priorít**
- **medzinárodné zloženie konzorcia**
- **novosť v európskom merítku**
- **predpísanú formu, časť A, B**



7. RP



NÁPADY



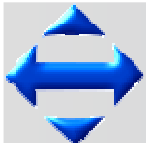
Bádateľský výskum na hraniciach súčasného poznania vo všetkých oblastiach vedy a techniky

Žiadne priority, jediným hodnotením bude výnimočnosť vedeckého nápadu

Podporovať najlepšie myšlienky a ľudí, ich nezávislosť, vytvárať podmienky

Iné pravidlá účasti, v projekte stačí jedno pracovisko, alebo 1 vedecký pracovník. Neúspešný projekt sa môže opakovane podať len raz, po úspešnom projekte , ďalší až za rok.

Riadenie nezávislou Vedeckou výskumnou radou



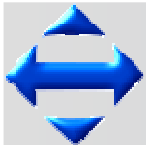
7. RP



L'UDIA



Školenie výskumníkov, MC
Dlhodobý tréning a rozvoj vedeckej kariéry
Spolupráca priemysel – akadémia
Rozvoj medzinárodnej spolupráce
Špecifické akcie



7. RP



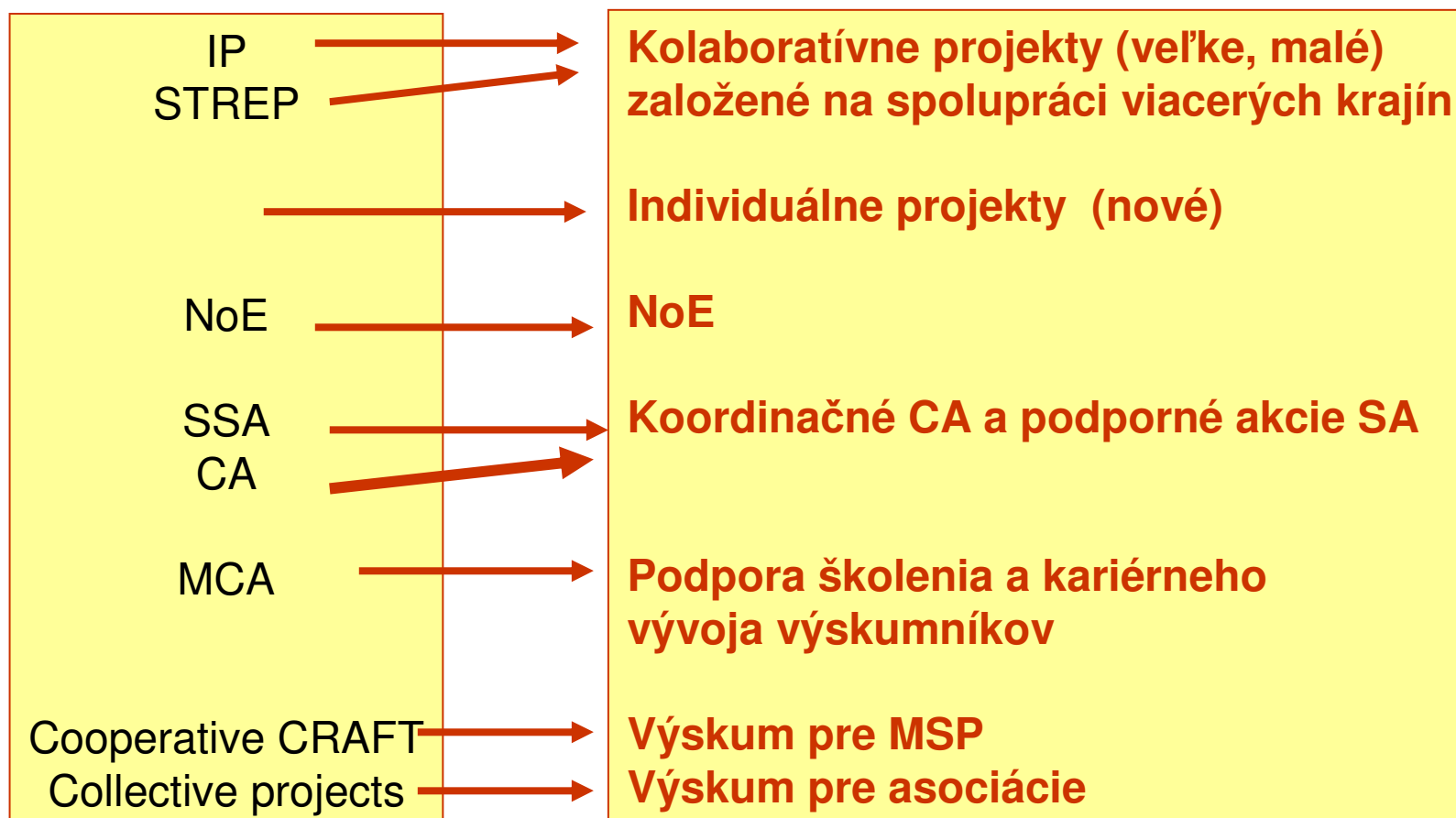


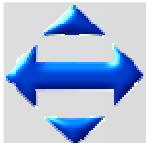
Nástroje (Funding Schemes)



FP6

FP7





Rozpočet



FP6

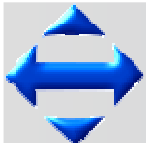
17 500 mil euro

FP7

**54 582 mil. euro
v bežných cenách**

**Rozpočet nebude dvojnásobný
40 % priemerné zvýšenie oproti 6. RP**

Spolupráca	32 365 mil. euro
Myšlienky	7 460 mil euro
Ľudia	4 728 mil. euro
Kapacity	4 217 mil. euro
JRC	1 751 mil. euro
Euratom	2 751 mil. euro

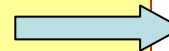


7. RP



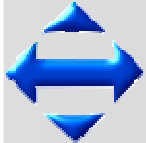
Zvýšenie rozpočtu ide

2/3 na nové aktivity
1/3 na doterajšie



Bezpečnosť
IDEAS

SPOULUPRÁCA **30 %** viacej
ERC nové
ĽUDIA **50 %** viacej
Kapacity MSP **50 %** viacej



7. RP

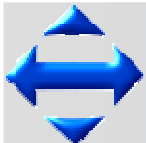


Pravidlá účasti 1

Bez modelov financovania !!!

(Financovanie podľa typu organizácií a špecifického programu)

- 75 % zdôvodniteľných nákladov neziskových výskumných organizácií
- 75 % stredné a vysoké školy
- 75 % ústredné orgány (public bodies)
- 75 % u MSP
- 50 % u ziskových výskumných organizácií
- 50 % demonštračné aktivity
- 100 % hraničný výskum
- 100 % koordinačné a podporné akcie
- 100 % Akcie podporujúce tréning a kariérny rast výskumníkov
- 100 % Riadenie konzorcia



7. RP



Pravidlá účasti 2

Ďalšie finančné pravidlá pre nepriame náklady, teda **RÉŽIA**

(PN – subkontrakt) x (0,2 resp. 0,6 resp. 0,4)

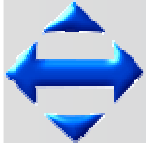
Výskumné projekty:

A/ 60 % pre neziskové verejné organizácie, univerzity, neziskové výskumné organizácie a MSP do konca roku 2009, potom 40 % s tendenciou prechodu na model plných nákladov, bývalý FC

B/ u ostatných účastníkov 20 % priamych nákladov,

Nevýskumné projekty

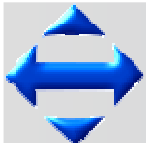
C/ 7 % pre podporné projekty CA, SA



7. RP



Výhoda je, že oproti 6. RP bude možné plánovať mzdové náklady bez tých obmedzení, ktoré platili v 6. RP pri použití modelu AC



7. RP



Čo treba dofinancovať ?

