European Defence Industrial Development Programme (EDIDP)

2019 calls for proposals, conditions for the calls and annex

based on
Regulation (EU) 2018/1092
and on
Commission implementing Decision C(2019) 2205

Version 1.0
4 April 2019

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	04.04.2019	Initial version	

Table of contents

1. Introduction

1.1. Implementation of the European Defence Industrial Development Programme (EDIDP)

The EDIDP is an industrial development programme, established by Regulation (EU) 2018/1092[1] (hereafter EDIDP Regulation), which is implemented through annual calls for proposals in 2019 and 2020. The calls are based on a two-year work programme defined in close cooperation with Member States and adopted by the Commission on 19 March 2019. The work programme contains a description of the categories and topics for which actions (development projects) will be funded through grants.

1.2. Scope and content of the document

This document contains the 2019 EDIDP calls for proposals, the conditions for the calls and an annex. It includes budgetary information, the criteria which the Commission will use to evaluate the proposals as well as other important information for applicants.

In line with the work programme, there will be nine calls for proposals in 2019, among which eight calls addressing the three priority areas defined in the EDIDP Regulation:

1. Preparation, protection, deployment and sustainability (one call);
2. Information management and superiority and command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR), cyber defence and cyber security (four calls);
3. Engagement and effectors (three calls).

An additional area for cross-domain capabilities has been added, containing one call for 2019 specifically dedicated to Small and Medium-sized Enterprises (SME) as mentioned in the EDIDP Regulation in order to encourage the participation of such enterprises and foster innovation.

The 2019 call related to *Preparation, protection, deployment and sustainability* is addressing the following category:

- Multipurpose unmanned ground system (EDIDP-MUGS-2019)

The 2019 calls related to *Information management and superiority and command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR), cyber defence and cyber security* are addressing the following categories:

[1] Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry, OJ L 200 of 7.8.2018, p. 30.

- Permanent air or space capabilities for Intelligence, Surveillance and Reconnaissance (ISR) and communication, tactical Remotely Piloted Air Systems (RPAS) and sensor suite for integration into air-traffic management (call EDIDP-ISR-2019);
- Cyber situational awareness and defence capabilities, military networks and technologies for secure communication and information sharing (call EDIDP-CSAMN-2019);
- Positioning, Navigation and Timing (PNT) and satellite communication capabilities (call EDIDP-PNTSCC-2019);
- European Command and Control (C2) system from strategic to tactical level (call EDIDP-ESC2S-2019).

The 2019 calls related to *Engagement and effectors* are addressing the following categories:

- Upgrade of current and development of next generation ground-based precision strike capabilities (call EDIDP-NGPSC-2019);
- Air combat capabilities (call EDIDP-ACC-2019);
- Future naval platforms and related technologies (call EDIDP-FNPRT-2019).

The 2019 call related to *Cross-domain capabilities* is addressing the following category:

- Innovative and future-oriented defence solutions (call EDIDP-SME-2019).

Some of the above-mentioned categories and related calls cover several topics of interest.

Important information

The detailed content of these calls is described in section 2 of this document.
The conditions related to these calls are provided in section 3 of this document and in the annex to this document.

Finally, it is reminded that a call for expression of interest to establish a list of experts to assist the Commission with tasks in connection with EDIDP has been published on DG GROW's website on 28 January 2019[2]. The Commission will select experts from this list to perform assessments of the proposals submitted by the applicants in response to the calls described hereafter in this document.

1.3. Key website

All information relating to the present calls for proposals can be accessed from the Commission's "Funding and tenders portal" website:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/edidp

1.4. Reference documents

[2] https://ec.europa.eu/growth/content/call-expression-interest-establish-list-experts-assist-european-commission-tasks-connection_en.

1.4.1. Basic texts

[Financial Regulation] - Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012[3].

[EDIDP Regulation] - Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry.

[EDIDP Work Programme] - Commission implementing Decision (C)2019 2205 on the financing of the European Defence Industrial Development Programme and the adoption of the work programme for the years 2019 and 2020.

1.4.2. Documents needed to apply

This document and its annex.
The submission form and its annexes (not available before the opening of the calls).

1.4.3. Additional documents

Guide for applicants (not available before the opening of the calls).
The model grant agreement and its annexes (not available before the opening of the calls).

[3] OJ L 193, 30.7.2018, p. 1–222.

2. Calls

The EDIDP calls for proposals for 2019 are described in this section.

