SHIELD PCP

SHIELD PCP Open Market Consultation Webinar in English

25 February 2026

SHIELD PCP

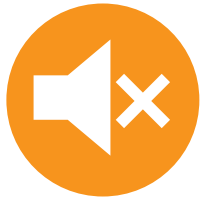
Welcome words

Etienne Genet
French Ministry of Interior

Welcome and house rules

This session is recorded, and the recordings will be shared.

The presentations will be shared.



Please stay muted unless you would like to speak regarding the topic.

Cameras are optional.

You can use the chat for questions and comments.

Funded by the European Union

Agenda

Hours	Topic	Presenter
	OMC event	
9:00 – 9:15	**Registration**	
9:15 – 9:30	**Welcome & opening remarks**	Etienne Genet *French Ministry of Interior*
9:30 – 10:00	**Explanation of the SHIELD PCP project (rationale, use cases, PCP process)**	Nina Czyżewska *Polish Platform for Homeland Security*
10:00 – 10:45	**Presentation of the state-of-the-art analysis**	Youssef Bouali *DIGINNOV*
10:45 – 11:00	**Coffee break**	
11:00 – 11:20	**OMC objectives and activities**	Azra Atalan *CORVERS*
11:20 – 12:20	**Interactive session**	Moderator: Youssef Bouali, *DIGINNOV* All participants
12:20 – 13:00	**Next steps**	Nina Czyżewska *Polish Platform for Homeland Security*
13:00 – 14:00	***Lunch break***	
	Matchmaking session	
14:00 – 14:10	**Introduction to the matchmaking session**	Nina Czyżewska *Polish Platform for Homeland Security*
14:10 – 15:10	**Presentation by suppliers of their company and capabilities**	All participants
15:10 – 16:00	**Matchmaking session**	All participants
16:00 – 16:10	**Closure**	Nina Czyżewska *Polish Platform for Homeland Security*

Funded by the European Union

SHIELD PCP

Presentation of the SHIELD PCP project (rationale, use cases, PCP process, pilots)

Nina Czyżewska
Polish Platform for Homeland Security

SHIELD PCP

Empowering Safety through Innovation

SHIELD PCP is a project funded by the European Union, which brings together first responders, public authorities, and technology providers to co-create innovative solutions for public spaces protection.

The overarching aim is to equip security stakeholders with cutting-edge technology procured through innovative processes, offering solutions that enable seamless coordination and cooperation among all stakeholders, especially law enforcement agencies (LEAs).

Using a **Pre-Commercial Procurement (PCP)** approach, the project transforms real operational needs into innovative tools that support safer, better-coordinated responses in dynamic crowd environments.

Funded by the European Union

Key facts

The primary goal of the **SHIELD PCP** is to foster innovation by empowering public buyers.

SHIELD PCP will contribute to increasing the impact of the work carried out in the EU security Research and Innovation ecosystem.

Funded by the European Union

How the project started

From SHIELD4CROWD to SHIELD PCP

SHIELD4CROWD laid the foundation for a European approach to protecting public spaces through innovation and Pre-Commercial Procurement (PCP).

By identifying common vulnerabilities, mapping technology gaps, and uniting security practitioners across Europe, the project prepared the ground for **SHIELD PCP**—turning shared needs into concrete innovation actions.

Funded by
the European Union

Challenge

Public spaces often host large, dynamic crowds—from daily urban movement to major events. Ensuring safety in such environments requires effective monitoring and assessing threats in real-time, particularly in complex and dynamic situations and facilitating real-time coordination between agencies, reliable communication systems, and accurate situational awareness.

SHIELD PCP focuses on four core capability areas:

- **Command centre coordination**
- **Secure communication**
- **Crowd monitoring**
- **Movement monitoring**

SHIELD PCP primarily addresses functionalities related to **advanced monitoring and situational awareness**, enabling the collection, aggregation and presentation of information relevant to the **understanding of evolving operational situations**.

Funded by the European Union

Command centre coordination

- Establish an integrated command centre to synthesise multi-agency information and serve as a **central hub for operational control**.
- Deliver a **real-time view** of the security environment.
- Enable **integration and fusion of data from multiple sensors**, **systems and operational inputs** to create a coherent situational picture.
- Support the **processing of diverse data types,** including video, image and other sensor-generated data within the operational environment.

Funded by the European Union

Secure communication

- Ensure **reliable and secure communication channels** to support coordinated crisis response and effective public information.
- Provide **dependable communication systems** that prevent misunderstandings and strengthen response cohesion.
- Deploy **resilient communication** tools capable of delivering rapid alerts and operational guidance to responders and the public.

Funded by the European Union

Crowd monitoring

- Enable continuous **monitoring of crowd dynamics**, particularly in high-density or fast-moving situations.
- Deploy advanced **tracking technologies** to analyse real-time data on **crowd density, movement patterns and behavioural anomalies**.
- Detect changes in crowd conditions, identify potentially **hazardous behaviour** and support timely crowd management measures to prevent escalation.

Funded by the European Union

Movement monitoring

- Enable **tracking the movement** of large groups and persons of interest.
- Deploy advanced tracking technologies to provide **real-time insight into individual and group behaviour**, even in dense crowd environments.
- Support **precise and targeted action** in response to emerging risks.

Funded by the European Union

Our Goals

Refine and validate the technological and operational **needs of security practitioners**

Build **a strong network** of public buyers and end-users across Europe

Develop, prototype, and validate **new security tools** through a phased PCP process

Ensure that all solutions respect **ethical, legal, and social standards**

Prepare a clear **pathway for market adoption**, including future large-scale procurement

Funded by the European Union

General Info

- Full name of the project:

  SECURITY HARMONIZED INNOVATION FOR ENHANCED LAW ENFORCEMENT CAPABILITIES IN DYNAMIC CROWD PROTECTION THROUGH PRE-COMMERCIAL PROCUREMENT

- Funded by: **HORIZON Europe**
- Timeline: **1 October 2025 – 30 September 2028**
- Consortium: **12 partners** from **7 Countries**
- Website: https://shieldpcp.eu/
- Project: GA N° **101225962**

Funded by the European Union

Consortium

CORVERS
COMMERCIAL & LEGAL AFFAIRS

MINISTERIO DEL INTERIOR

ISEM INSTITUTE

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Isdefe

SNCF

CIVIPOL

novadays

DigInnov

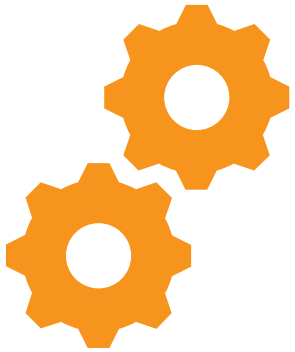
SAFE

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Polish Platform
For Homeland Security

Funded by the European Union

Expected Results



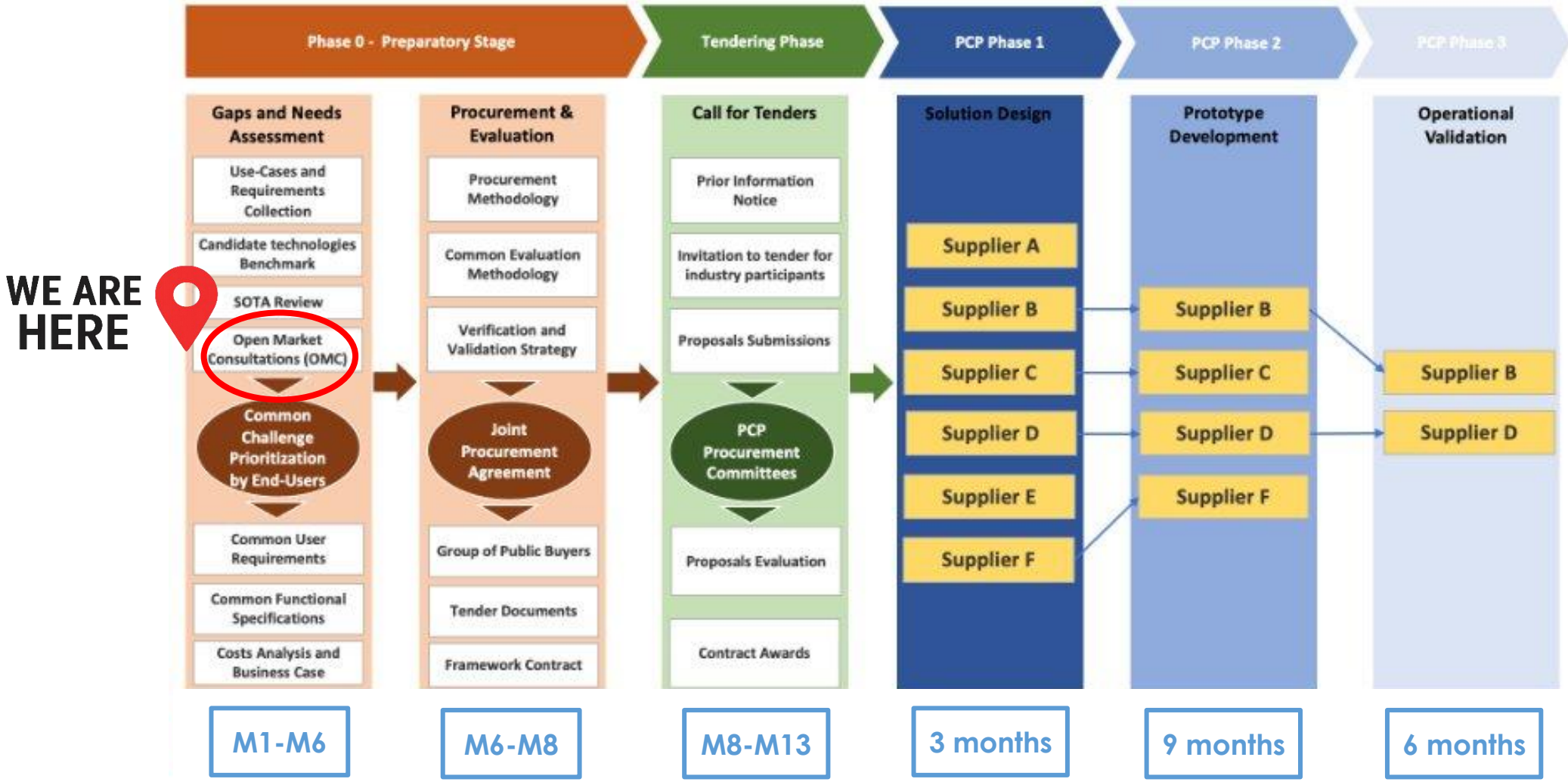
Through the **Pre-Commercial Procurement (PCP)** process, **SHIELD PCP** will develop and test **prototype solutions** in real operational environments in France, Spain, and Slovakia.

While the project will not deliver market-ready products, it will provide **tested concepts and a clear roadmap** for future large-scale deployment through **Public Procurement of Innovative Solutions (PPI)** or other funding mechanisms.

This approach strengthens cooperation, drives innovation, and improves Europe's capacity to protect public spaces.

