

# Examples of Public Procurement of R&D services within EU funded Security Research actions

*Paolo Salieri 18 / 10 / 2017*

*[paolo.salieri@ec.europa.eu](mailto:paolo.salieri@ec.europa.eu)*

PCP to steer the development of solutions towards concrete public sector needs, whilst comparing/validating alternative solution approaches

- No commitment to deploy.
- Alternative solutions to avoid supplier lock-in
- Risks & benefits of R&D (e.g. IPRs) shared with suppliers

## R&D / Pre-commercial Procurement (PCP)

### Phase 0



Curiosity  
Driven  
Research

### Phase 1



Solution design

Supplier A

Supplier B

Supplier C

Supplier D

### Phase 2



Prototype development

Supplier B

Supplier C

Supplier D

### Phase 3



Original development  
and testing of limited  
volume of 1<sup>st</sup> test  
products/services

Supplier B

Supplier D



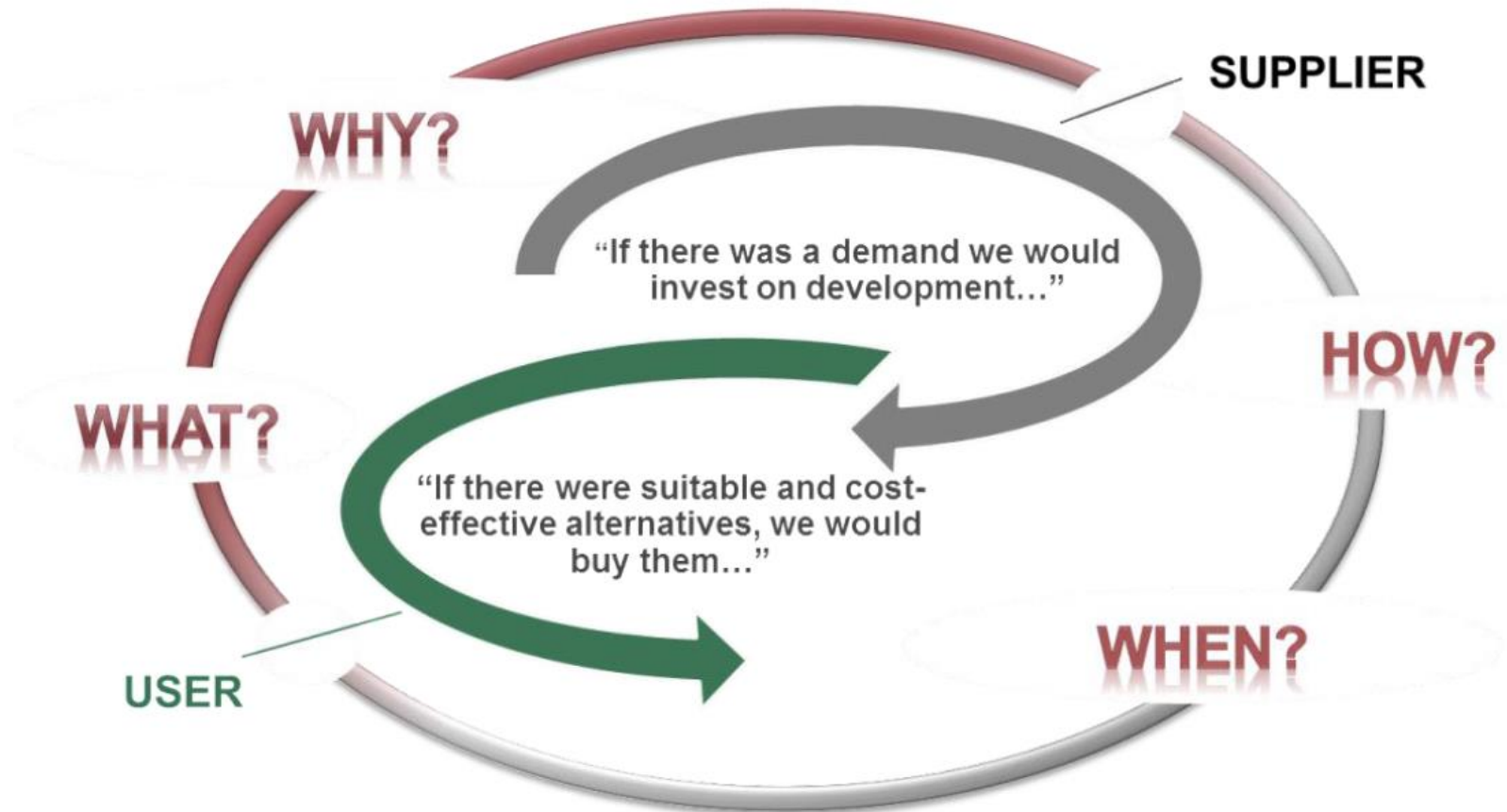
*On 15 /2/2011 the Programme Committee (PC) for Security Research decided not to foresee PCP in the implementation of FP7 Security Research Theme, because of "sensitivity" . It decided to postpone the matter to FP8 (Horizon 2020).*