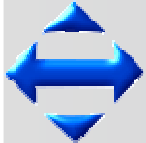
25 % ceny projektu

**10 % ceny projektu, ktoré EK vyplatí po
skončení projektu**

DPH

Kto dofinancuje ?

Vlastné zdroje, MŠ SR, Štrukturálne fondy



7. RP

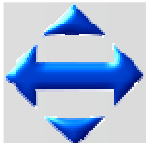


Financovanie NoE

Financovanie Siete exelentnosti (NoE)

Zásady:

- **Jednorázový grant (Lump sum)**
- **Výpočet podľa počtu výskumníkov**
- **23.500 euro/rok/výskumníka**
- **Max.počet výskumníkov je určený v pracovnom programe**
- **Platby budú uhrádzané na základe zhodnotenia výsledkov**



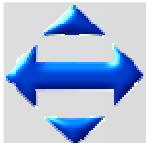
7. RP



Financovanie CA, SA

Financovanie podporných projektov CA a SA:

- 100 %** úhrada nákladov projektu
- 7 %** z priamych nákladov je réžia
- 100 %** riadenie konzorcia
- 100 %** tréning



7. RP



Pravidlá účasti 4

Finančný audit

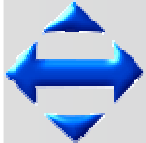
Stále menej.

Ak sú náklady > 375.000 euro audit je povinnosť každé obdobie riešenia

year 1 EC contribution= 175.000 No certificate

year 2 EC contribution= 200.000 Certificate has to be submitted (since $175.000+200.000 > 375.000$)

year 3 EC contribution= 150.000 No certificate because <375.000 when cumulated with all previous payments for which a certificate on the financial statements has not been submitted



7. RP

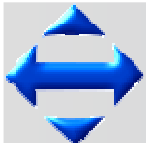


Pravidlá účasti 5

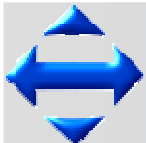
Kontrakt nahradí grant agreement

1. Spoločná technická zodpovednosť
2. Nebude spoločná finančná zodpovednosť, spoluzodpovednosť preberá EK
 - ✓ Zriadenie „Guarantee fund“ – bez finančných rizík, možnosť prijať slabšieho partnera, odpadá požiadavka finančných záruk od MSP

Zvýšená autonómia konzorcia - ako spravovať projekt, zmeny účastníkov



Ako sa zorientovať v dokumentoch ?



7. RP



cordis.europa.eu



European Union Research Funding



FP7 (2007-2013)



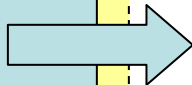
Find a Call



Activity Areas' Calls

-
-

Security



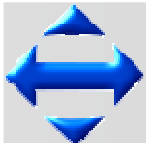
**FP7-
SEC-
2007-
1**



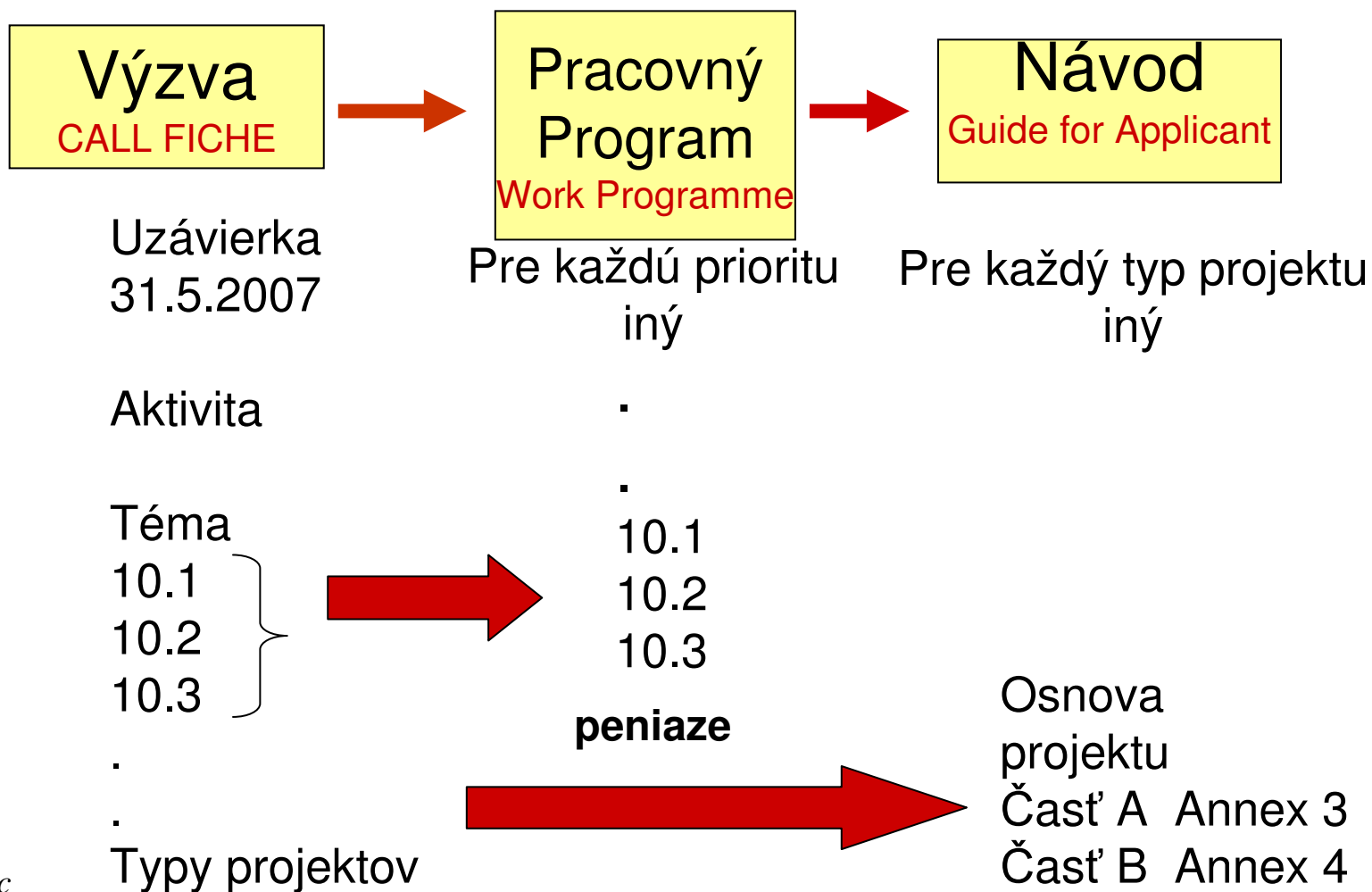
Call Fiche

Work Programme

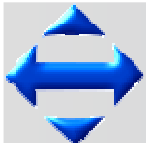
Guides for Applicants



7. RP – základné dokumenty



Marec
2007



7. RP



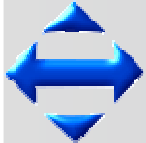
Ako písať projekt ?