Funded by the European Union

SHIELD PCP Innovation Procurement Phases



Funded by the European Union

PCP Development Phases

Funded by the European Union

PCP Budget Phases and Contractors

Phase 1
Solution Design

Budget: 450 000 euros
Number of contractors: at least 5

Phase 2
Prototype Development and Testing

Budget: 2 250 000 euros
Number of contractors: at least 3

Phase 3
Operational Testing in Real Environments

Budget: 900 000 euros
Number of contractors: at least 2

Funded by the European Union

SHIELD PCP

SHIELD PCP project (use cases, pilots)

Michaela Pukanová
Slovak Ministry of Interior

Pilot 1 – Panic at Football Stadium

Where / Who	• **MŠK Žilina Stadium (Slovakia) End-users: MOI, ISEMI** • **Support: State Police, FRS, Stadium Security, Municipal Police, EMS**
Main Problem	• A high-risk football match escalates into mass panic when ultras ignite smoke shells inside the stadium, causing fire, reduced visibility, blocked escape routes, and uncontrolled crowd movements.
SHIELD PCP Focus	• Improved **multi-agency coordination** (police, FRS, EMS, security). • Real-time **Common Operational Picture (COP)** shared across agencies. • Early **detection of suspicious groups, behaviours and prohibited objects.** • **Crowd movement monitoring** and congestion detection. • **Identification of perpetrators** before and during escalation.+ • Targeted **communication to spectators** to reduce panic and guide evacuation.

Funded by the European Union

Pilot 1- Requirements

- **1 CROWD SURVEILLANCE**
- **Real-time crowd density visualization:** Dynamic mapping of crowd density and movement within the stadium through an interactive heatmap.
- **Real-time visual alerts:** Instant notifications accompanied by live camera feeds in case of abnormal crowd movements or overcrowding in critical areas.
- **Access to relevant cameras:** Ability to display specific camera(s) monitoring the event, especially in high-density zones.
- **Early event indicators:** Detection of precursors to incidents (e.g., panic triggers, suspicious activities) with concise descriptions (e.g., fights, unattended bags).
- **Threat and event prioritization:** Hierarchical classification of threats and incidents for prompt operational response.
- **Evacuation and congestion alerts:** Detection and notification of evacuation movements, overcrowding zones, or blockages by analyzing movement patterns, including location, severity, timestamp, and recommended actions.

- **2. MOVEMENT MONITORING (GROUPS AND INDIVIDUALS)**
- **Real-time tracking of individuals or groups:** Visualize and monitor the movement of one or multiple persons within the stadium in real time.
- **Individual path selection:** Ability to select a specific individual to view their historical and live movement paths.

- **3. INTEGRATED COMMAND CENTER**
- **Access to a centralized operational dashboard:** A single interface consolidating real-time data, alerts, status updates, and multimodal information (text, images, video, sensor data), serving as a digital replica of the physical environment.
- **Common Operational Picture (COP):** A unified, continuously updated situational view accessible to all authorized units, providing a shared understanding of ongoing operations.
- **Geospatial visualization:** Display the positions of responders, exits, overcrowding zones, and other operational elements on an interactive geospatial map.
- **Action recommendations:** System-proposed operational actions to assist decision-making based on current events.
- **Secure stakeholder communication:** Enables coordinated, collaborative decision-making and responses during incidents.
- **Incident reporting:** Generate event reports summarizing decisions, timelines, interactions, and outcomes.
- **Comprehensive log recording:** Record all operational decisions, shared information, and executed actions for accountability and analysis.

- **4. FACILITATED AND SECURE COMMUNICATION**
- **Reliable message suggestions:** Receive predefined, trustworthy messages for public dissemination (announcements, digital screens, mobile apps) related to the ongoing incident, guiding people toward evacuation routes and exits.
- **Editable before dissemination:** Ability to modify proposed messages before sending; messages are not broadcast automatically.

Funded by the European Union

SHIELD PCP

SHIELD PCP project (use cases, pilots)

Inspector Chief Elisardo Morillo
Spanish National Police

Pilot 2 – Drone Attack Match Day

Where / Who	• **Metropolitano Stadium, Madrid (ES)** • **End-user: Policía Nacional** • **Support: LaLiga, SAMUR, 112, Local Police, Metro, EMT**
Main Problem	• A football match is disrupted by **weaponized and uncontrolled drones**, causing explosions, mass panic, and dangerous crowd surges toward exits and metro access points.
SHIELD PCP Focus	• Detection, tracking and neutralisation of **commercial and weaponized drones** • **Resilient anti-drone response** despite manipulated radio frequencies • Real-time **Common Operational Picture (COP)** across agencies • **Multi-agency coordination** via unified command and control • **Crowd surge detection and evacuation flow management** • **Secure public communication** to reduce panic and guide safe evacuation

Funded by the European Union

Pilot 2- Requirements

1. Common Operational Picture & Dashboards

- **Display of points of interest**. The system shall display Points of Interest (POIs), including responding units, personnel, equipment, suspects/perpetrators (where legally allowed) and relevant operational markers.
- **Real-time tracking on operational map**. The system shall support real-time tracking of responders, assets and identified perpetrators, displaying their movements on the operational map.
- **Centralised multi-source platform.** The system shall provide a centralised platform that aggregates multi-source data streams to deliver real-time situational awareness to authorised agencies.
- **Unified operational console for missions**. The system shall provide a unified operational console that supports joint missions by consolidating mission-specific information, tasks, resources and communication channels into a single interface.
- **Unified dashboard for joint operations**. The system shall provide a unified dashboard that supports decision-making, coordination and communication among all operational units, enabling shared situational awareness and collaborative action.
- **Dynamic synchronisation of COP data,** The system shall dynamically synchronise operational data, updates, alerts and status changes so all users see an up-to-date, consistent COP without manual refresh.
- **Alerts for evacuation/blocked flows**. The system shall detect and alert when evacuation movements, crowd congestion or blockages occur, analysing movement patterns and issuing alerts with location, severity, timestamp and recommended actions, logging all alerts and operator responses.

2. Crowd Monitoring & Analytics

- **Behavioural analytics for suspicious behaviour**. The system shall deploy AI behavioural analytics to detect suspicious objects, unusual/aggressive behaviours, panic indicators and other risk-related anomalies using existing CCTV and sensors.
- **Indoor crowd density indicators**. The system shall provide real-time indoor crowd density indicators on a map, including direction of movement, combining IoT and computer vision.
- **Capacity management via density indicators**. The system shall integrate indoor density indicators into the dashboard to manage capacity, monitor occupancy against thresholds and alert when limits are approached.
- **Anomaly detection in station/onboard cameras**. The system shall analyse video from station/onboard cameras to detect crowd anomalies and generate real-time alerts, allowing operators to select which cameras have AI detection enabled.

3. Logging, Post-incident Analysis & Evidence

- **Detailed log metadata.** The system shall record timestamps, user identity, data sources and associated system components for each log entry.
- **Secure tamper-proof log storage**. The system shall implement a secure, tamper-proof infrastructure for storing logs and generating post-incident reports, ensuring data integrity and compliant access.

4. Behavioural Threat Detection

- **Non-biometric violent/hazardous act detection.** The system shall detectindividuals/groups engaged in violent/hazardous acts using non-biometric characteristics (behaviour patterns, movement dynamics.

Pilot 2- Requirements

5. Drone & Anti-drone Management

- **Anti-drone management module.** The system shall provide a dedicated anti-drone module consolidating detection, classification, tracking, alerting and counter-drone functionalities.
- **Integration with jamming/counter-drone systems**. The system shall support integration with authorised drone-jamming and counter-drone systems, enabling lawful mitigation actions through the anti-drone module.
- **Aerial monitoring with ground fusion**. The system shall integrate drones/UAVs with ground sensors and camera networks to provide a unified, multi-layer operational picture and advanced inspection capabilities.
- **Drone trajectories vs crowd & responders**. The system shall integrate real-time drone trajectory data with crowd density maps and responder positions, display flight paths, predict impact zones and highlight abnormal trajectories near sensitive areas.

6. Architecture & Interoperability

- **Unified communication interface**. The system shall provide a unified communication interface that allows all emergency stakeholders to interact through a single secure environment supporting voice, messaging, data exchange and coordinated tasking.
- **Compatibility with national infrastructures**. The system shall ensure compatibility with existing communication systems, protocols and national infrastructures (radio networks, emergency systems, TETRA variants, LTE/5G PS networks, legacy platforms) via standards-based interfaces and configurable adapters, without replacing sovereign assets.

7. Other requirements

- **Integrated tools in coordination centre**. The system shall allow integration of coordination, communication, analytics and operational support tools within the centralised coordination centre.
- **Pseudonymised/anonymised data views.** The system shall provide simulated, pseudonymised or anonymised data representations when real operational information cannot be shared, ensuring confidentiality and realistic coordination.
- **Access control & data segregation.** The system shall enforce access control and role-based permissions ensuring strict data segregation between agencies, groups and domains, complying with confidentiality, security and data-protection regulations.
- **Real-time update latency**. The system (including COP map and all geospatial layers) shall display updated information from all integrated sources with an end-to-end latency not exceeding 2 seconds under specified conditions.
- **Message consistency & integrity.** The system shall ensure consistency and integrity of transmitted messages across all channels, preventing duplication, corruption or loss of critical information.

SHIELD PCP

SHIELD PCP project (use cases, pilots)

Celine Lor
SNCF

Pilot 3 – Multi-Actors Coordination After a Massive Knife Attack

Where / Who	• **Gare du Nord (Paris-Nord), France** • **End-users: FMI, SNCF** • **Support: Préfecture de Police (BRI, CCOS, SDRPT), Paris Fire Brigade, DNPAF, National Gendarmerie, Operation Sentinelle, SNCF & private users**
Main Problem	• **Simultaneous knife attacks** inside the station and surrounding streets cause chaos among thousands of travellers, requiring rapid understanding of the situation and coordinated multi-agency response.
SHIELD PCP Focus	• **Rapid situational understanding** through multi-source data fusion • Shared **Common Operational Picture (COP)** across police, transport and rescue services • **Multi-agency coordination** with reduced decision-making latency • **Crowd behaviour monitoring** and surge detection • **Smart evacuation flow management** inside station and public space • **Targeted communication** to travellers and staff to reduce panic and guide safe evacuation

SHIELD PCP – Requirements FRANCE

Scenario: At Gare du Nord, an individual exhibiting suspicious behaviour enters the station and moves into the dense passenger flow. Moments later, a knife attack occurs, triggering crowd movements and panic.

CROWD SURVEILLANCE

- **Real-time passenger flow visualization**
  Dynamic mapping of crowd density and movement within the station through an interactive heatmap.
- **Real-time visual alerts**
  Instant notifications accompanied by live camera feeds in case of abnormal crowd movement or overcrowding in critical areas.
- **Access to relevant cameras**
  Ability to display the specific camera(s) monitoring the event.
- **Early event indicators**
  Detection of precursors to incidents (e.g., panic triggers) with a concise description (e.g., knife attack, unattended baggage explosion, people running, etc.).
- **Threat and event prioritization**
  Hierarchical classification of threats and incidents for prompt operational response.
- **Evacuation and congestion alerts**
  Detection and notification of evacuation movements, overcrowding zones, or blockages by analysing movement patterns, including location, severity, timestamp, and recommended actions.

MOVEMENT MONITORING (GROUPS AND INDIVIDUALS)

- **Real-time tracking of individuals or groups**
  Visualize and monitor the movement of one or multiple persons within the station in real time.
- **Individual path selection**
  Ability to select a specific individual to view their historical and live movement paths.

FACILITATED AND SECURE COMMUNICATION

- **Reliable message suggestions**
  Receive predefined, trustworthy messages for public dissemination (announcements, digital screens, mobile apps, etc.) related to the ongoing incident, guiding people toward evacuation routes and exits.
- **Editable before dissemination**
  Ability to modify proposed messages before sending; messages are not broadcast automatically.