*At the same time the Commission proposed Pre-Operational Validation (POV) as an "ad - hoc" set-up appropriate for the Security Research Theme (because of its mission driven nature).*

**POV is not PCP.**

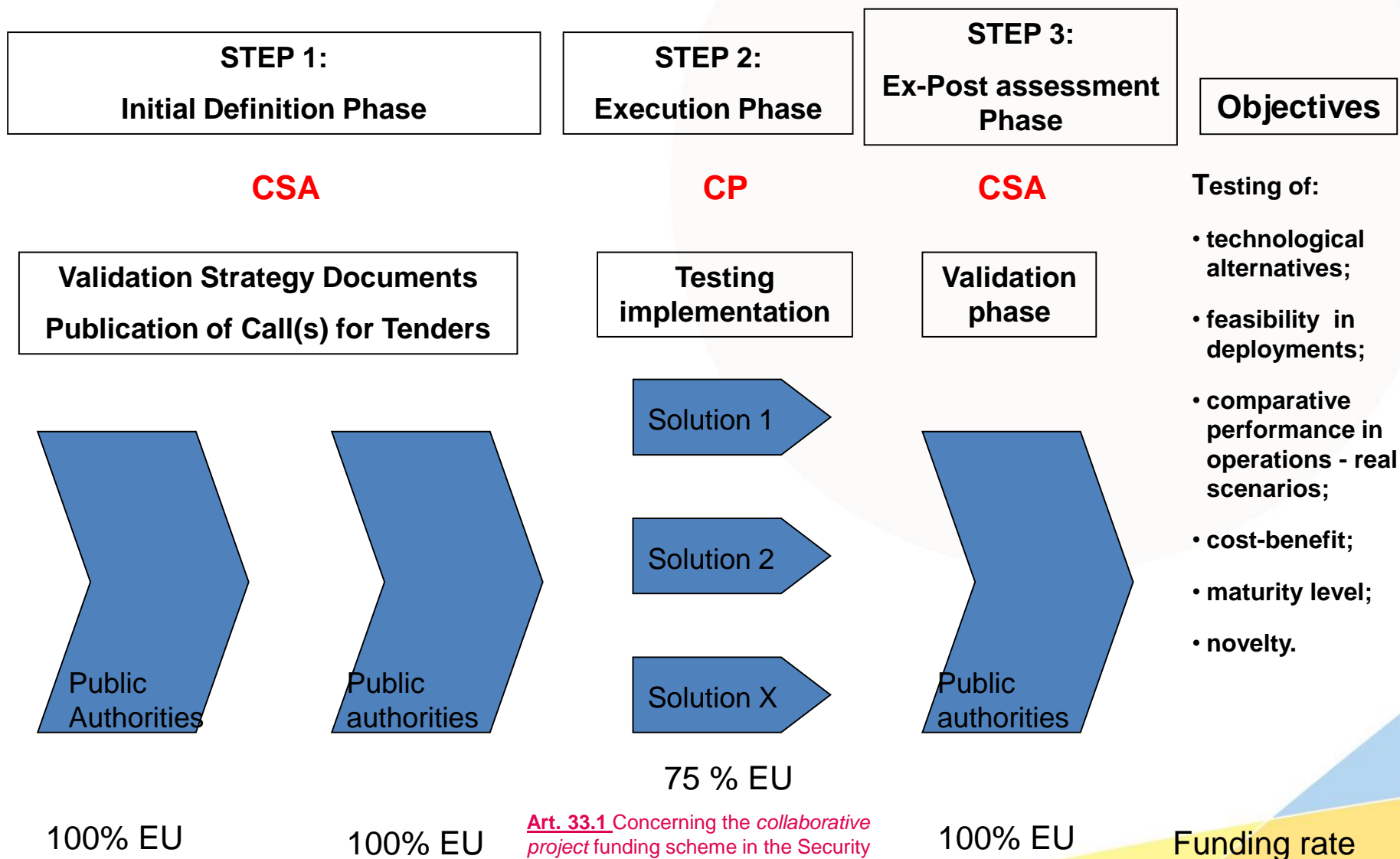
*POV is to provide an instrument for "validation" (as requested by industry) by the public sector (in an area of EU political relevance – such as Border Security).*