Časť A, A1, A2, A3

Annex 3 Guide for Applicants

Časť B Annex 4 Guide for Applicants

LEN ELEKTRONICKY **EPSS !!!!**



7. RP



Záver 1

Pozitívne zmeny pre výskum

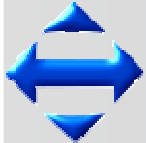
Všeobecne vyššie financie

Žiadne finančné modely

Možnosť plánovať mzdové prostriedky aj u kmeňových zamestnancov

Väčší dôraz na obsah ako na formu

Vyššie režijné náklady



7. RP



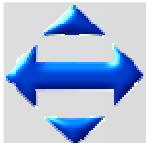
Záver 2

Negatívne zmeny pre výskum

Nutnosť dofinancovať chýbajúcich 25 %

Nutnosť použiť vlastné zdroje, alebo
žiadať o dofinancovanie MŠ SR alebo
štrukturálne fondy.

Pripravovať sa na prechod na model
priamych nákladov.



7. RP



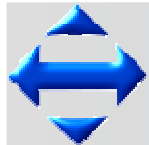
Záver 3

Pozitívne zmeny pre výrobné orientované MSP

Zvýšenie grantu na projekt z 50% na 75%
Zvýšenie réžie na 60 % (do konca r. 2009)
Vynechanie predkladania bankových záruk

Odstránenie kolektívnej finančnej zodpovednosti,
čo uľahčí vstup MSP do výskumných konzorcií,

Zvýšenie rozpočtu pre MSP o 50%



Čo je priorita SECURITY ?

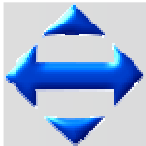


Čo je SECURITY...

- civilne orientovaná
- venuje sa socio-ekonomickým otázkam ako aj technologickým riešeniam
- venuje sa antagonistickým aktivitám (teroristické útoky, priemyselné katastrofy a prírodné katastrofy)
- krízovo orientovaná (pred, počas a po kríze)
- podpora bezpečnostnej politiky v 4 hlavných úlohách a 3 prierezových aktivitách
- vývoj aplikovaných technológií s dôrazom na zapojenie koncových užívateľov

Čo nie je Security...

- vojensky orientovaná
- výlučne technologicky orientovaná
- zaoberajúca sa otázkami „safety“
- orientácia na všeobecnú diskusiu o spoločnosti, politike, klimatické a environ. zmeny v budúcnosti
- aktivity za týmito úlohami (okrem prípadu naliehavej politickej potreby)
- základný výskum a výlučné vytváranie nových technológií

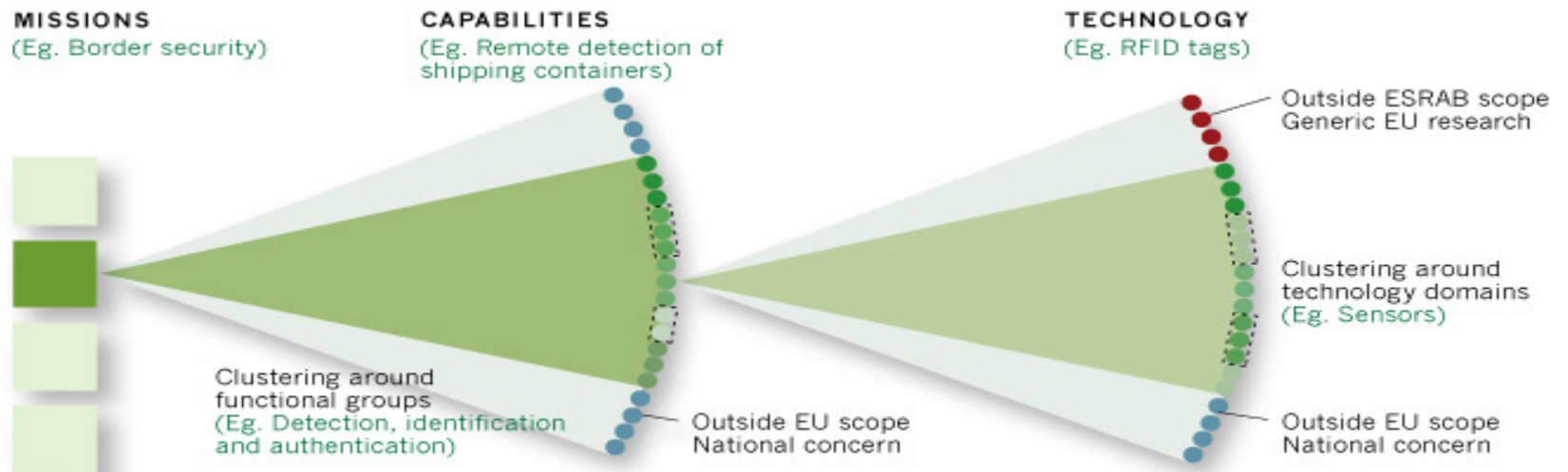


Ako funguje prioritizácia SECURITY?

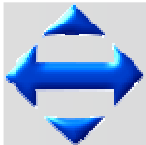


ESRAB sa orientuje na 4 hlavné úlohy (misie):

- Ochrana pred terorizmom a organizovaným zločinom
- Ochrana hraníc
- Ochrana kritických infraštruktúr
- Obnovenie bezpečnosti v prípade krízy

