Security (law enforcement): AI-based pilots

DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI

Gilles Robine, DG HOME

Objective

- to enable the final validation and to foster the **uptake of artificial intelligence (AI) systems for law enforcement (LE)** by running large scale pilots in Law Enforcement Agencies (LEAs) premises

- to close the gap between prototypes developed with the support of EU funded programmes (i.e. up to TRL 7) and systems proven in operational environment that bring clear added value to police practitioners (i.e. TRL 8/9)

Security (law enforcement): AI-based pilots

- Budget: **€5 million**

- Co-funding rate: 50% except for SMEs where a rate of 75% applies

- Pre-financing up to 50% of the maximum grant

- Indicative project duration: 24 months

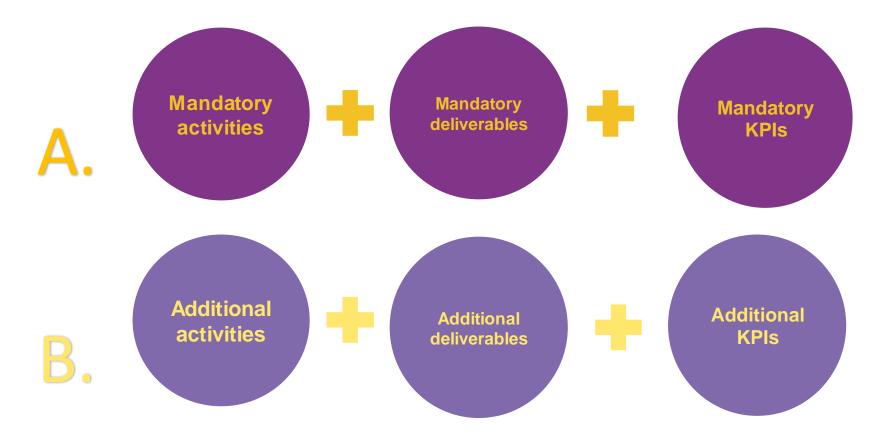- Detailed information is available online: Call Website,

Call Text and FAQ

Targeted stakeholders

- Minimum **2 law enforcement agencies (LEAs)** required for consortium composition -> main beneficiaries

- Other **public or private entities** are welcome in the consortium to provide support to LEAs on:
  - technical aspects, e.g. to develop solutions, create databases
  - legal aspects, e.g. to ensure compliance with EU regulations
  - to provide trainings.

- Participation of **Small and Medium Size Enterprises (SMEs)** is highly encouraged!

Logic in the call text

A.

Mandatory activities + Mandatory deliverables + Mandatory KPIs

B.

Additional activities + Additional deliverables + Additional KPIs

Mandatory activities

1. Identify and build on **technologies** with core functions of **digital investigations** (e.g. filtering and clustering illegal content, finding patterns and correlations in unstructured datasets) -> preference for **open source solutions**

2. **Roll out the tool(s) in LEA's premises** over at least a 6-month period

3. **Train** (when relevant), **adapt** (when relevant) and **evaluate** the solution(s) on operational datasets and real use cases

4. Demonstrate compliance of the solution(s) in terms of **usability, efficiency** and compliance with EU standards as regards **privacy** and **data protection** and provide further feedback on parts to be improved

5. **Ensure** a permanent **uptake** of the solution(s) after the piloting phase

6. Demonstrate that the solution(s) could **benefit a number of EU LEAs**

Additional recommended activities

1. Create a **set of annotated data** that could be shared among LEAs and Europol (and possibly feed the data space for security)

2. Develop and provide **trainings** to **law enforcement practitioners** that could be shared among LEAs and potentially **CEPOL** (European Union Agency for Law Enforcement Training) and **ECTEG** (European Cybercrime Training and Education Group)

3. Refer to the work of the **Europol Innovation Lab (EIL)** to identify **innovative solutions,** to **coordinate** the creation of large-scale pilots AI systems for LE amongst themselves and to **disseminate the results**

4. Refer to the work of **EACTDA** (European Anti-Cybercrime Technology Development Association)

5. **Coordinate & create synergies** with activities in Horizon 2020, Horizon Europe & Internal Security Fund Police programmes

What we do NOT want

1. Pilots that are **NOT** building on innovative solutions (e.g. mere purchasing of existing commercial tools)

2. Solutions that do not have the potential to benefit to law enforcement at large beyond the piloting phase

   a. The business needs should be common to several LEAs,

   b. Software enhancement should be reversed to the LE community (licensing scheme is important)

Initiatives on which the proposals could build

1. Projects in the framework of Horizon Europe: AIDA, GRACE, INFINITY and STARLIGHT (notably),

2. Relevant networks of practitioners : **EACTDA** (Development of tools in the area of digital investigation), **ECTEG** (Development of trainings in the area of Cyber), **CYCLOPES** (Innovation / Cybercrime)

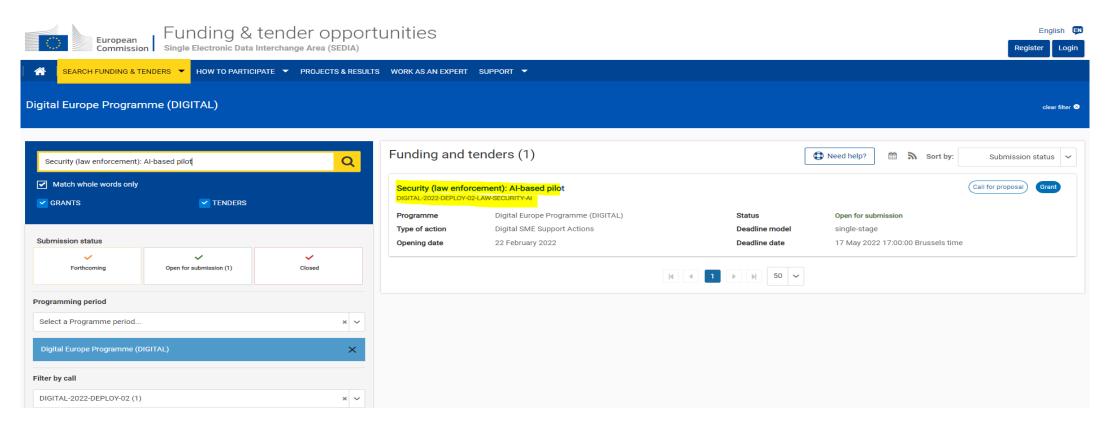3. Foresee interaction with Europol Innovation Lab and EMPACT Cyber attacks

Specific attention to:

fundamental rights challenges via:

- bias mitigation

- non-discrimination mechanisms

- measures on data quality and protection

- compliance with the EU legal framework on data processing for police purposes - Directive 2016/680 of 27/04/2016 and GDPR

Apply via [Funding & tenders](#) portal

Contact for additional information

HADEA-DEP-DIGITAL-CALLS@ec.europa.eu

Thank you