2.1. Call EDIDP-MUGS-2019 – Multipurpose unmanned ground system

There are significant cooperation opportunities in Europe regarding unmanned systems, which could be based on a shared operational concept and the resulting harmonisation of requirements. Unmanned Ground Systems (UGS) can be used to cooperate with manned military vehicles and complement their capabilities (*e.g.* patrol/combat missions in urban warfare or convoys' protection in asymmetric warfare conditions, in which the UGS can act as expendable "flanker" or "fore-runner" or close fire support and check point). UGS can also replace manned military vehicles in missions which would expose the crew of manned vehicles to excessive risks (*e.g.* unmanned combat medical evacuation (MEDEVAC) in the "last mile", when the risk of mines and/or Improvised Explosive Device (IED) is too high or in areas which might be CBRN (Chemical, Biological, Radiological and Nuclear) contaminated). UGS, unmanned ground based capabilities could be complemented by static or transportable/deployable "Combat Support Point Systems" (CSPS), based on a static or transportable/deployable structure which could include:

- Sensors for surveillance and/or intelligence gathering;
- Force protection capability (by means of non-lethal armaments);
- Static or mobile/transportable Command and Control (C2).

Proposals are invited against the following topic

EDIDP-MUGS-2019: Multipurpose architecture for unmanned ground systems and solutions for systems integration and manned-unmanned teaming.

Specific challenge

European strategy and co-operation in developing autonomous land systems has to be ambitious for EU troops to effectively engage, protect, deploy, sustain and command in the future battlefield. Specific challenges include:

- The reduced acceptance of loss of human life in society leads to expectations that future conflicts must be fought using combined unmanned and autonomous systems to accomplish missions with the least possible risk to soldiers;
- Collateral damage risks increase due to population density in operational theatres and require an accurate, up-to-date common operational picture and adequate information management for precise targeting;
- New weapon systems (laser, acoustic, railguns, *etc.*) provide new opportunities, but on the other hand lead to new requirements and demands for force protection and operational security;
- Emerging technologies allow building greater overmatch distances to affect adversaries and, on the other hand, require advanced force protection measures against adversaries' assets.

There is therefore an increasing need to deploy unmanned systems to reduce the danger to civilian populations, armed forces personnel, manned platforms, as well as to increase robustness, sustainability and resilience of ground systems. The Capability Development Plan (CDP) analysis confirms this by prioritizing developing unmanned ground combat capabilities and systems with evolving levels of autonomy.

Scope

Proposals shall address design or prototyping of a system, not excluding upstream and downstream activities, which should:

- Include a system capable of manned-unmanned and unmanned-unmanned teaming with other robotic unmanned aerial and ground platforms as well as traditional manned vehicles to provide combat support and combat service support to ground forces;
- Increase situational awareness and force protection of ground units, their combat effectiveness, endurance, mobility and autonomy, and enable faster deployment;
- Have the ability to be deployed in support of dismounted troops in all types of geographic and operational environments (including denied environments) with evolving levels of autonomy and robustness for transport and supply delivery, force protection, interdiction, ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance), communication relay, military engineering support, medical evacuation or CBRN protection;
- Lower workload for UGS operator(s) through maximum use of artificial intelligence and assisted functions (*e.g.* autonomous mobility, automatic target/threat detection/tracking/prioritization), in order to assure better awareness of the tactical situation for UGS operator(s) (information superiority in a network enabled scenario);
- Include modular design and interoperability of the UGS, in order to ensure transferability of the relevant technology to other platforms (including existing manned vehicles) and simplify payload integration during the follow-up development projects.

Proposals can also include the integration of an increased number of unmanned systems (swarming) to be remotely operated by human beings.

Targeted activities

The proposals shall cover at least the design of a multipurpose unmanned ground system, not excluding upstream and downstream activities, such as feasibility study or prototyping and testing in an operational environment.

Main high-level requirements

The system shall meet the following general requirements:

- Be designed for operations encompassing the entire spectrum of conflicts from permissive to denied environments, by day, night and in adverse weather conditions;
- Provide, when necessary, in addition to functioning as part of mechanized troops, advanced mobility and a reduced footprint allowing systems to support dismounted troops in different environments, where traditional manned vehicles are not able to operate;

- Support all types of missions of infantry units without compromising their stealth and endurance;
- According to the UGS weight class, have design elements for protection which address the appropriate threats;
- Be equipped with cyber secure and Electronic Warfare (EW) resilient C2;
- Have a modular, open, scalable and cyber-secure architecture for different manned and unmanned capabilities;
- Provide a modular architecture for future upgrades and implementation of different autonomous functions;
- Be capable of manoeuvring autonomously to pre-planned battle positions and have the ability to carry at least a squad sized unit equipment;
- Have autonomous functions for unmanned ground systems' LOS (Line Of Sight) and BLOS (Beyond Line Of Sight) missions;
- Be based on a ground vehicle on which a variety of payloads can be mounted to support various mission functionalities: transport, fire-support, ISR (Intelligence, Surveillance and Reconnaissance), EW and cyber, *etc*. The sensors and communication systems of the ground vehicle shall have the capability to be integrated into broader networks;
- Ensure that autonomy related capabilities, that can cause collateral damage, are restricted to human-in-the-loop or human-on-the-loop common control in order to minimize collateral damage risks ensure operations under rules of engagements.