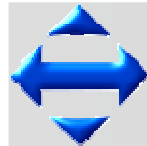


Marec
2007



Štruktúra WP

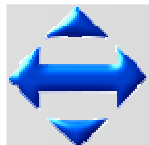
*Marec
2007*



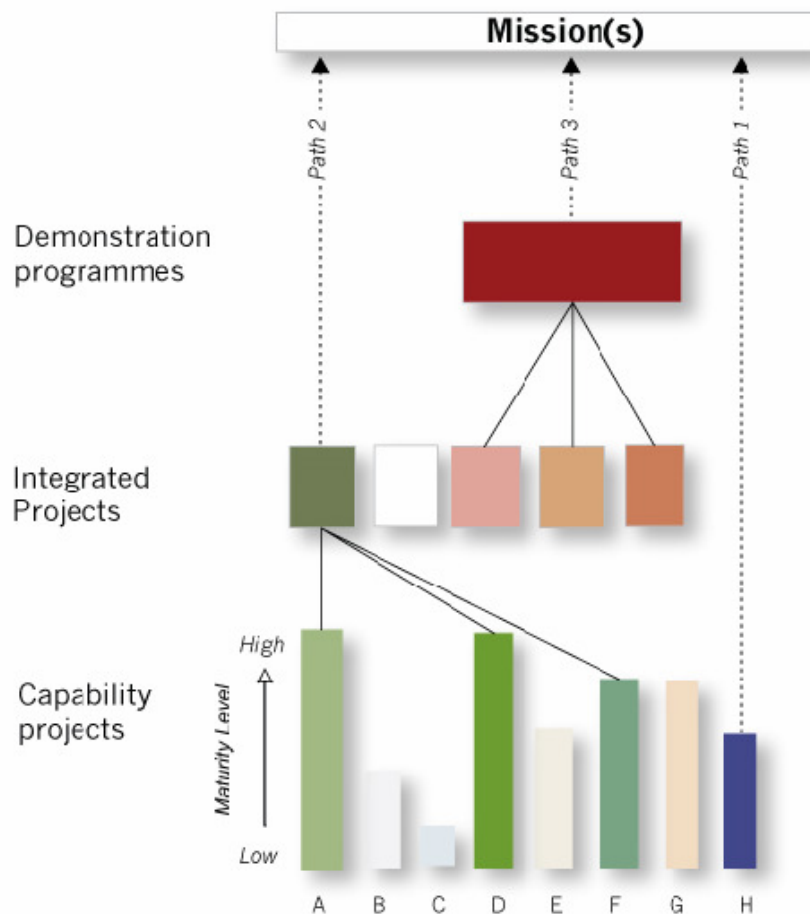
Aktivity v rámci priority SECURITY



- **4 Security úlohy / aktivity:**
 - Bezpečnosť obyvateľstva
 - Bezpečnosť infraštruktúry a verejných služieb
 - Inteligentný dozor a bezpečnosť hraníc
 - Obnovenie bezpečnosti a ochrany pri vzniku krízy
- **3 Prierezové aktivity:**
 - Integrácia bezpečnostných systémov , vzájomná prepojitelnosť a ich súčinnosť
 - Bezpečnosť a spoločnosť
 - Koordinácia a štrukturalizácia výskumu bezpečnosti



Ako funguje priorita SECURITY?



← **System systémov**
- kombinácia výstupov z IP
- Multi-mission

← **Vývoj systému a jeho overovanie**
- kombinácia „capability projects“
- orientovaný na konkrétnu úlohu

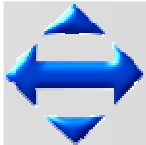
← **Capability development**
- vývoj 1 technológie
- Multi misijný aj misijne orientovaný



Ako funguje priorita SECURITY?



- **SP Cooperation** **32.413 M€**
 - Health
 - Food, Agriculture & Biotechnology
 - Information & Communication Technologies
 - Nanosciences, Nanotechnologies, Materials & new Production Technologies
 - Energy
 - Environment (including Climate Change)
 - Transport (including Aeronautics)
 - Socio-economic Sciences & Humanities
 - Space
 - **Security** **1.400 M€**



Security v 7.RP



- **4 Security úlohy / aktivity:**

1. Bezpečnosť obyvateľstva
2. Bezpečnosť infraštruktúry a verejných služieb
3. Inteligentný dozor a bezpečnosť hraníc
4. Obnovenie bezpečnosti a ochrany pri vzniku krízy

- **3 Prierezové aktivity:**

5. Integrácia bezpečnostných systémov , vzájomná prepojitelnosť a ich súčinnosť
6. Bezpečnosť a spoločnosť
7. Koordinácia a štrukturalizácia výskumu bezpečnosti

- **Oblasť** Demonstration projects
celkové náklady do výšky 30-40 M€,
fáza 1: 1 - 1,5 roky,
fáza 2: ~ 4 roky

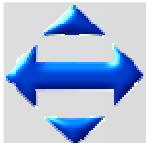
- **Oblasť** Integration projects
celkové náklady do výšky 10-25 M€, ~ 4 roky

- **Oblasť** Capability projects
celkové náklady do výšky 2-5 M€, 2-4 roky

Nemýliť si s „funding schemes“:

Collaborative projects (CP)

Coordination and support actions (CSA)



Security v 7.RP

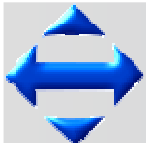


Demonstration Projects:

- systém systémov
- poskytujú spoločný rámec v oblastiach mimoriadneho európskeho záujmu
- závisia na vývoji v „building blocks“ (IP, CP)

ESRAB identifikoval v 7.RP 5 tém pre DP:

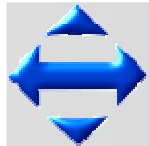
- | | |
|---|------------|
| ➤ Celoeurópsky integrovaný systém kontroly hraníc | uverejnené |
| ➤ Bezpečnosť verejnej dopravy | v 1. výzve |
| ➤ Systém krízového manažmentu | |
| ➤ Logistika a bezpečnosť dodávateľských reťazcov | |
| ➤ CBRNE | |



Demonštračné projekty



- **fáza 1 :**
 - Definovanie strategických „roadmaps“
 - rozširovanie povedomia medzi „účastníkmi“ bezpečnosti v EÚ, obzvlášť koncový užívateľia
 - Funding scheme: Coordination and support action
0.5 - 1 M€, ~ 1 rok
- **fáza 2 (neskoršie výzvy, samostatné návrhy a evaluácia) :**
 - implementácia demonštračného projektu
 - veľké konzorciá (vrátane verejných / súkromných účastníkov a kon. užívateľov)
 - blízke štandardizácii a trhu
 - Funding scheme: Collaborative project
30 - 40 M€, ~4 roky



Kedy pripravovať DP, fázu 1?

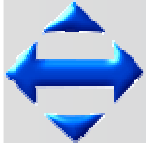


- Rozumieť oblasti bezpečnostnej politiky
- Analyzovať potreby na strane dopytu
- Identifikovať všetkých relevantných účastníkov zo strany dopytu a ponuky (úrady, agentúry, kon. užívateľov, priemysel, výskum, univerzity atď.)
- Plán zapojenia účastníkov do projektu
- Analyzovať technologické smery a ďalšie ukazovatele
- Analyzovať stupeň vyspelosti jednotlivých technológií, IPR ...
- Skontrolovať možné sporné body na národných úrovniach (transfer / export licencií, utajované informácie)
- Porozumieť možným rizikám a zaobchádzanie s nimi
- Plánovanie budúceho vývoja demonštračných aktivít vrátane socio-ekon., technologického a školiaceho aspektu

- > možný 1 grant na tému
- fáza 2 nebude automaticky pridelená konzorciám, ktoré sú úspešné vo fáze 1, nová výzva a nové evaluácie
- WP pre témy z fázy 2 budú vytvorené na základe výstupov z fáze 1



WP Aktivity	Oblasť WP (témy)	Collaborative projects (CP)	Coordination and support actions (CAs and SAs)
Aktivity 1 - 4	Demonstration project, fáza 1		1-1,5 roka 0,5 M€
	Demonstration project, fáza 2	4 roky 30-40 M€	
	Integration project	4 roky 10-25 M€	
	Capability project	2-4 roky 2-5 M€	
Aktivita 5		2-4 roky 2-5 M€	
Aktivita 6		2-4 roky up to 2 M€	0,5-3 roky, 0,5 M€
Aktivita 7			0,5-3 roky, 0.5 M€

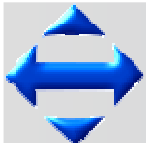


Security



- v roku 2007
 - 1 pracovný program
 - 2 výzvy na podávanie projektov

*Marec
2007*



Security Research Call 1 **FP7-SEC-2007-1**



22 December 2006 **Zverejnenie výzvy**

31 May 2007 **Deadline**

~155 M€

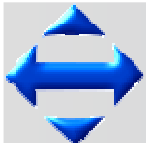
Jún/Júl 2007 **Evaluácia**

August 2007 **Zoznam podporených projektov**

September 2007 **Začiatok negociácií**

December 2007 **1. podpisy GA**

cordis.europa.eu/fp7/calls/



Načasovanie Joint Call ICT & Security 1
FP7-ICT-SEC-2007-1



30 August 2007 **Zverejnenie**

29 November 2007 **Deadline**

20 + 20 M€

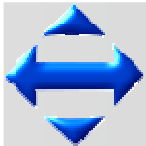
December 2007 **Evaluácia**

Január 2008 **Zoznam podporených projektov**

Február 2008 **Začiatok negociácií**

Jeseň 2008 **Podpisovanie GA**

cordis.europa.eu/fp7/calls/



WP 2007 - Misia / Aktivita 1: Bezpečnosť obyvateľstva



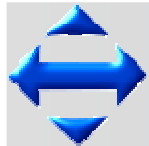
2 Integration projects:

- Intelligent urban environment observation system
- Integrated mobile security kit

6 Capability projects:

- Detection, identification & authentication
- Stand off scanning and detection of hidden dangerous materials and/or stowaways, fast and reliable alerting and specification
- Improved control of explosives throughout their “lifecycle”
- Positioning & localisation
- Localisation and tracking of chemical components in substance production
- Observation through water, metal, ground etc
- Situation awareness & assessment (surveillance)
- Water distribution surveillance
- Secure strategic information management system

Collaborative projects



WP 2007 - Misia / Aktivita 2: Bezpečnosť infraštruktúry a verejných služieb



1 Demonstration project:

- Security of critical infrastructures related to mass transportation (phase 1)

CSA

1 Integration project:

- Integrated protection of rail transportation

4 Capability projects:

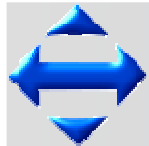
Detection, identification & authentication

- Detection of unattended goods and of owner
- Detection of abnormal behaviour of vehicles both in wide and small land areas
- Detection of abnormal behaviour

Situation awareness & assessment (surveillance)

- Small area 24 hours surveillance

Collaborative projects



WP 2007 - Misia / Aktivita 3: Inteligentný dozor a bezpečnosť hraníc



1 Demonstration project:

- Integrated border management system (phase 1)

} **CSA**

3 Integration projects:

- Main port security system (including containers)
- Unregulated land borders and wide land surveillance system
- Integrated check points security

3 Capability projects:

Detection, identification & authentication

- Air 3D detection of manned and unmanned platforms

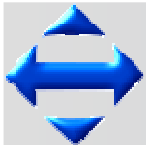
Situation awareness & assessment (surveillance)

- Surveillance in wide maritime areas through active and passive means

Communication

- Solutions for ensuring disruption-tolerant end-to-end communication availability, relying on physical and logical technologies, on diversity of hybrid systems

Collaborative projects



WP 2007 - Misia / Aktivita 4: Obnovenie bezpečnosti a ochrany pri vzniku krízy



4 Integration projects:

- Network enabled command and control system
- Integrated specialist search and rescue system
- Post incident basic service restoration system
- Wireless communication for EU crisis management

4 Capability projects:

Situation awareness & assessment (surveillance)

- Developing a common operational picture between regional and national authorities, first responders etc.

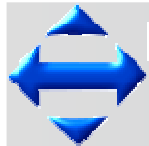
Command & control

- Intelligent decision support

Incident response

- Personal equipment
- Neutralisation of devices/effects

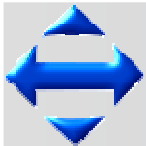
Collaborative projects



Integrácia bezpečnostných systémov , vzájomná prepojitelnosť a ich súčinnosť



- V tejto výzve nie sú témy k tejto aktivite
- Môžu byť podané projekty v aktivite 1, 2, 3 a 4.
- Témy budú vypísané pre spoločnú výzvu Joint Call ICT & Security 1



WP 2007 – Prierezová aktivita 6: Bezpečnosť a spoločnosť (1)



Citizens and Society

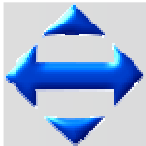
- Understanding factors that cause citizen's feeling of security and insecurity
- Human behaviour before, during and after crisis situations to understand how people react to threat alerts and security instructions
- Communication strategies of public authorities (including media strategies) before, during and after crises concerning risks, security threats and measures

Understanding organisational structures and cultures of public users

- Behavioural, organisational and cultural issues to understand public user needs including those for joint European action
- Inventories of existing national resources, institutional mandates and practices across relevant sectors

Foresight, scenarios and security as an evolving concept

- Research in broad societal foresight to capture new and emerging threats as well as other aspects of security as an evolving concept (e.g. ethical and economic aspects)
- Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)



WP 2007 – Prierezová aktivita 6: Bezpečnosť a spoločnosť (2)

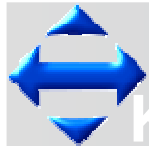


Security Economics

- Research survey on the emerging field of European security economics research to provide an analytical framework for complementary research
- European Security Indicator: methodological research to provide a few select indicators of security and security policy in Europe measuring the effects of both insecurity and security policies on the economy
- Public finance: Studying the scale, function and roles of various types of government security spending across Europe and time

Ethics and justice

- How to take the necessary measures to ensure the security of citizens while respecting the civic rights and how this is implemented in practice, particularly addressing the issue of privacy and security
- Ethical implications of the continuum of internal and external security

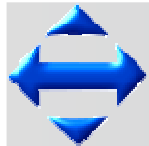


WP 2007 – Prierezová aktivita 7:

Koordinácia a štrukturalizácia bezpečnostného výskumu



- Technology Watch
- European Security Research Networks, incl. for standardisation
- Network of facilities for test and validation of security related products
- Transparency and networking amongst Member States and associated countries
- Supply chains and market integration
- Trans-national co-operation among NCP's



Joint Call ICT & Security 1 FP7-ICT-SEC-2007-1



ICT témy

- vývoj technológií pre vytváranie, monitorovanie a riadenie bezpečnosti,
- tvorba odolných a vždy použiteľných informačných infraštruktúr schopných odolať plánovaným útokom a náhodným poruchám,
- prepojenie na kritické infraštruktúry,
- zabezpečenie integrity dát a plynulé poskytovanie dôveryhodných služieb,
- podpora dynamicky sa meniacim požiadavkám

Security témy

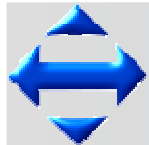
- Hodnotenie rizika a riešenie nepredvídaných udalostí v oblasti vzájomne prepojených dopravných a energetických sietí
- Inteligentný dozor vzájomne prepojených dopravných a energetických sietí
- Podpora ICT jednotkám prvého nasadenia pre krízy vyskytujúce sa v kritických infraštruktúrach



Aktualizácia WP



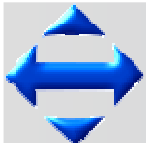
- **22. December 2006**: výzva publikovaná s provizórnym WP – vs.1
Prečo ?: FP7 vstúpil do platnosti 1. Januára 2007
- Formálne bol WP prijatý **27. Februára** a zverejnený 28. Februára - vs. 2
- V **apríli 2007** bude presne stanovený rozpočet na rok 2008 a bude uverejnená 3. verzia WP