INTEGRATED COMMAND CENTER

- **Access to a centralized operational dashboard**
  A single interface consolidating real-time data, alerts, status updates, and multimodal information (text, images, video, sensor data), serving as a digital replica of the physical environment.
- **Common Operational Picture (COP)**
  A unified, continuously updated situational view accessible to all authorized units, providing a shared understanding of ongoing operations.
- **Geospatial visualization**
  Display the positions of responders, exits, overcrowding zones, and other operational elements on an interactive geospatial map.
- **Action recommendations**
  System-proposed operational actions to assist decision-making based on current events.
- **Secure stakeholder communication**
  Enables coordinated, collaborative decision-making and responses during incidents.
- **Incident reporting**
  Generate event reports summarizing decisions, timelines, interactions, and outcomes.
- **Comprehensive log recording**
  Record all operational decisions, shared information, and executed actions for accountability and analysis.

SHIELD PCP

SHIELD PCP requirements

Youssef Bouali
DIGINNOV

Requirements

Common Operational Picture & Dashboards	• A **real-time, synchronised Common Operational Picture (COP)** integrating video, sensor feeds, geolocation data, incident reports and alerts into a single geospatial interface accessible to authorised agencies. • Interactive dashboards supporting joint mission coordination, including layered visualisation (crowd, responders, infrastructure, congestion, blind spots) and mission-specific filtering. • Continuous dynamic data synchronisation ensuring all authorised stakeholders share a consistent, up-to-date operational view without manual refresh. • Decision-support overlays (risk indicators, predictive layers, KPI monitoring) to support both tactical and strategic coordination. • **Priority:** Core operational capability – predominantly Mandatory and High Priority.
Crowd Monitoring & Analytics	• AI-driven real-time analytics for detection of **abnormal crowd behaviour**, panic triggers, density anomalies and surge dynamics. • **Predictive** modelling of crowd evolution, including context-aware factors (event phases, exits, congestion patterns). • Automated alerting workflows with operator validation and confidence scoring. • Integration of indoor/outdoor density heatmaps and adaptive evacuation route optimisation. • **Priority:** Strong emphasis on Mandatory and High Priority capabilities for anomaly detection and density monitoring.
Geolocation, Tracking & Geofencing	• Unified real-time tracking of responders, assets and (where lawful) identified suspects on a shared geospatial map. • Accurate indoor positioning in multi-level venues and automatic position updates without manual reporting. • Correlation of positional data with video streams and sensor inputs. • Geofencing and restricted-area alerting mechanisms. • **Priority:** High Priority operational tracking; selected Medium elements for advanced positioning and drone tracking.

Requirements

Drone & Anti-drone Management	• Detection, classification and tracking of authorised and unauthorised drones. • Integration of aerial data with crowd maps and responder positions. • Interfaces with lawful counter-drone systems and radar feeds. • **Priority:** Primarily Medium Priority but strategically relevant for high-risk events.
Behavioural Threat Detection	• AI-based detection of coordinated hostile behaviours and non-biometric violent acts. • Identification of suspicious objects and weapon-like artefacts. • GDPR-compliant behavioural analysis avoiding prohibited biometric practices where not lawful. • **Priority:** Mandatory for non-biometric violent act detection; High Priority for advanced anomaly detection.
Logging, Post-Incident Analysis & Evidence	• Tamper-proof logging of decisions, communications and actions with full metadata traceability. • Automated post-incident reporting capabilities. • Secure storage ensuring integrity and evidentiary value. • **Priority:** Mandatory logging integrity; High Priority operational traceability.
Architecture & Interoperability	• Open, modular and interoperable architecture using standardised protocols and APIs. • Middleware for integration with legacy systems without replacing sovereign infrastructures. • Unified communication and data exchange layer. • **Priority:** Predominantly Mandatory – foundational architectural requirement.
Decision Support & AI	• AI-driven threat prioritisation and predictive scenario modelling. • Response recommendation engines with human oversight. • Continuous learning and model performance monitoring. • **Priority:** High Priority for predictive dashboards; Mandatory human authority over decisions.

Funded by the European Union

Requirements

Public Information & Alerting	Operator-approved, **multi-channel and multilingual public messaging** (PA, screens, SMS/apps, cell broadcast) with geo-targeted and accessible evacuation guidance.
Multimedia Intelligence & VMS	Secure, prioritised sharing of photos/clips/live video and **compatibility with major VMS** platforms to support operational viewing and AI-driven detection.
Multi-agency Platform & Deployment	Single interoperable platform enabling progressive onboarding, federated integration, secure real-time information exchange, and unified joint communication tools.
Command Hierarchy & Workflows	Digitised **command hierarchy** with **rule-based approvals**, structured tasking/deconfliction, and automated escalation workflows aligned with statutory decision precedence.
Data Integration & Fusion	**Real-time ingestion and fusion** of CCTV, body-worn, reports, drones, radar and environmental/behavioural sensors, plus simulation/sandbox modes with protected data views.
Access Control & Data Governance	Multi-level data-sharing controls enforcing strict segregation, role-appropriate hierarchy views, and governance-compliant access to integrated data.
Performance & Latency	Real-time updates within tight latency targets, high-throughput multimodal processing, and high-quality, usable geospatial rendering under operational stress.
Communications & Networks	Secure, redundant, anti-jamming communications with overload management, E2EE/key management, failover across heterogeneous networks, and reliable indoor/underground coverage.

Funded by the European Union

Requirements - Compliance

GDPR & Fundamental Rights Compliance	• Data protection by design and by default. • DPIA support and purpose limitation enforcement. • Safeguards for biometric and sensitive data processing.
AI Governance & Trustworthy AI	• AI risk classification, documentation and lifecycle logging. • Human oversight mechanisms and explainable outputs. • Bias monitoring, robustness testing and drift detection.
Critical Entity Resilience (CER Alignment)	• Multi-hazard resilience modelling and degraded-mode operation. • Interdependency and cascading risk visualisation. • Simulation-based preparedness and recovery coordination.

Funded by the European Union

SHIELD PCP

Presentation of the state-of-the-art analysis results

Youssef Bouali
DIGINNOV

Overview of relevant patents, standards and literature

- Establish a **targeted and up-to-date State-of-the-Art (SOTA) baseline** by systematically identifying relevant patents and standards using requirement-derived keywords and structured patent searches.
- Ensure **coverage accuracy and relevance** through iterative keyword refinement and analytical filtering of search results to avoid omissions and over-specific queries.
- Generate an evidence-based foundation to support subsequent **TRL assessment and COTS analysis.**

Methodology:

1. Based on the keywords identified from the list of requirements to deliver the existing patents & standards:
    - Define the keywords.
    - Perform the IPlytics search (standards and patents).
    - Analyze the search outcomes to identify the relevant ones.
2. Throughout the search process, the list of keywords was further refined to weed out extremely precise queries that could potentially overlook pertinent items
3. The search was limited to the years 2015 to 2025 in order to guarantee that the material included was up to date and focused on modern research and technology.

Keywords Used

1. Common operational picture
2. Multi-agency coordination
3. Real-time situational awareness
4. Public space security
5. Incident management platform
6. Emergency command center
7. Real-time geofencing
8. Tracking
9. Security operations
10. Emergency response
11. Tactical response
12. Urban drone monitoring
13. Security drone detection
14. Airspace threat assessment
15. Multimedia intelligence
16. Video analytics
17. Evidence management
18. Chain of custody
19. Real-time
20. Security incident
21. Behavioural threat detection
22. Predictive analytics
23. Public space surveillance
24. Law enforcement operations
25. Crowd behaviour analysis
26. Anomaly detection
27. Computer vision
28. Public event surveillance
29. Sensor data fusion
30. Interoperability framework
31. Heterogeneous systems
32. First responder support
33. Public safety integration
34. Command & control fusion
35. Public warning system
36. Localized alerting
37. Urban emergencies
38. Crowd evacuation

Funded by the European Union

Examples of queries used

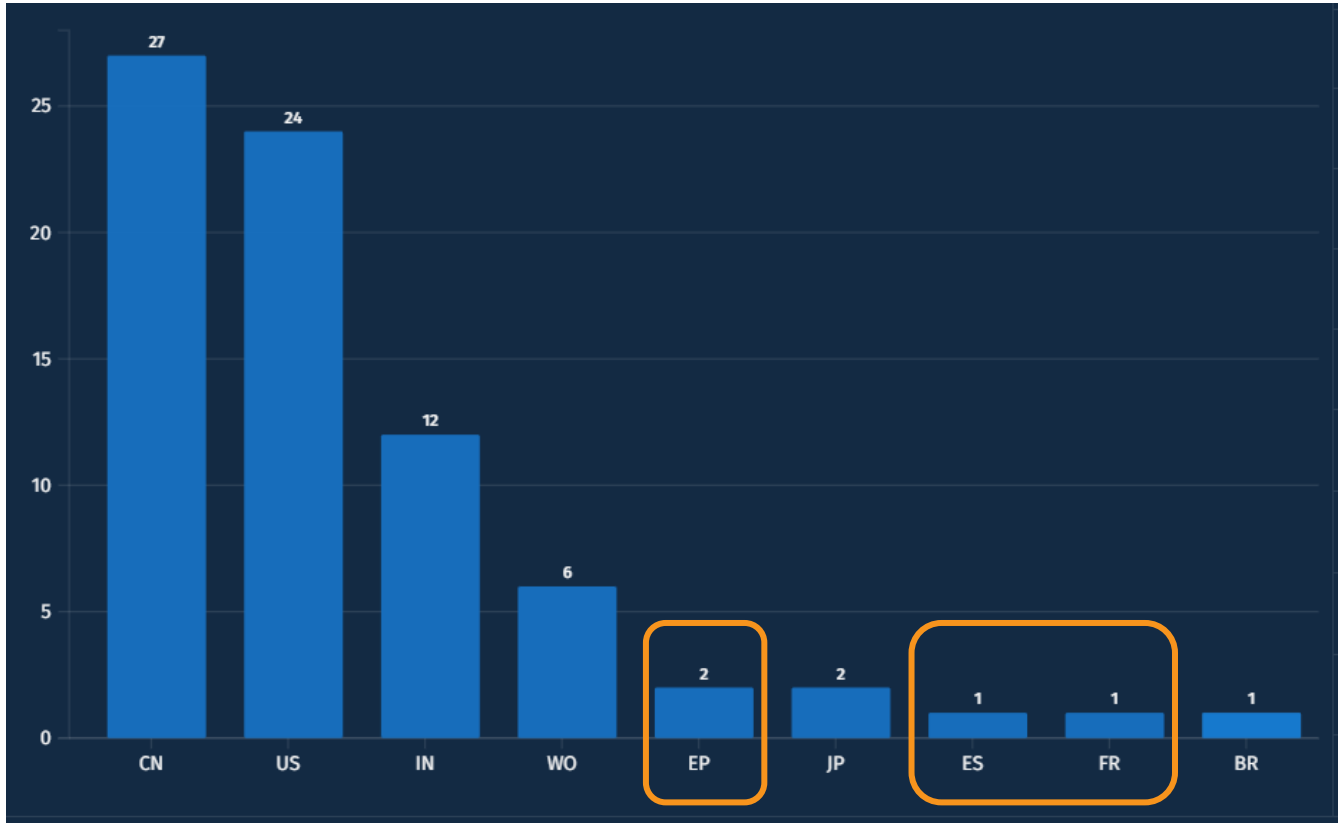
	Query	Results
1	(all:(common operational picture)) AND (all:(multi\-agency coordination)) AND (all:(real\-time situational awareness)) AND (all:(public space security)) AND (all:(incident management platform)) AND (all:(emergency command center))	305
2	(all:(real\-time geofencing)) AND (all:(tracking)) AND (all:(security operations)) AND (all:(emergency response)) AND (all:(tactical response))	156
3	(all:(urban drone monitoring)) AND (all:(security drone detection)) AND (all:(airspace threat assessment))	146
4	(all:(multimedia intelligence)) AND (all:(video analytics)) AND (all:(evidence management)) AND (all:(chain\-of\-custody)) AND (all:(real\-time)) AND (all:(security incident))	123
5	(all:(behavioural threat detection)) AND (all:(predictive analytics)) AND (all:(public space surveillance)) AND (all:(law enforcement operations))	8
6	(all:(crowd behaviour analysis)) AND (all:(anomaly detection)) AND (all:(computer vision)) AND (all:(public event surveillance))	78
7	(all:(sensor data fusion)) AND (all:(interoperability framework)) AND (all:(security operations)) AND (all:(heterogeneous systems)) AND (all:(first responder support)) AND (all:(public safety integration)) AND (all:(command \& control fusion))	372
8	(all:(public warning system)) AND (all:(localized alerting)) AND (all:(localized alerting)) AND (all:(urban emergencies)) AND (all:(crowd evacuation))	75

Funded by the European Union

Results

- We identified more than 958 patents with 76 being strongly relevant to our use case.