**In POV there is no R&D development in phases.**



*\*G. Whyles, JERA Consulting, "Innovation procurement for efficiency, quality and sustainability",  
PUBLIC DEMAND OF INNOVATION, MINECO, Madrid 2 October 2012*

# POV - Implementation modality



## 3 examples of POVs

*CLOSEYE* [www.closeye.eu](http://www.closeye.eu)



*EWISA* [www.ewisa-project.eu](http://www.ewisa-project.eu)

*EUCISE 2000*  
<http://www.eucise2020.eu/>



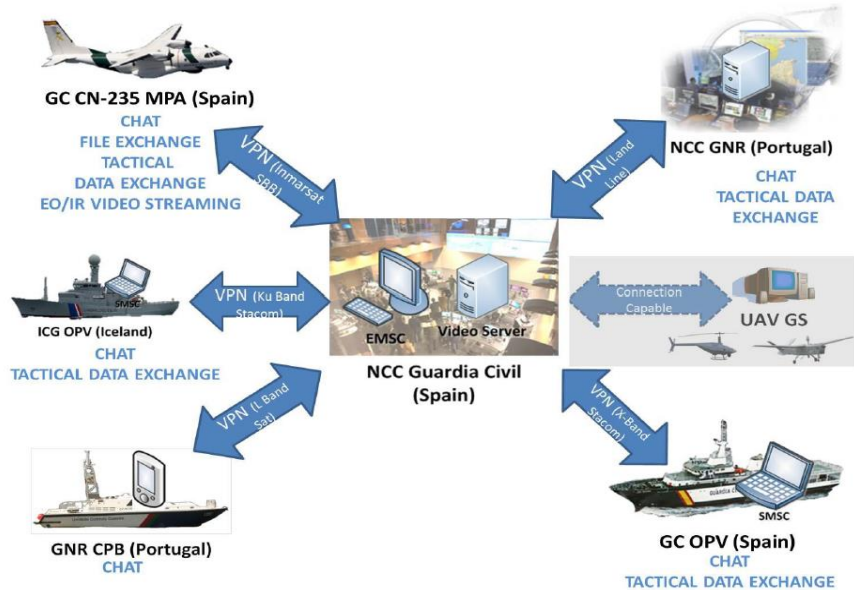


Figure 12 – Lot 2, Solution 1 functional design



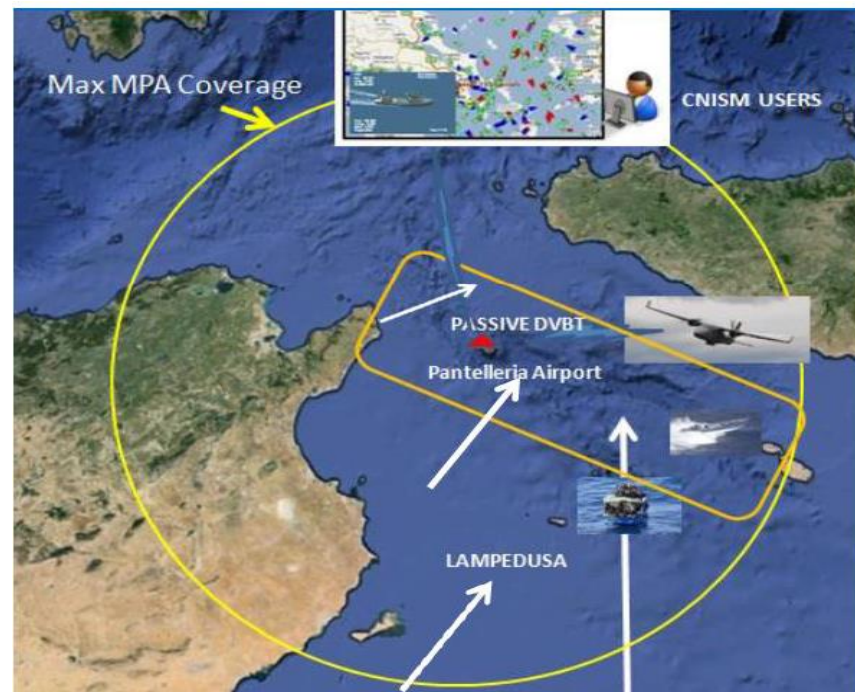
a scheme of the positive impact that CLOSEYE systems could have on each of the EUROSUR components:

	National Coordination Centres (NCC)	National Situational Pictures (NSP) *	Communication network	European Situational Picture (ESP) *	Common Pre-frontier Intelligence Picture (CPiP) *	Common application of surveillance tools
LOT1 SOL1						
DIISM	✓	✓		✓		
SAT	✓	✓				✓
MRI	✓	✓		✓		
LOT1 SOL2						
Passive RADAR	✓	✓				✓
ABNORMAL BEH.	✓	✓				✓
MPA	✓	✓	✓	✓		✓
LOT2 SOL1						
EMSC	✓	✓		✓		✓
SMSC	✓	✓		✓		✓
ICCCS	✓	✓		✓		✓
LOT2 SOL2						
Acoustic sensor	✓	✓				✓
ESM sensor	✓	✓				✓

Figure 18 – CLOSEYE systems impact on EUROSUR components



Figure 11 – Lot 1, Solution 2 functional design



# CLOSEYE

---

- ▶ Research carried out as planned / coordinated by Member States authorities, some of the validated applications are now in use (i.e. by Guardia Civil)
- ▶ Solutions tested in a heterogeneous multi-national and multi-asset environment (e.g. Joint Operation INDALO 2015), allowing the exchange of tactical surveillance data among units from different Member States participating in one same mission.
- ▶ Under the 2015 Union Actions for the Internal Security Fund, the Commission included the procurement of equipment and applications, call HOME/2015/ISFB/AG/ESUR/ *“to support the improvement of border surveillance by enhancing cooperation between Member States in the framework of EUROSUR, including, whenever appropriate, cooperation with third countries (especially neighbouring countries)”*. In December the Commission decided to award the ES/PT proposal (ESPIAS) which directly follows CLOSEYE.
- ▶ **The first (and only) example of an R&D project paving the way to an initiative (of Member States) supported by the ISF fund.**









## **Security Authorities realise that demand based R&D approach can bring them benefits.**

However:

**Big effort** (both by EC and participants) needed to mobilise demand side constituency. Much more for a PCP - POV project than for a collaborative R&D project.

For authorities to be motivated, support is needed at national level.

Encouraging a consortium of Member States to jointly approach the supply side (and take joint liability for R&D investments) requires much more commitment than encouraging "*typical*" participants in FP7 to file a grant application to recuperate a percentage of costs of their R&D.

Economic crisis made it more difficult to leverage additional resources.



EU Council (e.g. conclusions on *strengthening the internal security authorities' involvement in security-related research and industrial policy (9814/13)*) recognizes importance of using modern and adequate technologies in the field of internal security....

... "*which necessitates an increased involvement of internal security authorities in research and a proactive involvement with suppliers of modern security technologies*".

# CHALLENGES AND HURDLES for the Security market



***Market fragmentation:*** divided along national boundaries.

***Institutional nature:*** Demand mainly driven by requirements of (single) national public authorities that are the (if not sole) buyers of end products. The development is subject to a 'technology push' model and is limited by standards, again defined at the national level.

***Limits of the existing funding schemes:*** innovation cycles are quite long and existing funding schemes offer limited flexibility, whilst threats evolve rapidly and often require urgent responses. It is typically very difficult at the R&D stage to predict market opportunities.

***Aggregation of demand and supply:*** no previous history at EU level.

***Competition from third countries:*** growing, both from the US and from Asian competitors. US competitors benefit from a stable and strong internal market, as well as from recognised US labels.