Budúce výzvy

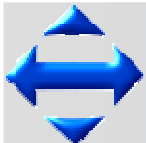


- Ročné výzvy priority SECURITY budú zverejnené v Júni 2008
- Podmienky pre viac spoločných výziev
- Stanovenie ročných rozpočtov
- **Security Research Call 2 (2008)**
 - 3 Demonstration projects fáza 1: Logistic and supply chain security; CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives); Aftermath crisis management system
 - Integration projects: Advanced forensic toolbox; Secure strategic information management system; Detection system for abnormal behaviour; Open space security; Built infrastructure protection; Sea borders surveillance system; Extended smart borders; First responder of the future
- **Security Research Call 3 (2009)**
 - 2 Demonstration projects fáza 2 (na základe výsledkov fázy 1- Security Research Call 1)
- **Security Research Call 4 (2010)**
 - 3 Demonstration projects fáza 2 (na základe výsledkov fázy 1- Security Research Call 2)
- **Security Research Calls 5 (2011) and 6 (2012):**
 - zatiaľ nestanovené

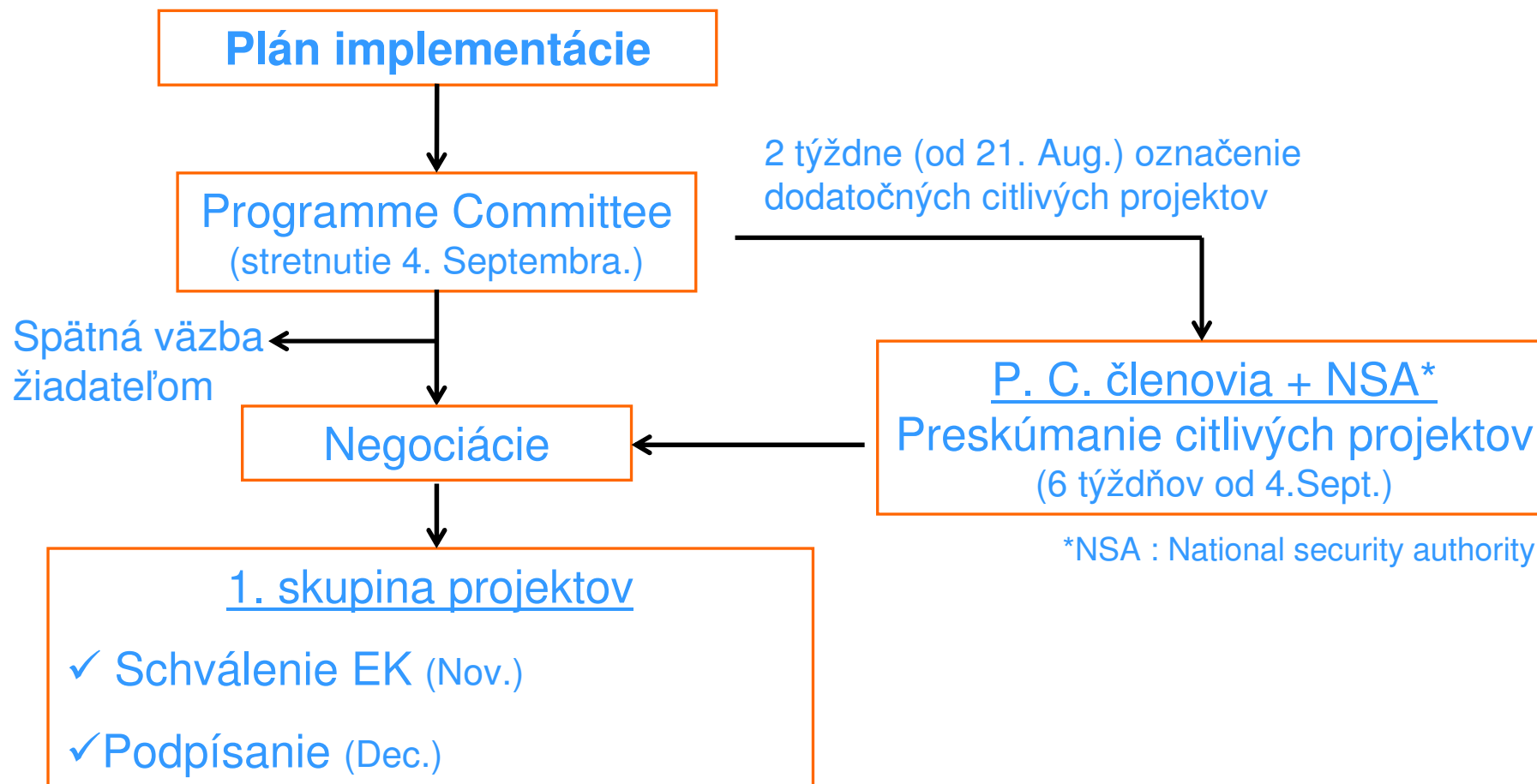


Evaluácia

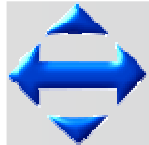
*Marec
2007*



Evaluácia



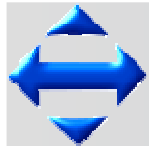
*NSA : National security authority



FP7- Security Call 1 : eSubmission



- Povinné podávanie projektov elektronicky EPSS
- Veľmi podobné ako FP6
- EPSS bude k dispozícii min. mesiac pred **deadlinom**



Evaluačné kritériá



3 rovnaké kritériá pre SP Spolupráca :

- Scientific / technological quality
- Implementation
- Impact

Ale rozdielna štruktúra kritérií pre CSA a Collaborative projects

Každé kritérium je ohodnotené od 1 do 5.

Threshold pre každé kritérium je 3, celkový musí byť aspoň 10.



Štruktúra kritérií



Pre všetky projekty:

Vedecká a/alebo technická úroveň	Kvalita a efektívnosť realizácie a riadenia	Potenciálny dopad cez vývoj, šírenie a použitie výsledkov
Vhodnosť návrhu a kvalita cieľov	Vhodná štruktúra a postupy riadenia	Príspevok na európskej a/alebo medzinárodnej úrovni podľa očakávaných výsledkov v príslušnom pracovnom programe



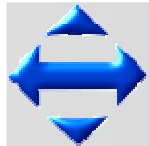
Štruktúra kritérií **Kolaboratívne projekty**



Vedecká a/alebo technická úroveň	Kvalita a efektívnosť realizácie a riadenia	Potenciálny dopad cez vývoj, šírenie a použitie výsledkov
Pokrok za súčasný stav poznania	Kvalita konzorcia ako celku (zahrňujúc komplementaritu a rovnováhu)	Vhodnosť opatrení pre šírenie/využívanie výsledkov výskumu a riadenia IPR
Kvalita a efektívnosť VT metodológie a pracovného plánu	Vhodnosť predložených zdrojov (rozpočet, personál, zariadenia....)	

	<p>1. Scientific and/or technological excellence <i>(relevant to the topics addressed by the call)</i></p> <p>(award)</p>	<p>2. Quality and efficiency of the implementation and the management</p> <p>(selection)</p>	<p>3. The potential impact through the development, dissemination and use of project results</p> <p>(award)</p>
All funding schemes	<ul style="list-style-type: none"> • <i>Soundness of concept, and quality of objectives</i> 	<ul style="list-style-type: none"> • Appropriateness of the management structure and procedures • Quality and relevant experience of the individual participants 	<ul style="list-style-type: none"> • <i>Contribution, at the European [and/or international] level, to the expected impacts listed in the work programme under relevant topic/activity</i>
Collaborative projects	<ul style="list-style-type: none"> • <i>Progress beyond the state-of-the-art</i> • Quality and effectiveness of the S/T methodology and associated work plan 	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • Appropriateness of measures for the dissemination and/or exploitation of project results, and management of intellectual property.
Networks of Excellence	<ul style="list-style-type: none"> • <i>Contribution to long-term integration of high quality S/T research</i> • Quality and effectiveness of the joint programme of activities and associated work plan 	<ul style="list-style-type: none"> • Quality of the consortium as a whole (including ability to tackle fragmentation of the research field, and commitment towards a deep and durable integration) • Adequacy of resources for successfully carrying out the joint programme of activities 	<ul style="list-style-type: none"> • Appropriateness of measures for spreading excellence, exploiting results, and disseminating knowledge, through engagement with stakeholders and the public at large.