- From 83 patents worldwide only 4 were filled within the EU.



Funded by the European Union

Results *Strong Patent Coverage in Core Building Blocks*

AI-Based Crowd Monitoring

Advanced analytics for crowd behavior and anomaly detection

Multi-Sensor Data Fusion

Integration of heterogeneous sensor inputs for comprehensive situational awareness

Geolocation & Tracking

Real-time positioning and movement monitoring capabilities

Drone/Anti-Drone Capabilities

UAV deployment and countermeasure technologies

These components demonstrate strong maturity in analytics, sensing, and situational awareness

Funded by the European Union

Results *Critical Gaps Identified Areas with Insufficient Patent Coverage*

Shared Common Operational Pictures (COP)

Role-based visualization across multiple agencies

Command Hierarchy & Workflow Management

Cross-authority coordination and decision chains

Coordinated Decision-Making Tools

Multi-agency collaborative decision support systems

Public Information & Alerting

Integrated communication mechanisms for citizens

Interoperability & Architecture Integration

System-level integration frameworks and standards

Non-Functional Requirements

Usability, privacy-by-design, governance, deployment models

These components are essential for integrated, multi-agency operations

Funded by the European Union

Results

No single patent or existing solution covers the full range of SHIELD PCP requirements

The technology landscape is fragmented, with individual components well-developed but lacking holistic integration

Funded by the European Union

Market Overview – Top 10 Applicants (TR) - EU

Within **Europe**, **Intel** leads in patent share but records a **low TR score (7.72)**, indicating limited technical impact. Other European applicants show **very low or zero TR**, suggesting early-stage or incremental innovations with weak citation influence. Overall, the European landscape appears **concentrated and low in technical relevance**.

Ultimate Owner	Patents	Fam.	Share	MC	TR
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0
McGill University	1	1	25%	1.2	0

Ultimate Owner	Patents	Fam.	Share	MC	TR
Inspur Group	1	1	1.3%	0.24	19.12
PIERCE AEROSPACE	1	1	1.3%	2.2	18.49
CIVIL AVIATION MAN INSTITUTE OF CHINA	1	1	1.3%	0.21	13.36
INTELLISHOT HOLDINGS INC	1	1	1.3%	1.33	11.65
Intel	1	1	1.3%	1.1	11.24
Enjoyor	1	1	1.3%	0.15	11.12
QOMPLX	1	1	1.3%	20.01	10.6
Ariake Japan	1	1	1.3%	1.09	7.7
InterDigital	2	1	2.6%	1.33	7.66
GOWARE	1	1	1.3%	0.67	7.04

Technical Relevance (TR) indicates a patent's importance based on how often it is cited.

- **High TR:** Highly influential, widely cited technology.
- **Low TR:** Niche or less relevant technology, rarely cited.

Funded by the European Union

Market Overview – Top 10 Applicants (TR) - World

In contrast, the **global landscape excluding Europe** is dominated by **high-TR applicants**, led by **Inspur Group (19.12)** and **Pierce Aerospace (18.49)**. Despite holding small portfolios, these players demonstrate **strong technical influence**, highlighting a more mature and impactful innovation environment outside Europe.

Ultimate Owner	Patents	Fam.	Share	MC	TR
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0
McGill University	1	1	25%	1.2	0

Ultimate Owner	Patents	Fam.	Share	MC	TR
Inspur Group	1	1	1.3%	0.24	19.12
PIERCE AEROSPACE	1	1	1.3%	2.2	18.49
CIVIL AVIATION MAN INSTITUTE OF CHINA	1	1	1.3%	0.21	13.36
INTELLISHOT HOLDINGS INC	1	1	1.3%	1.33	11.65
Intel	1	1	1.3%	1.1	11.24
Enjoyor	1	1	1.3%	0.15	11.12
QOMPLX	1	1	1.3%	20.01	10.6
Ariake Japan	1	1	1.3%	1.09	7.7
InterDigital	2	1	2.6%	1.33	7.66
GOWARE	1	1	1.3%	0.67	7.04

Funded by the European Union

Market Overview – Top 10 Applicants (MC) - EU

Within **Europe**, patent activity is characterized by **uniformly low market coverage**, with all leading applicants showing **MC values close to or below 1**. This indicates a **limited commercial footprint**, suggesting that European filings in this space remain **early-stage or narrowly targeted**, with little evidence of broad market deployment.

Ultimate Owner	Patents	Fam.	Share	MC	TR
McGill University	1	1	25%	1.2	0
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0

Market Coverage (MC) indicates a patent's geographic scope and perceived market value.

- **High MC:** Broad international protection, high perceived global market potential.
- **Low MC:** Limited geographic protection, lower perceived international market potential.

Ultimate Owner	Patents	Fam.	Share	MC	TR
QOMPLX	1	1	1.3%	20.01	10.6
Strong Force Innovation	4	1	5.1%	19.96	4.3
Johnson Controls	1	1	1.3%	19.8	2.33
LUCOMM TECH	1	1	1.3%	18.47	4.48
LUCOMM TECH INC	1	1	1.3%	18.47	4.48
LUCOMM TECHNOLOGIES	1	1	1.3%	18.47	4.48
MOBILE MAVEN LLC	1	1	1.3%	11.26	2.92
YARDARM TECHNOLOGIES INC	3	1	3.8%	8.74	5.56
AI CONCEPTS	1	1	1.3%	5.36	0
Eaton	1	1	1.3%	2.35	0

Funded by the European Union

Market Overview – Top 10 Applicants (MC) - World

In contrast, the **global landscape excluding Europe** is led by applicants with **very high MC values**, notably **QOMPLX (20.01)**, **Strong Force Innovation (19.96)**, and **Johnson Controls (19.8)**, with several others clustered around **MC ≈ 18–11**. This indicates a **substantially broader market reach** compared to European applicants.

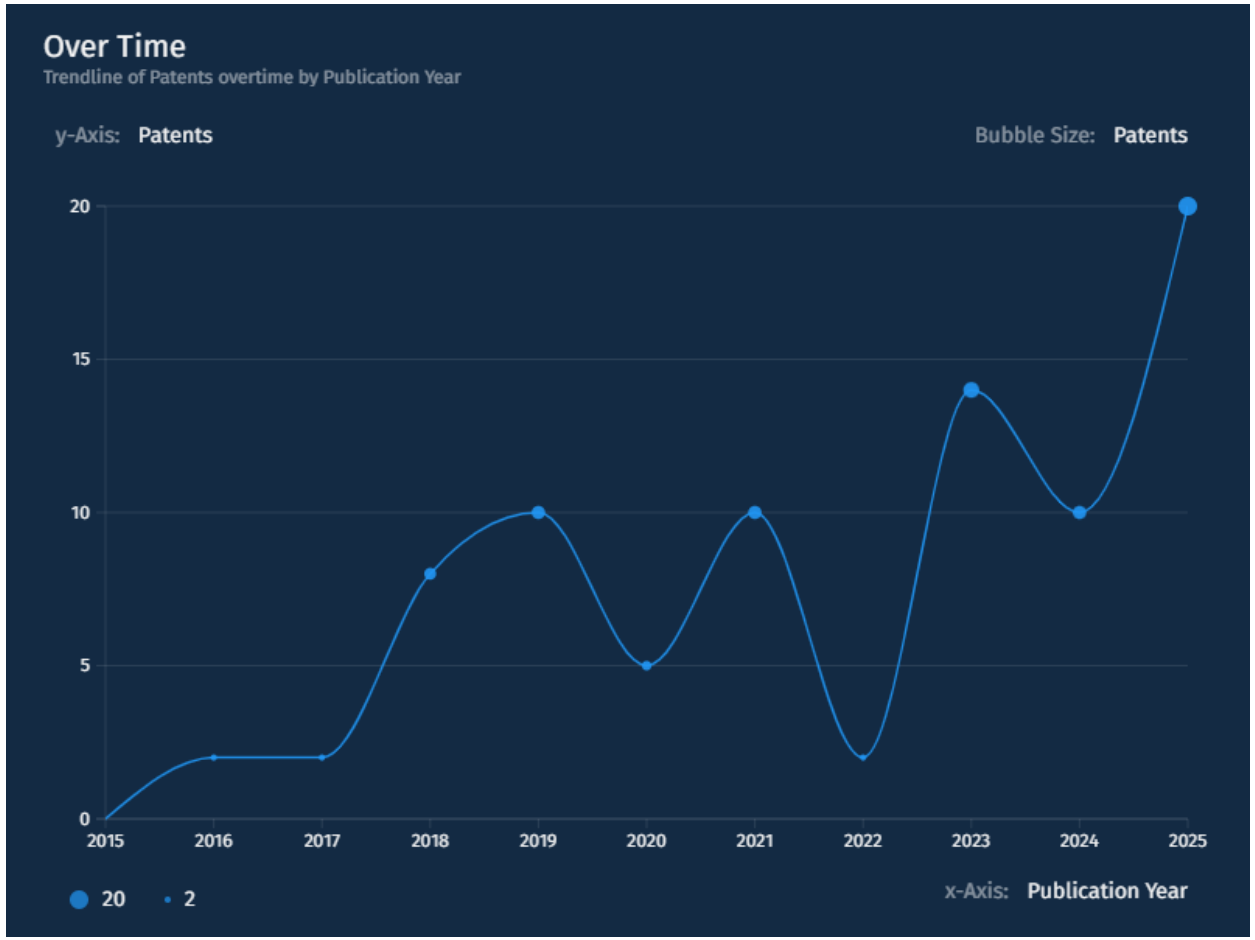
Ultimate Owner	Patents	Fam.	Share	MC	TR
McGill University	1	1	25%	1.2	0
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0

Ultimate Owner	Patents	Fam.	Share	MC	TR
QOMPLX	1	1	1.3%	20.01	10.6
Strong Force Innovation	4	1	5.1%	19.96	4.3
Johnson Controls	1	1	1.3%	19.8	2.33
LUCOMM TECH	1	1	1.3%	18.47	4.48
LUCOMM TECH INC	1	1	1.3%	18.47	4.48
LUCOMM TECHNOLOGIES	1	1	1.3%	18.47	4.48
MOBILE MAVEN LLC	1	1	1.3%	11.26	2.92
YARDARM TECHNOLOGIES INC	3	1	3.8%	8.74	5.56
AI CONCEPTS	1	1	1.3%	5.36	0
Eaton	1	1	1.3%	2.35	0

Funded by the European Union

Market Overview – Patent Pub. Over Time

Patent activity shows a **gradual increase** with intermittent fluctuations, followed by a **strong rebound from 2023 onward**. The sharp rise toward **2025** indicates **renewed innovation momentum** and growing R&D focus in this field.