# **PCPs in security research "Secure Societies"**

SEC-04-DRS-2017 Broadband communication systems

SEC-08-FCT-2017 Forensic Techniques on a) trace qualification, and b) broadened use of DNA

SEC-13-BES-2017 Next generation of information systems to support EU external policies

## SEC-04-DRS-2017: Broadband communication systems

### Specific Challenge:

- *So far each EU Member States has adopted its own (broadband) radio-communication system for security forces (police, first responders, etc.). Such systems are not necessarily compatible with each other.*

*Proposals must involve buyer organizations from at least 8 EU Member States or Associated Countries.*

### Expected Impact:

- *Established EU-interoperable broadband radio communication system for public safety and security, providing better services to first responders and police agencies and allowing shorter reaction times to prevent from casualties or victims, deployed by 2025.*
- **Indicative EU contr.** requested (and budget estimated): **10 M €**



# **Council conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe**

*3135th JUSTICE and HOME AFFAIRS Council meeting  
Brussels, 13 and 14 December 2011*

## **INVITES THE MEMBER STATES**

- to raise the level of forensic science by establishing and developing their relevant forensic science infrastructure, to ensure the highest quality of forensic service providers in order to meet the requirements of the state of art of science and technology, whilst respecting the rules regarding the protection of personal data,
- to designate a single point of contact in their respective administrations for disseminating information in relation to the activities developed to implement these conclusions, including the forensic science infrastructure,
- to engage in the coordination and cooperation of and between the relevant national stakeholders so as to ensure that the activities set out in the action plan will be followed up at national level,
- to support and assist the creation and development of a European Forensic Science Area,

## **INVITES THE COMMISSION**

- to consider the adoption of appropriate legal and non-legal measures to support the activities set out in the action plan,
- to support the Member States' efforts to raise the standards of forensic science products and services and the efforts of ENFSI, EUROPOL and other such international organisations as Member States consider appropriate in creating a European Forensic Science Area, in particular through appropriate funding measures in the context of the relevant multiannual framework programme.



# SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

## Scope:

The most promising forensic techniques need to be developed further, and brought up from experiment to a toolkit usable on a daily basis across Europe. This can be achieved if forensic laboratories from a broad variety of EU countries with diverse legal systems agree on common technical standards and join forces.

**Phase 0:** To prepare an inventory of forensic technologies already available at **TRL 4 or 5** (*validated in lab / relevant environment*), and to identify, within areas covered by the various **ENFSI** working groups, a subset of technologies to be brought at **TRL 8** (*system complete and qualified*);

**Phase 1:** To prepare the tenders packages for calls for tenders to build prototypes of a toolkit integrating the above-mentioned subset of technologies, that can be used across Europe; To develop EU-wide benchmarks and validation methods for forensic technologies;

**Phase 2:** To implement the calls for tenders to generate 2 prototype toolkits from 2 different sources;

**Phase 3:** To benchmark and validate the 2 toolkits against the methods developed during Phase 1;

**Phase 4:** To draft curriculum for pan European training in forensic technologies, and to plan for assessment across Europe; to **initiate the EU-wide certification of the toolkits** based on the results of Phase 3.

Forensic laboratories or institutes from a minimum of 5 EU Member States or international organisations must be beneficiaries and should be directly involved in the carrying out of the tasks foreseen in the grant (additional participation is encouraged).

Indicative EU contr. requested (and budget estimated for topic) : **10 M €**

## SEC-13-BES-2017: Next generation of information systems to support EU external policies

### Scope:

- *This topic is to support the development of a cost-effective common Situational Awareness, Information Exchange and Operation Control Platform.*

### Expected Impact:

- *Solid basis for a full-scale, cost-effective common situational awareness, information exchange and operation control platform for EU civilian external actions.*
- *Improved management of EU resources' allocated to EU civilian external actions.*

*Type of Action: Pre-Commercial Procurement (max **10M**) - **TRL 8** (system complete and qualified).*

## **SEC-13-BES-2017: Next generation of information systems to support EU external policies**

**Phase 1:** Plan research and design of the platform, based on common performance levels, requirements and associated specifications for the development of a cost-effective common situational awareness, information exchange and operation control platform for EU civilian external actions

Phase 1 should lead to calls for tender for services focusing on technologies identified to be part of a unique architecture.

**Phase 2:** The research and specification work to lead to at least 2 versions of flexible platforms to support, each, several scenarios for EU actions under different framework conditions.

**Phase 3:** By the end of 2020, the project should have documented, tested, and validated the use of each platform in at least two operational scenarios within actual multinational operations. The participation of relevant and competent authorities in the consortium of buyers is a prerequisite.

Indicative EU contr. requested (and budget estimated for topic) : **10 M €**

# The future

*In Security Research the exploitation of the PCP and PPI tools is still in its infancy. It will be further explored in future work programmes.*

- *SU-GM02-2018-2020: Strategic pre-commercial procurements of innovative, advanced systems to support security*
- *SU-GM03-2018-2019-2020: Pre-commercial procurements of innovative solutions to enhance security*