		1. Scientific and/or technological excellence <i>(relevant to the topics addressed by the call)</i> (award)	2. Quality and efficiency of the implementation and the management (selection)	3. The potential impact through the development, dissemination and use of project results (award)
Co-ordination & support actions	CA	<ul style="list-style-type: none"> • Contribution to the co-ordination of high quality research • Quality and effectiveness of the co-ordination mechanisms, and associated work plan 	<ul style="list-style-type: none"> • Quality of the consortium as a whole (including complementarity, balance) [for SA: only if relevant] • Appropriateness of the allocation and justification of the resources to be committed (budget, staff, equipment) 	<ul style="list-style-type: none"> • Appropriateness of measures for spreading excellence, exploiting results, and dissemination knowledge, through engagement with stakeholders, and the public at large.
	SA	<ul style="list-style-type: none"> • Quality and effectiveness of the support action mechanisms, and associated work plan 		
Research for the benefit of specific groups		<ul style="list-style-type: none"> • Innovative character in relation to the state-of-the art • Contribution to advancement of knowledge / technological progress • Quality and effectiveness of S/T methodology and associated work plan 	<ul style="list-style-type: none"> • Quality of the consortium as a whole (including complementarity and balance) • Appropriateness of the allocation and justification of the resources to be committed (budget, staff, equipment) 	<ul style="list-style-type: none"> • <i>Appropriateness of measures for the dissemination and/or exploitation of project results, and management of intellectual property</i>



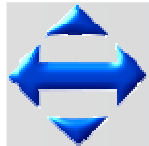
Evaluačné kritériá



Kritéria sú detailne popísané v „Guides for applicants“

Špecifikum pre Security napr.:

- zahrnutie koncových užívateľov
- projekty orientované na aktivitu - misiu
- Komplementarita s PASR



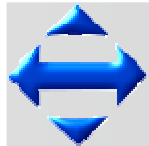
Plán evaluácie.



1. týždeň (25-29 Jún) : IP + CSA
2. týždeň(2-6 Júl) : Capability projects
3. týždeň (9-13 Júl) : hearings (výsluch) for IP (nad threshold)

Rozdielne skupiny expertov pre jednotlivé oblasti.

Navrhovatelia budú upovedomený o výsledku po zasadnutí P.C. (4. September)



Horné limity financovania

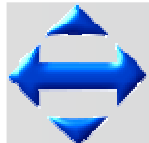


Kolaboratívne projekty:

- do výšky 75% pre neziskové výskumné organizácie, stredné a vysoké školy, MSP
- Do výšky 50% pre veľké podniky
- pre prioritu SECURITY 75%:
 - pri vývoji technológií pre veľmi malé trhy a s rizikom marketingového zlyhania
 - a zrýchlenom vývoji zariadení ako odozva na nové hrozby
 - musí byť presvedčivo preukázané v návrhu projektu

Coordination and support actions:

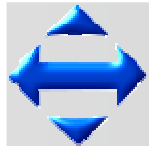
- do 100%



INCO



- Definícia = tretie krajiny, ktoré nepatria medzi AC
- Všeobecné pravidlo: sú vítané
- Je potrebné zdôrazniť prínos z medzinárodnej spolupráce
- Vlastné zdroje financovania okrem rozvojových krajín
- výnimky sú špecifikované vo WP
- V roku 2007 sú všetky témy otvorené INCO



Preskúmanie citlivých návrhov



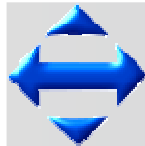
Citlivým návrhom je návrh, ktorý :

- zaobchádza s utajovanými informáciami (CI)
- dochádza k výmene utajovaného materiálu (potreba transferu resp. exportných licencií)
- príslušný objekt záujmu je viazaný na národné alebo medzinárodné právne normy

Identifikovanie citlivých materiálov:

- Navrhovateľmi
- Evaluátormi
- Komisiou
- Výborom

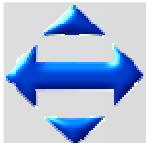
Hĺbkové preštudovanie citlivých materiálov odpovedajúcim členom programového výboru s podporou národnej bezpečnostnej agentúry



Čo možno považovať za utajované informácie



- **Informácie požadujúce ochranu proti neoprávnenému použitiu**
- **Biologické, chemické, rádioaktívne a nukleárne materiály**
- **Informácie a materiály, ktoré spadajú pod bezpečnostné opatrenia**
- **Materiály, ktoré sú predmetom exportných kontrol**



Utajované informácie



- Každá krajina má svoj vlastný národný klasifikačný systém
- V záujme výmeny citlivých informácií v rámci EÚ bol vytvorený jednotný systém klasifikácie CI
- Tento je prijatý každou členskou krajinou
- V rámci EU projektu, CI môžu byť vymenené medzi členmi EU na základe tejto klasifikácie a procedúr pre ne stanovených
- Každý MS vytvoril vlastnú National Security Authority (NSA)
- NSA riadia klasifikačné procedúry pre entity v materskom členskom štáte



Úrovně klasifikácie CI

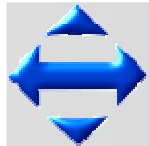


EU TOP SECRET: nepovolaná manipulácia môže spôsobiť mimoriadne vážne ohrozenie základných záujmov EU resp. jedného alebo viacerých MS. V rámci aktivít v FP7 nebudú žiadne návrhy obsahovať ***EU TOP SECRET informácie.***

SECRET UE: nepovolaná manipulácia môže vážne poškodiť základné záujmy EU resp. jedného alebo viacerých MS.

CONFIDENTIEL UE: nepovolaná manipulácia môže poškodiť základné záujmy EU resp. jedného alebo viacerých MS.

RESTREINT UE: nepovolaná manipulácia môže znevýhodniť záujmy EU resp. jedného alebo viacerých MS.