Funded by the European Union

Market Overview – Geography

Patent activity is highly concentrated outside Europe, led by **China (29 patents)** and the **United States (26 patents)**, followed by **India (12 patents)**, positioning Asia and North America as the main innovation hubs.

Europe's footprint remains limited (EP: 2 patents) and 1 in Spain and 1 in France, reflecting a smaller regional presence and highlighting that, while innovation exists, it has yet to reach global scale — **pointing to an opportunity for strengthened R&D collaboration and investment within the region.**

Funded by the European Union

TRL Assessment

Objectives:

- Assess the maturity of technology domains described in EU & international patent publications.
- Identify the technology readiness baseline of underlying concepts relevant to SHIELD PCP requirements.
- Determine whether existing technological domains already cover all or only partial requirement categories.

Methodological Approach

1. **Patent Screening**
   - For each relevant patent publication identified, we selected **three (3) top related existing technologies**.
2. **Technology-Level TRL Assessment**
   - Each technology (not the patent per se) was assessed against the **TRL scale (1–9)**.
   - A **justified TRL level** was assigned based on evidence of validation, prototyping, operational testing and integration.
3. **Market & Application Mapping**
   - For each assessed technology, we identified **example applications / existing market solutions**, where available.
4. **Requirement Coverage Analysis**
   - Each technology was mapped to the **relevant SHIELD PCP requirement category**.
   - Objective: verify whether current technologies collectively cover **all, most, or only specific clusters** of SHIELD PCP requirements.

Funded by the European Union

TRL Assessment – key findings

World excluding EU

Total technology domains analysed	207
Average TRL	5
TRL 1 Basic concepts observed	0
TRL 2 Technology concept formulated	0
TRL 3 Experimental proof of concept	3
TRL 4 Technology validated in lab	55
TRL 5 Technology validated in relevant environment	75
TRL 6 Technology demonstrated in relevant environment	66
TRL 7 System prototype demonstrated in operational environment	7
TRL 8 System complete and qualified	1
TRL 9 Actual system proven in operational environment	0

EU Only

Total technology domains analysed	13
Average TRL	5 - 6
TRL 1 Basic concepts observed	0
TRL 2 Technology concept formulated	0
TRL 3 Experimental proof of concept	1
TRL 4 Technology validated in lab	2
TRL 5 Technology validated in relevant environment	3
TRL 6 Technology demonstrated in relevant environment	4
TRL 7 System prototype demonstrated in operational environment	2
TRL 8 System complete and qualified	1
TRL 9 Actual system proven in operational environment	0

Funded by the European Union

TRL Assessment - Key Takeaway

- The assessment concerns the **maturity of technological domains described in patent publications**, not the legal status or commercial exploitation of the patent itself.
- Across both datasets (World and EU-only), the **average maturity converges around TRL 5–6**, meaning most technologies are validated in laboratory or relevant environments but **not yet fully operationally qualified**.
- Globally, the landscape is characterised by:
  - Strong concentration in **TRL 4–6** (validation & demonstration stages)
  - Very limited presence at **TRL 7–8**
- The EU subset shows a **slightly stronger positioning in TRL 5–6**, but still minimal presence at higher TRLs, confirming a **systemic gap between technological demonstration and fully qualified deployment**.

Strategic Implications for PCP

The results confirm that:

- The market is **technologically active but not operationally mature**.
- There is a clear **transition gap from demonstration to qualification and large-scale deployment (TRL ≥8)**.
- Integration across SHIELD PCP requirement categories remains fragmented rather than systemic.

Funded by the European Union

Overview innovative suppliers (ongoing)

Objectives:

- Assess the availability and maturity of **Commercial-Off-The-Shelf (COTS) solutions** provided by EU technology companies.
- Identify existing market capabilities relevant to SHIELD PCP requirement categories.
- Determine maturity, integration potential, and cost implications of deployable solutions.

Methodological Approach

1. Update of Initial Cost Analysis (SHIELD4CROWD Baseline)

- Revision and refinement of previously assessed COTS and market assumptions.
- Alignment with current technological evolution.

2. Desk Research of EU Market Solutions

- Systematic identification of relevant EU-based providers and commercially available systems.
- Analysis of publicly available technical documentation and deployment evidence.

3. RFI-based Market Input (Ongoing Process)

- Direct information collected from technology providers through the **Request for Information (RFI)**.
- Validation of TRL, capabilities, integration readiness, and operational deployment claims.

Overview innovative suppliers (ongoing)

Companies analysed so far

Belgium	1
Cyprus	2
Denmark	1
France	52
Germany	2
Greece	2
Italy	4
Lithuania	1
Poland	3
Portugal	1
Slovakia	1
Spain	13
Sweden	1
Total companies	**84**

TRL breakdown of market solutions

Total COTS	**96**
TRL 1 Basic concepts observed	**0**
TRL 2 Technology concept formulated	**1**
TRL 3 Experimental proof of concept	**2**
TRL 4 Technology validated in lab	**6**
TRL 5 Technology validated in relevant environment	**8**
TRL 6 Technology demonstrated in relevant environment	**11**
TRL 7 System prototype demonstrated in operational environment	**10**
TRL 8 System complete and qualified	**19**
TRL 9 Actual system proven in operational environment	**39**

Funded by the European Union

Overview innovative suppliers - Key Takeaway

- The EU market already provides **fully deployable components and subsystems**.
- However, solutions are typically:
  - Focused on **specific capability areas** rather than holistic coverage.
  - Designed for standalone deployment, not necessarily **integrated multi-capability architectures** aligned with SHIELD PCP requirements.

Implications for SHIELD PCP

- PCP should **not replicate mature standalone solutions** already available at TRL 8–9.
- The innovation opportunity lies in:
  - **System-level integration**
  - Interoperability across capability areas
  - Operational coordination and data fusion
  - Bridging fragmented COTS into a coherent, validated ecosystem

Key Message: The EU market is technologically mature - the remaining gap is architectural, integrative, and operational rather than purely technological.

Funded by the European Union

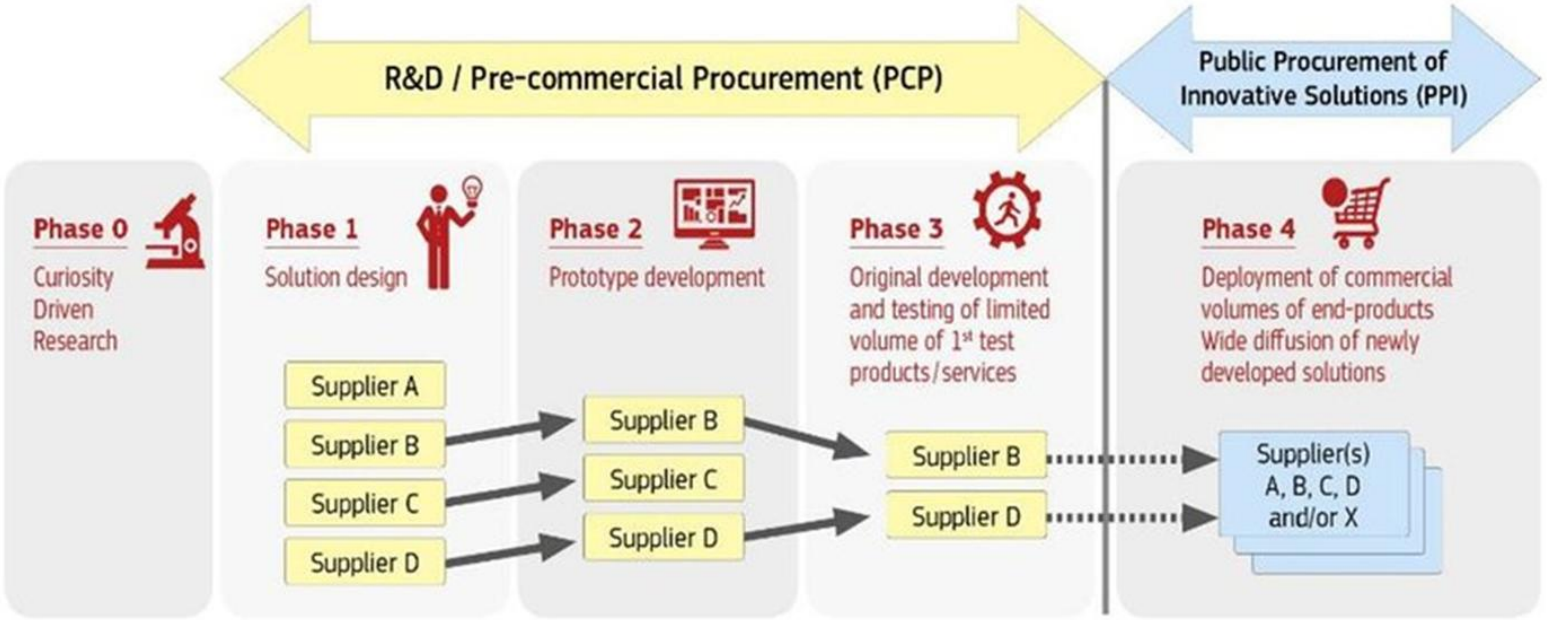
SHIELD PCP

OMC objectives and activities

Azra Atalan
Corvers Procurement Services BV

Innovation Procurement

*Innovation Procurement happens when **public buyers** acquire the **development** or **deployment of pioneering innovative solutions** to address specific **mid-to-long-term public sector needs**.*

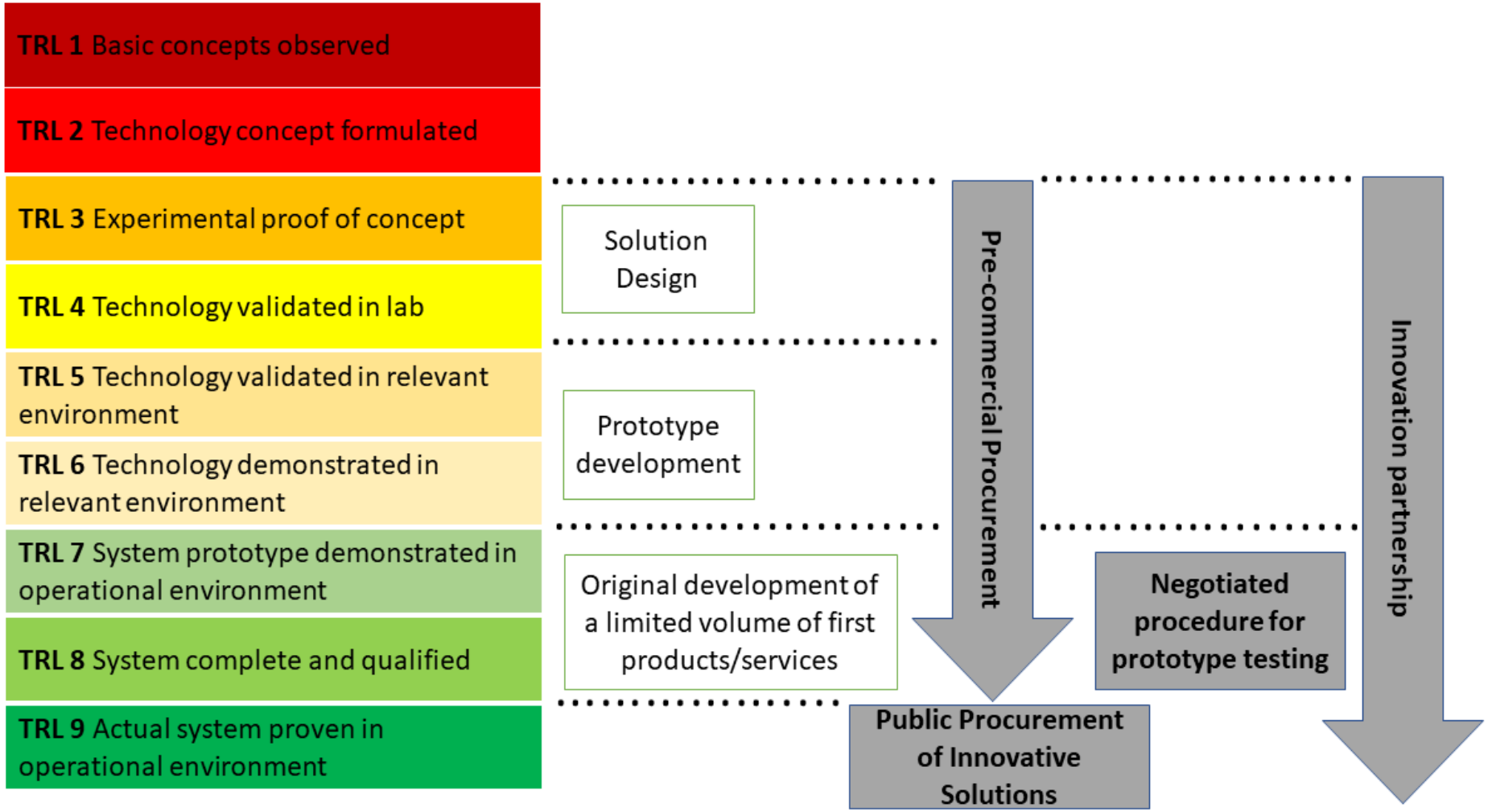


Source: European Commission, 2016

- Innovation procurement is a tool for addressing pressing societal challenges across various sectors: Health care, climate change, energy efficiency, transport, security etc.

Funded by the European Union

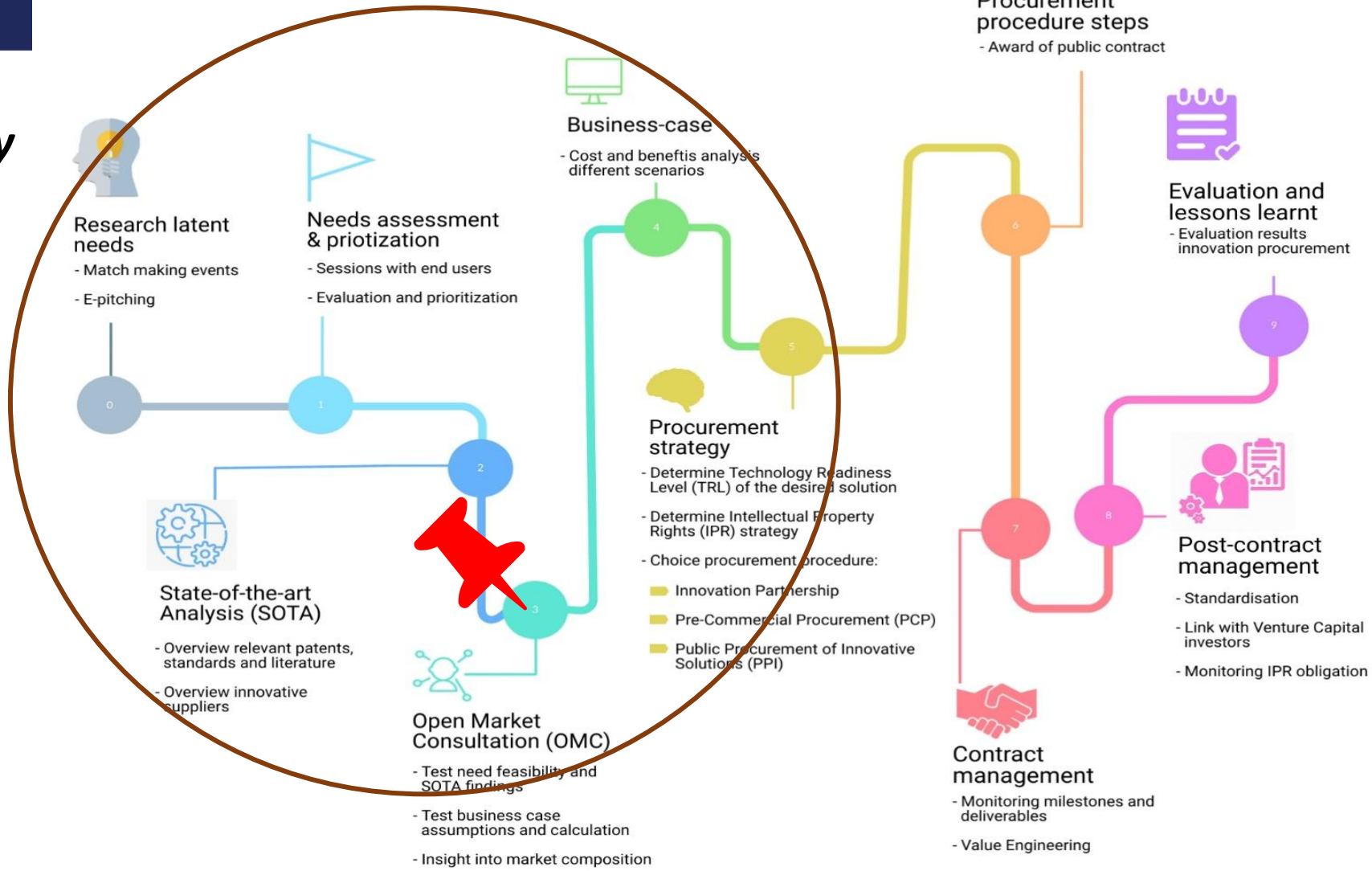
Technology Readiness Level (TRL)



Funded by the European Union

eafip methodology step-by-step

Preparatory Phase



Funded by the European Union

What is an Open Market Consultation (OMC)?

European Commission, https://projects.research-and-innovation.ec.europa.eu/en/node/11962#:~:text=An%20open%20market%20consultation%20is%20an%20open%20dialogue,to%20meet%20the%20needs%20of%20the%20procurer%20%28s%29.

Before launching a procurement procedure, **contracting authorities may conduct market consultations with a view to preparing the procurement** and informing economic operators of their procurement plans and requirements.

Contracting authorities may also seek or accept advice from independent experts or authorities or from market participants. That advice may be used in the planning and conduct of the procurement procedure, provided that such advice does not have the effect of distorting competition and does not result in a violation of the principles of non-discrimination and transparency.

In essence, an open market consultation is **an open dialogue between procurer(s) and the market**, in which the procurers ask for the view of the market to identify the ability thereof to meet the needs of the procurer(s).

Funded by the European Union

Why Conduct an Open Market Consultation (OMC)?

Market consultations bridge the gap between the supply side and the demand side.
Suppliers are informed about the needs and expectations of the procurers.
Procurers are informed about what the market has to offer, including how is the supply chain, which gives a view on European resilience and autonomy.

PROCURERS can cross-check:

- Prior-art-analysis and IPR Search
- Analysis of the Standards' landscape
- Key contractual set-up and conditions for the procurement
- Project feasibility (e.g. business case)

SUPPLIERS are informed about the public procurers' needs

Funded by the European Union

Objectives of the OMC

Validate the findings of the State-Of-The-Art (SOTA) analysis and discuss the viability of possible technical and financial provisions/ functionalities.

Raise awareness of the industry and relevant stakeholders (including other users) regarding the upcoming PCP.

Collect insights from the industry and relevant stakeholders (including users) to finetune the tender specifications.

Funded by the European Union

Why is it important to consult the market?

An open market consultation will reveal **whether the need is met by a readily available commercial solution or whether R&D (PCP) or close-to-market innovation (PPI) is needed to meet the need**.

When the solution to the need is not readily available, the open market consultation will help the public procurer to choose the right form of innovation procurement.

If R&D is still required to meet the need, a PCP is the suitable choice (potentially followed by a PPI). If there are already suitable innovative solutions close to the market that have already passed the R&D stage and are ready for commercial deployment by a launch customer, a PPI is the suitable choice.

Source: EAFIP Toolkit, Module 2, https://eafip.eu/toolkit/module-2/

Funded by the European Union

The Role of OMC

The market consultation is important in several ways:

It enables you to **cross-check** the previous market analysis (SOTA) and helps validate the innovation potential of the need.

It provides **feedback on how to raise interest from the market** to answer to the upcoming call for tender, the type of players on the market and what they can offer.

It creates **awareness** within the suppliers' market regarding the public procurers' needs.

It allows to cross-check the **feasibility and market acceptance** of the envisaged contract set-up (key contractual conditions, budget, timeframe, etc.).

Funded by the European Union

Timeline of the OMC activities

Date	Event
24 November 2025	Publication of the Prior Information Notice (PIN) on TED.
19 December 2025	Publication of the OMC documents on the project's website: www.shieldpcp.eu Publication of the EU Survey questionnaire.
27 January 2026	OMC webinar in French
27 January 2026	OMC webinar in Spanish
28 January 2026	OMC webinar in Slovak
29 January 2026	OMC webinar in Polish
29 January 2026	OMC webinar in Italian
25 February 2026	OMC event in English - Paris, France (hybrid)
12 March 2026	Deadline for the submission of answers to the questionnaire in EU Survey (17:00 CET)
19 March 2026	Publication of the OMC report
20 March 2026	Closure of the OMC

Funded by the European Union

OMC activities (milestones)

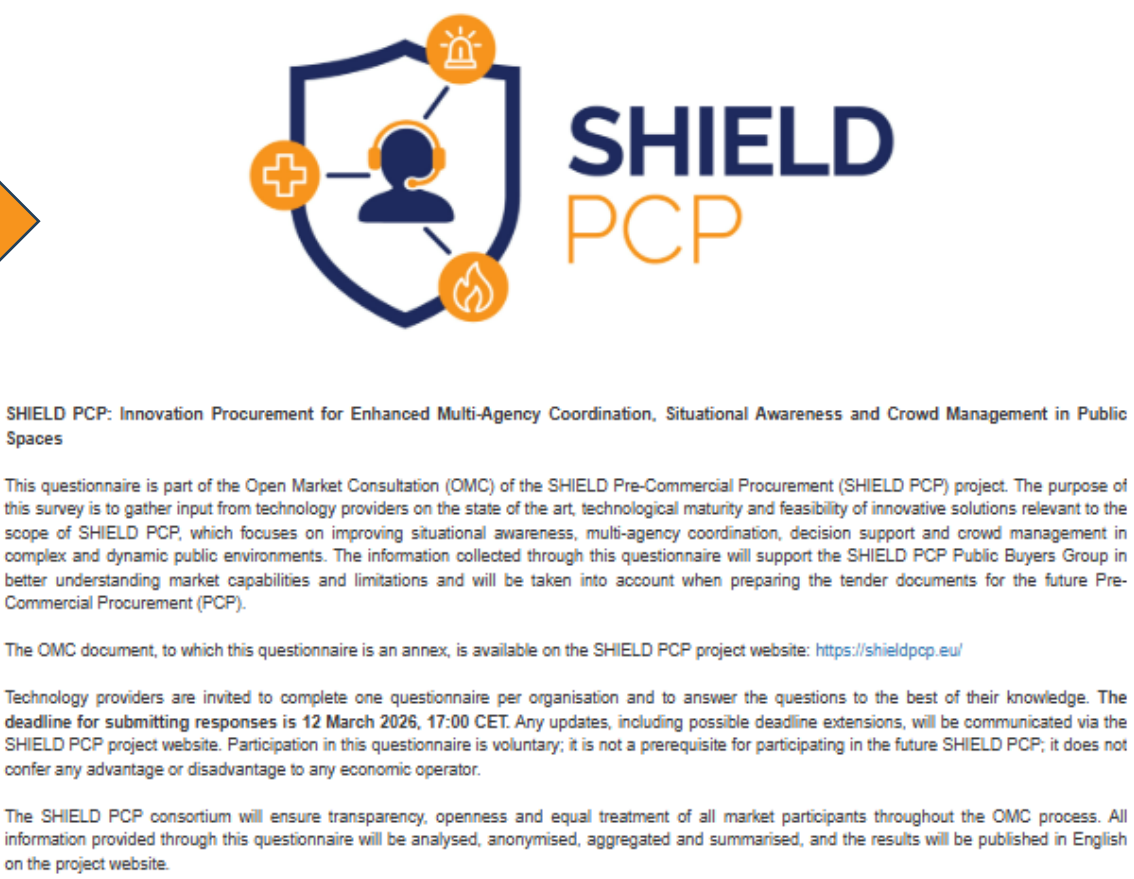
Prior Information Notice (PIN) on TED.	https://ted.europa.eu/en/notice/-/detail/824607-2025
The OMC document has been published on the project website.	SHIELD PCP - OMC Document
RFI questionnaires have been published on the EU survey platform.	https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire
The OMC webinars are planned in different languages.	
The findings (anonymised) will be published through an OMC report.	