Citlivé návrhy s účasťou mimo Európy



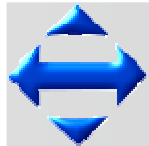
- **klasifikácia CI v EU** je záväzná len pre MS
- každý účastník v EU projekte musí rešpektovať svoju **národnú** legislatívu a reštrikčné opatrenia
- Citlivé projekty môžu zahŕňať účasť AC resp. tretích krajín
- krajiny, ktoré majú podpísaný tzv „**security agreement**“ s EU sa v prípade manipulácie s týmito inform. môžu naň odvolať
- špeciálne MoU (Memorandum of Understanding) môže byť dohodnuté medzi krajinami, ktoré sú súčasťou manipulácie s takýmito inform., ale len pre konkrétny projekt
- *V prípade, že v projekte nie sú CI, nie sú žiadne reštrikcie, ktoré by bránili účasti AC resp. tretích krajín*



Používanie citlivých informácií



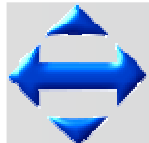
- v 1. výzve CI nesmú byť súčasťou návrhu projektu
- avšak, projekt môže pre svoje riešenie CI použiť resp. výstup z projektu môže byť CI
- v takom prípade
 - návrh projektu musí byť označený na prvej strane časti B ako „**security sensitive**“
 - tabuľka „**deliverables**“ musí špecifikovať klasifikačnú úroveň každého „**deliverable**“ (plnenia)
 - **Security Aspect Letter (SAL)** musí byť priložený k návrhu projektu
- *V budúcnosti budú otvorené výzvy kde sa bude manipulovať s CI*



Úvodná strana návrhu projektu časť B



- Theme 10: Security
- Call FP7-SEC-2007-1
- **DECLARATION: This proposal concerns/does not concern a security sensitive project**
- Proposal full title:
- Proposal acronym:
- Type of funding scheme:
 - Collaborative Project
 - Integration Project or Capability Project
- **Work programme topics addressed** (*if more than one, indicate their order of importance to the project*)
- Name of the coordinating person:
- List of participants:



Zoznam „Deliverables“ obsahujúcich CI



Del. no.	Deliverable name	WP no.	Lead participant	Estimated indicative person-months	Nature	Dissemination level	Delivery date
TOTAL							

Please indicate the dissemination level using one of the following codes:

PU = Public

PP = Restricted to other programme participants (including the Commission Services).

RE = Restricted to a group specified by the consortium (including the Commission Services).

CO = Confidential, only for members of the consortium (including the Commission Services).

CL restraint UE = Classified with the mention of the classification level “Restreint UE”

CL confidentiel UE = Classified with the mention of the classification level “Confidentiel UE”

CL secret UE = Classified with the mention of the classification level “Secret UE”



Security Aspects Letter



- **SAL musí byť súčasťou návrhu projektu a musí obsahovať:**
- **úroveň utajenosti (ich klasifikácia) **background** a **foreground****
- **požiadavka na vlastnenie vývoznnej licencie**
- **špeciálne opatrenia týkajúce sa niektorých materiálov**
- **prístup účastníkov k informáciám**
- **povolenia resp. splnomocnenia (alebo požiadavky)**
- **exportnú licenciu**

- *Toto musí byť vytvorené po dohode s NSA*



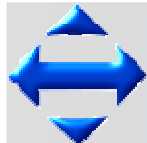
SAL (*Classified information*)



Use of classified Background information						
Subject	Classification level	Owner (+country)	Beneficiaries wanting to access			Comments including purpose of the access
			Name (+country)	Clearance	Date of access	

Production of classified Foreground information						
Subject	Classification level	Owner (+country)	Beneficiaries involved in production or wanting to access			Comments including purpose of the access and future use of information
			Name (+country)	Clearance	Date of production	

Marec
2007



SAL (*Export/transfer licence - topics submitted to legal restrictions*)



Exchange of sensitive material subject to export or transfer licence						
Subject	Type of material	Owner (+country)	Beneficiaries requiring access to sensitive material			Comments including purpose of the export or transfer
			Name (+country)	Licence ref	Date of transfer	

Topic submitted to legal restrictions						
Subject	Restrictions description	Ref to national or international legislation	Beneficiaries subject to restrictions			Comments
			Name (+country)	Action taken	Date of action	

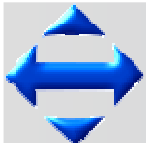
Marec
2007



Zaobchádzanie s citlivými návrhmi



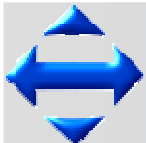
- **CI citlivé projekty musia byť označené navrhovateľmi projektu**
- **Evaluátori musia potvrdiť, že CI citlivé projekty sú označené navrhovateľmi**
- **Komisia má tiež právo kontrolovať CI citlivosť projektov**
- **po evaluácii, členovia PC a prísediaci pozorovatelia obdržia zoznam všetkých návrhov a zoznam doporučených projektov (návrhy na začatie negociácií a rezervný zoznam)**
- **členovia PC a prísediaci budú mať prístup k projektom s účasťou z ich krajiny**
- **členovia PC a prísediaci môžu určiť niektoré projekty ako CI citlivé**
- **všetky doporučené CI citlivé projekty budú podrobené hĺbkovej kontrole**



Híbková kontrola.



- Bude organizovaná individuálne podľa návrhov:
 - pre CI citlivé návrhy na doporučenie financ.
 - CM resp. NSA krajín, ktorých účastníci majú prístup k utajovaným inform.
- Výsledok:
 - odporučenie na negociácie
 - odporučenie nepodporiť projekt z dôvodu nízkej kompetentnosti resp. nedostatku skúseností s riadením CI pri niektorých účastníkoch projektu
- Navrhovatelia obdržia správu o tejto kontrole



Závery a odporúčenia

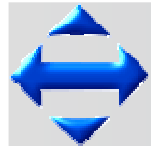


Čo a kedy?

- Work programme 2007/2008

Ako?

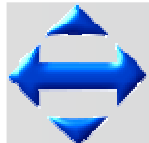
- Guides for applicants (3 verzie pre bezpečnosť – CP / CA / SA)



Na čo dávať pozor (1)



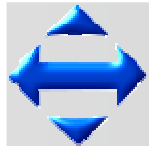
- návrhy musia súvisieť s témou vypísanou v pracovnom programe pre danú výzvu, v opačnom prípade budú vylúčené alebo nízko hodnotené
- navrhovatelia projektu musia rozumieť oblasti bezpečnostnej politiky, ktorú chcú podporiť
- návrhy projektov musia zohľadňovať filozofiu a štruktúru priority SECURITY (DP, IP, CP)
- zvoliť vhodnú schému financovania
- vytvoriť dobré konzorcium – zahrnúť koncových užívateľov
- splniť všetky pravidlá
- jasná prezentácia, jednoduchý jazyk
- pravidelne kontrolovať CORDIS
- dopísať návrh projektu a potvrdiť ho pre **deadlinom** !!



Na čo dávať pozor (2)



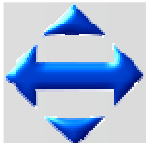
- **Consortium agreement** je povinný
- min. počet účastníkov podľa „Rules for participation“
- návrhy projektov nesmú obsahovať **utajené informácie** (dôvod na vylúčenie), navrhovaná aktivita môže CI obsahovať
- v prípade, že sa používajú utajené info. na vstupe resp. utajené info. predstavujú výstup projektu musí návrh projektu obsahovať „Security aspect letter“ definujúci úroveň utajenia.
- účastník, ktorí žiada o príspevok 75% musí preukázať:
 - že pôsobí na malom trhu
 - je vysoká pravdepodobnosť marketingového zlyhania
 - potrebu zrýchleného vývoja zariadenia v súvislosti s novými hrozbami



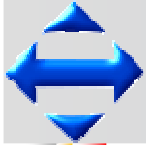
Na čo dávať pozor (3)



- konzorciá so zastúpením MSP a konečných užívateľov sú silne podporované, v procese hodnotenia v rámci kritéria „Quality and efficiency of the implementation and management“



- EU Security research websites:
 - <http://ec.europa.eu/enterprise/security>
 - <http://cordis.europa.eu/security>
 - <http://cordis.europa.eu/fp7/calls/>
- Helpdesk:
 - entr-security-research@ec.europa.eu



ĎAKUJEM ZA POZORNOSŤ

Ing. Peter Beňo

beno@apvv.sk www.apvv.sk

02/ 5720 4562