Funded by the European Union

RFI Questionnaire

Please access the survey through this link:
https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire

The deadline for replying to the questionnaire is 12 March 2026.



SHIELD PCP
Request for Information Questionnaire

SHIELD PCP

SHIELD PCP: Innovation Procurement for Enhanced Multi-Agency Coordination, Situational Awareness and Crowd Management in Public Spaces

This questionnaire is part of the Open Market Consultation (OMC) of the SHIELD Pre-Commercial Procurement (SHIELD PCP) project. The purpose of this survey is to gather input from technology providers on the state of the art, technological maturity and feasibility of innovative solutions relevant to the scope of SHIELD PCP, which focuses on improving situational awareness, multi-agency coordination, decision support and crowd management in complex and dynamic public environments. The information collected through this questionnaire will support the SHIELD PCP Public Buyers Group in better understanding market capabilities and limitations and will be taken into account when preparing the tender documents for the future Pre-Commercial Procurement (PCP).

The OMC document, to which this questionnaire is an annex, is available on the SHIELD PCP project website: https://shieldpcp.eu/

Technology providers are invited to complete one questionnaire per organisation and to answer the questions to the best of their knowledge. **The deadline for submitting responses is 12 March 2026, 17:00 CET.** Any updates, including possible deadline extensions, will be communicated via the SHIELD PCP project website. Participation in this questionnaire is voluntary; it is not a prerequisite for participating in the future SHIELD PCP; it does not confer any advantage or disadvantage to any economic operator.

The SHIELD PCP consortium will ensure transparency, openness and equal treatment of all market participants throughout the OMC process. All information provided through this questionnaire will be analysed, anonymised, aggregated and summarised, and the results will be published in English on the project website.

Funded by the European Union

Questionnaire (Challenges and Requirements)

PCP challenge and requirements

* 1- Are you aware of any existing or emerging technologies in the field of protection of public spaces and crowd management (as described in SHIELD PCP)?
  - ○ Yes
  - ○ No

* 2- Are you currently developing or have you developed any solution relevant to any of the following use cases? *(Tick all that apply and describe briefly)*
  - ☐ Use Case 1: Panic at football stadium.
  - ☐ Use Case 2: Drone Attack Match Day.
  - ☐ Use Case 3: Multi-actors coordination after a massive knife attack in a train station.
  - ☐ No solution was developed for any of the use cases above.

* 3- Which of the following capability areas do you consider most critical to address these scenarios? *(Select up to 3 options.)*
  - ☐ Real-time common operational picture (COP) and dashboards for commanders
  - ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
  - ☐ Counter-drone detection and neutralisation systems
  - ☐ AI-supported decision-making tools for incident management
  - ☐ Inter-agency communication and coordination platform
  - ☐ Multi-source data fusion and sensor integration
  - ☐ Evacuation support and crowd routing systems
  - ☐ Public alerting and communication to citizens (e.g. emergency messaging)

4- What are the safety mechanisms and fail-safe features your solution would include to avoid collateral damage or unintended consequences?

5- Do you identify any technical, operational or organisational barriers, gaps or missing needs in relation to the scope and requirements of SHIELD PCP?
  - ○ Yes
  - ○ No

6- Can your solution be modularised or integrated with external platforms or APIs (e.g., EMS, law enforcement systems)?
  - ○ Yes
  - ○ No

7- If you were to participate in the SHIELD PCP, please indicate your indicative time allocation (in months) for each of the following phases: *(Total should not exceed 23 months.)*

	Number of months
* Phase 1: Solution Design:	
* Phase 2: Prototype Development:	
* Phase 3: Validation & Demonstration:	

* Please briefly justify your estimated time:

8- If you were to participate in the SHIELD PCP, please provide your indicative budget allocation (in EUR) per PCP phase: *(Please be aware that there is a predefined budget allocation for this PCP project, and the total available budget will be divided across phases and participating contractors. For the purpose of this question, please assume a total indicative PCP budget of EUR 3,600,000.)*

	Amount of budget
* Phase 1: Solution Design (€):	
* Phase 2: Prototype Development (€):	
* Phase 3: Validation & Demonstration (€):	

This field is required.

* Please briefly justify your estimated budget distribution:

9- Do you feel that the use cases and requirements described (spanning common operational picture, crowd monitoring, geolocation tracking, communications, etc.) cover all the critical needs of the PCP challenge? Are there any significant challenges or needs that you believe are missing from our list?

* 10- Which of the listed requirements in Annex III do you anticipate being the most technically or operationally challenging to implement, and what makes them challenging? Please highlight any requirements you see as high-risk or particularly complex.

* 11- What do you anticipate will be the main cost drivers in developing and deploying an integrated solution for these scenarios? *(Select up to 2 options.)*
  - ☐ Specialised hardware (e.g. sensors, drones, cameras)
  - ☐ Software development (analytics, AI algorithms, user interfaces)
  - ☐ System integration of components and data sources
  - ☐ Communication infrastructure (networks, devices, radios)
  - ☐ Training and change management for end-users
  - ☐ Ongoing maintenance and support of the system.
  - ☐ Other

* 12- Which approach do you believe is more effective for delivering the solution sought in this PCP? *(Select one option.)*
  - ○ A single-vendor integrated platform (one provider/consortium delivering all components as a unified system)
  - ○ A modular solution (multiple specialised components from different providers, designed to interoperate)
  - ○ No strong preference / Either approach can work

13- How important is it that the solution uses open standards and interfaces to interoperate with existing systems and third-party components?
Reset to initial position

Not important — Very important

0 (0 — 5)

14- Can you provide any other recommendations regarding the SHIELD PCP solution(s)?
  - ○ Yes
  - ○ No

RFI Questionnaire (State-of-the-art analysis)

State-of-the-art analysis

15- Do you think there is room for technological development beyond the state of the art?

- ○ Yes
- ○ No

16- What is the current Technology Readiness Level (TRL) of your solution(s) or their main components?
Please indicate the TRL for the relevant functional requirement groups described in the OMC document (Annex III), if applicable.

17- What are the main limitations of the current state of the art that your solution aims to address, and what improvements would it introduce compared to existing approaches would your solution introduce?

18- Do you rely on any patented technology or standards?

- ○ Yes
- ○ No

19- Are there existing patents or intellectual property barriers that could limit your solution's development or deployment?

- ○ Yes
- ○ No

* 20- Which of the following areas already have mature solutions available on the market (high readiness, e.g. TRL 8–9)? *(Select all that apply.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

* 20- Which of the following areas already have mature solutions available on the market (high readiness, e.g. TRL 8–9)? *(Select all that apply.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

* 21- In which areas do you see the least mature state-of-the-art, requiring the most innovation? *(Select up to 3 options that represent the biggest gaps.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

* 22- Which emerging technologies do you think could significantly enhance solutions for these scenarios? *(Select up to 3 options.)*

- ☐ Artificial Intelligence / Machine Learning
- ☐ Internet of Things (IoT) sensors and smart cameras
- ☐ 5G or advanced wireless communication networks
- ☐ Cloud computing and edge processing for real-time data
- ☐ Advanced drone technologies and robotics
- ☐ Big data analytics and predictive modelling
- ☐ Other

Funded by the European Union

RFI Questionnaire (Miscellaneous)

Miscellaneous

23- What additional information, requirements or clarifications (if any) would you need to make a well-founded plan for the development and/or deployment of a solution within SHIELD PCP

* 24- Would your organisation consider participating in the upcoming SHIELD PCP procurement (tender) as a solution provider? *(Select one.)*

- ○ Yes – we would likely participate
- ○ Maybe – we need more information/depends on conditions
- ○ No – unlikely to participate

* 25- Do you intend to participate as a single entity or as part of a consortium?

- ○ Single entity
- ○ Consortium

26- Could you please indicate the name of your proposed solution or innovation?

27- Could you please provide an image or visual representation of your proposed solution or innovation, if available?

Only files of the type png,jpg,jpeg,gif,bmp are allowed

Select file(s) to upload

* 28- Which modules or macro-functionalities does your proposed solution intend to address?

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ None

29- How would you describe your technology, and how does it relate to the SHIELD PCP requirements?

* 30- How would you describe the innovation level of your technology and its differentiation from the current state of the art? *(Please describe the innovation aspects of your solution, the state of the art in the market, and how your solution is differentiated.)*

* 31- What is the target market addressed, and who will use your technology? (*Please indicate which user groups your solution addresses.)*

- ☐ Public bodies (e.g., law enforcement agencies, civil protection authorities, cities, defence sector)
- ☐ Private-sector security operators (e.g., guarding services, event security management)
- ☐ Mixed public-private security operators (e.g., critical infrastructure operators, utilities)

Please provide additional details if needed:

32- What are the main technological, legal, ethical or operational risks and challenges associated with the development and deployment of your solution, and how could these be mitigated? *Please explain.*

33- How do you consider the interoperability of the solution?
Please describe how your solution addresses interoperability with existing systems, standards, platforms, or infrastructure.

* 34- Did you already take part in a European project, or has the development of your solution /technology been co-funded by the European Union? If so, please provide the name of the project, the Grant Agreement number and some further information.

* 35- How did you hear about the project SHIELD PCP?

- ☐ Project website (shieldpcp.eu)
- ☐ Tenders Electronic Daily (TED)
- ☐ European Commission / Horizon Europe communication channels
- ☐ Partner organisation or consortium member
- ☐ Social media (LinkedIn, X/Twitter, etc.)
- ☐ Event, workshop or webinar
- ☐ Email newsletter or mailing list
- ☐ Other (please specify)

36- Do you have any suggestions and/or remarks?

Funded by
the European Union

SHIELD PCP

Interactive session Q&A

All participants

Moderator: Youssef Bouali

Methodology

The pilots will be presented. After each pilot, participants will be invited to respond to a short set of questions via the QR.

There are additional questions regarding the main components and the market value.

The questions aim to capture how market solutions could contribute to different stages of the scenario.

Approximately **30 minutes** allocated for the questions and answers.

The results will be aggregated, anonymised, and reflected in the final OMC report.

Funded by the European Union

QR code

Funded by
the European Union

Pilot 1 - Panic at Football Stadium

Funded by the European Union

Pilot 1 – Panic at Football Stadium

Where / Who	• **MŠK Žilina Stadium (Slovakia) End-users: MOI, ISEMI** • **Support: State Police, FRS, Stadium Security, Municipal Police, EMS**
Main Problem	• A high-risk football match escalates into mass panic when ultras ignite smoke shells inside the stadium, causing fire, reduced visibility, blocked escape routes, and uncontrolled crowd movements.
SHIELD PCP Focus	• Early **detection of suspicious groups, behaviours and prohibited objects** • **Identification of perpetrators** before and during escalation • Real-time **Common Operational Picture (COP)** shared across agencies • Improved **multi-agency coordination** (police, FRS, EMS, security) • **Crowd movement monitoring** and congestion detection • Targeted **communication to spectators** to reduce panic and guide evacuation

Funded by the European Union

Questions for stadium panic scenario

Q1 – Crowd Analytics Maturity & Scalability: How mature and scalable are your real-time crowd analytics capabilities in high-density stadium environments?

A. Operationally proven in multiple large-scale stadium events (TRL 8–9).
B. Demonstrated in real operational pilots but limited large-scale validation (TRL 6–7).
C. Validated in controlled or semi-operational environments (TRL 5–6).
D. Prototype-level analytics requiring further optimisation for high-density deployment (TRL 4–5).
E. Conceptual or modular component requiring significant R&D to reach operational level (TRL ≤4).

Q2 – Integration with Existing Stadium Infrastructure: To what extent can your solution integrate with existing CCTV, VMS, PA and access-control systems at pilot sites?

A. Plug-and-play integration via standard APIs and protocols; minimal adaptation required.
B. Integration feasible with moderate configuration and middleware adjustments.
C. Integration possible but requires custom development per pilot site.
D. Requires partial infrastructure upgrades or additional hardware deployment.
E. Requires substantial infrastructure replacement or redesign.

Q3 – Real-Time Evacuation & Alert Synchronisation: Can your system dynamically calculate evacuation routes and synchronise public alerting under strict latency conditions?

A. Fully automated route optimisation and multi-channel alerting validated under real stress conditions (<2s latency).
B. Real-time route optimisation validated; alerting integration partially tested.
C. Route modelling available but requires further optimisation for real-time deployment.
D. Static or semi-dynamic evacuation planning only.
E. No integrated evacuation optimisation capability.

Funded by the European Union

Pilot 2 – Drone Attack Match Day

Funded by the European Union

Pilot 2 – Drone Attack Match Day

Where / Who	• **Metropolitano Stadium, Madrid (ES)** • **End-user: Policía Nacional** • **Support: LaLiga, SAMUR, 112, Local Police, Metro, EMT**
Main Problem	• A football match is disrupted by **weaponized and uncontrolled drones**, causing explosions, mass panic, and dangerous crowd surges toward exits and metro access points.
SHIELD PCP Focus	• Detection, tracking and neutralisation of **commercial and weaponized drones** • **Resilient anti-drone response** despite manipulated radio frequencies • Real-time **Common Operational Picture (COP)** across agencies • **Multi-agency coordination** via unified command and control • **Crowd surge detection and evacuation flow management** • **Secure public communication** to reduce panic and guide safe evacuation

Funded by the European Union

Questions for the drone attack scenario

Q1 – Drone Detection & Tracking Maturity: What is the maturity of your drone detection and trajectory tracking capabilities?

A. Operationally deployed with validated performance in urban/stadium environments (TRL 8–9).

B. Demonstrated in real operational pilots with partial urban validation (TRL 6–7).

C. Tested in controlled environments; limited field validation (TRL 5–6).

D. Early-stage prototype requiring further development (TRL 4–5).

E. Concept stage; major development required (TRL ≤4).

Q2 – Provision vs Integration of Drone Technologies (Budget & Timeline): Within PCP constraints, how would you address drone technologies for this pilot??

A. Provide complete drone detection and counter-drone solution within PCP budget and timeframe.

B. Provide detection components and integrate with existing counter-drone systems at pilot sites.

C. Integrate exclusively with existing radar/drone systems deployed locally.

D. Hybrid approach depending on pilot site maturity and available infrastructure.

E. Not feasible within PCP timeframe/budget without scope reduction.

Q3 – Air-Ground Data Fusion & Impact Prediction: Can your system fuse drone trajectory data with crowd, responder and infrastructure layers in real time?

A. Fully integrated air-ground fusion engine with predictive impact modelling validated operationally.

B. Real-time fusion possible; predictive modelling partially implemented.

C. Basic fusion capability; predictive features require further development.

D. Data visualisation only (no predictive correlation).

E. No current capability for multi-layer fusion.

Funded by the European Union

Pilot 3 – Multi-Actors Coordination After a Massive Knife Attack

Funded by the European Union

Pilot 3 – Multi-Actors Coordination After a Massive Knife Attack

Where / Who	• **Gare du Nord (Paris-Nord), France** • **End-users: FMI, SNCF** • **Support: Préfecture de Police (BRI, CCOS, SDRPT), Paris Fire Brigade, DNPAF, National Gendarmerie, Operation Sentinelle, SNCF & private**
Main Problem	• **Simultaneous knife attacks** inside the station and surrounding streets cause chaos among thousands of travellers, requiring rapid understanding of the situation and coordinated multi-agency response.
SHIELD PCP Focus	• **Rapid situational understanding** through multi-source data fusion • Shared **Common Operational Picture (COP)** across police, transport and rescue services • **Multi-agency coordination** with reduced decision-making latency • **Crowd behaviour monitoring** and surge detection • **Smart evacuation flow management** inside station and public space • **Targeted communication** to travellers and staff to reduce panic and guide safe evacuation

Questions for Multi-Actors Coordination After a Massive Knife Attack

Q1 – Multi-Agency Interoperability: How mature is your federated multi-agency integration capability?

A. Proven interoperable platform across multiple agencies and communication systems (TRL 8–9).

B. Operational pilots completed; scaling to cross-border scenarios ongoing (TRL 6–7).

C. Technically feasible but limited multi-agency validation (TRL 5–6).

D. Integration possible but requires substantial configuration per agency.

E. Requires major architectural redesign to support federated operations.

Q2 – Suspect Tracking & Behavioural Detection (Legal Compliance): What is the status of your suspect tracking and behavioural analytics capabilities under EU legal constraints?

A. Operational deployment with full GDPR/AI Act compliance documentation.

B. Deployed in pilots; compliance framework partially formalised.

C. Technically available; compliance documentation under development.

D. Requires significant adaptation to meet EU legal and ethical constraints.

E. Not currently compliant for EU deployment.

Q3 – Command Hierarchy & Decision Workflow Execution: How capable is your system in modelling and enforcing digital command hierarchies and escalation workflows?

A. Fully configurable digital hierarchy engine with automated escalation validated operationally.

B. Hierarchy modelling available; escalation partially automated.

C. Basic workflow routing; advanced automation requires development.

D. Manual workflow support only.

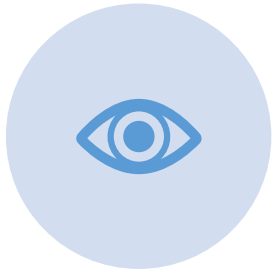
E. No structured digital hierarchy management capability.

Funded by the European Union

Main Components

COMMAND CENTRE COORDINATION

SECURE COMMUNICATION



CROWD MONITORING

MOVEMENT MONITORING

Funded by the European Union

Questions regarding the main components

Command Centre Coordination

Q1. Can your solution provide real-time multi-source data fusion (video, sensors, communication inputs) into a single operational dashboard with interoperability to existing public safety systems?

1. Yes, already operational (TRL 7–9)
2. Yes, at prototype level (TRL 5–6)
3. Partially (requires integration with third parties)
4. Not currently, but feasible within PCP timeframe
5. Not feasible within PCP timeframe

Secure Communication

Q2. Can your solution ensure secure, encrypted, and resilient communication (including in high-density environments such as stations or stadiums) while interoperating with existing public safety communication networks?

1. Fully compliant and deployable
2. Technically feasible but requires adaptation
3. Feasible only with infrastructure upgrades
4. Significant technical/legal barriers exist
5. Not within our current scope

Crowd Monitoring

Q3. Can your crowd monitoring solution detect and classify abnormal crowd behaviour in real time while complying with EU data protection regulations (e.g., no biometric identification)?

1. Yes, already compliant and validated
2. Yes, but requires further legal/ethical validation
3. Partially (limited behavioural detection capability)
4. Not currently compliant.
5. Not within our solution scope

Movement Monitoring

Q4. Can your movement monitoring technology accurately track individual and group trajectories in complex environments (indoor/outdoor) without relying on biometric identification?

1. Yes, validated in operational environments
2. Yes, tested in pilot environments
3. Technically feasible but not yet validated
4. Requires a combination with other technologies
5. Not feasible within PCP scope

Funded by the European Union

Question regarding the market value

Based on your market knowledge, what is the current market value of comparable solutions, and what is your estimated future market value of the proposed solution(s)?

Please provide a brief justification for your assessment (e.g. key assumptions, market trends, or benchmarks used).

Funded by the European Union

Q&A

Funded by
the European Union

SHIELD PCP

Conclusions and next steps

Nina Czyżewska

Polish Platform for Homeland Securit

What are the conclusions?

- SHIELD PCP aims to better understand market capabilities, maturity and innovation potential to address challenges related to multi-agency coordination, situational awareness and crowd management in public spaces.
- The Open Market Consultation is a non-binding, exploratory process designed to gather structured input from technology providers, research organisations and innovators.
- Input received through the RFI questionnaire and OMC events will help the Public Buyers Group:
  - ✓ Validate and refine functional requirements
  - ✓ Assess feasibility and technological readiness
  - ✓ Identify risks, gaps and innovation opportunities
- Participation in the OMC does not create any advantage or disadvantage for future procurement procedures.

Funded by the European Union

Next steps

RFI questionnaire remains open until **12 March 2026 (17:00 CET)**
→ All participants are encouraged to submit or finalise their responses.

The SHIELD PCP consortium will:
→ Analyse and aggregate feedback received from the market
→ Prepare and publish the **OMC Report summarising findings (March 2026)**

Outcomes of the OMC will be used to:
→ Finalise the procurement strategy.
→ Refine technical and functional requirements.
→ Prepare the future PCP tender documentation.

All updates will be communicated via the SHIELD PCP website and official channels.

Funded by the European Union

Call for Tender

Publication: May 2026

Reception of bids: June–August 2026

A sufficient period will be provided to prepare and submit proposals.

The Call for Tender will outline requirements, pilot sites, and evaluation criteria.

Evaluation will consider:

1. Technical Innovation and Feasibility
2. Cost and Value for Money
3. Operational Impact and Scalability
4. Social and Ethical Impact

Funded by the European Union

Tender Awards

Announcement: October 2026

Bids will undergo:

- Administrative eligibility checks
- Assessment against exclusion, selection, and pass/fail criteria
- Scoring of technical and financial criteria

Suppliers selected for Phase 1 will be invited to proceed.

Funded by the European Union

Thank you for your attention!

SHIELD PCP

contact@shieldpcp.eu

www.shieldpcp.eu

www.linkedin.com/company/shieldpcp

Funded by the European Union