Budget

The Union is considering a contribution of up to EUR 30 600 000 to support proposals addressing the above-mentioned topic and its specific challenge, scope, targeted activities and main high-level requirements.

Expected impact

- Enhanced interoperability between armed forces of Member States;
- Increased situational awareness and force protection of ground units, their combat effectiveness, endurance, mobility and autonomy to enable faster deployment, and to enhance the interoperability and affordability of ground forces;
- Faster decision-making and significantly increased resilience and protection of soldiers in any environment;
- Contribution to rebuild a credible deterrent in terms of land combat capability, by introducing in the shortest time the right number of advanced logistic and combat vehicles in general as well as CSPS and introducing the unique capabilities of UGS to operate in high risk scenarios;
- Reduction, through commonality and mass production, of the acquisition and life-cycle costs for each Member State;
- Contribution to the strategic autonomy of the European Union.

2.2. Call EDIDP-ISR-2019 – Permanent air or space capabilities for Intelligence, Surveillance and Reconnaissance (ISR) and communication, tactical Remotely Piloted Air Systems (RPAS) and sensor suite for integration into air-traffic management

The lack of different airborne Intelligence, Surveillance and Reconnaissance (ISR) capabilities is assessed as critical. The Capability Development Plan (CDP) underlines the permanence of the need for tracking of ships, aircraft and other equipment through a continuous air-space wide-area via interoperable unmanned surveillance system able to operate in all weather conditions and all types of environment (including denied) and with assured data integrity. Permanent ISR and communication air and space platform, tactical Remotely Piloted Aircraft System (RPAS) and sensors should contribute to information collection and the timely delivery of the information obtained for use in the production of intelligence and situational awareness.

Proposals are invited against any of the following topics

- **EDIDP-ISR-TRPAS-2019:** Development of a low-observable tactical RPAS with the capability to provide near real time information and with modern self-protection;
- **EDIDP-ISR-DAA-2019:** European Detect and Avoid (DAA) function based on new sensors and processing for RPAS integration into air-traffic management;
- **EDIDP-ISR-EHAPS-2019:** European High Altitude Platform Station (Euro-HAPS) solution for Union defence (surveillance of maritime zones, land borders or critical assets);
- **EDIDP-ISR-PEO-2019:** Persistent earth observation from space with automated interpretation of data and information, including artificial intelligence, cloud solutions and real time on-board processing by sensors.

Budget

The Union is considering a contribution of up to EUR 43 700 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay attention to the civil and dual-use on-going initiatives at Union level to avoid any duplication (especially with Copernicus).

2.2.1. Topic EDIDP-ISR-TRPAS-2019 – Development of a low-observable tactical RPAS with the capability to provide near real time information and with modern self-protection

Specific challenge

In Europe, the lack of different airborne ISR capabilities is assessed as critical. The 2018 Capability Development Plan (CDP) underlines the permanence of the need for tracking of ships, aircraft and other equipment through a continuous air-space wide-area via interoperable unmanned surveillance system able to operate in all weather conditions and all types of environment (including denied) and with assured data integrity. Tactical RPAS systems and sensors are a key element to information collection and the timely delivery of the information obtained for use in the production of intelligence and situational awareness.

Additionally, the 2018 CDP long-term analysis indicates that Member States of the Union need the ability to create and use a real-time common operational picture, through the fusion of various types of intelligence, as a collaborative planning and task-execution tool on all unit levels, thus enhancing operational effectiveness through a unified information exchange system. The interoperability of unmanned systems (including tactical RPAS), in terms of both Command and Control (C2) data and ISR product exchange is a key enabler towards that direction.

Finally, future long-term capability requirements are projected to include systems with evolving levels of autonomy in order to improve swarming of unmanned systems in air, land or maritime domains and, among other tasks, assist in the gathering of intelligence.

Scope

Proposals shall address feasibility, detailed design and prototyping of a tactical RPAS system, capable of performing ISR missions, which includes the aircraft, ground control station and ISR product library. Several key aspects of the system need to be addressed in the proposals:

- Interoperability in terms of both C2 and ISR product exchange in near real time, always depending on the availability of a suitable communication infrastructure, since this approach will allow intelligence fusion with additional sources towards the creation of a useful Common Operational Picture (COP);
- Support for multiple versatile sensor payload configurations and suitable on-board processing capable of extracting useful information from the captured data so that a useful COP can be provided to tactical personnel in near real time;
- Low observability and/or other cost effective self-protection measures, which can maximize the survivability of the tactical RPAS system;
- Support for multiple, independent communication systems used in various configurations (redundant, parallel, roaming);
- Autonomy and swarming capabilities to improve ISR operations while maximizing the survivability of the tactical RPAS system.

Targeted activities

The proposals shall cover the initial phases of the development of the tactical RPAS including in particular:

- Feasibility study: concept of operations (CONOPS) definition, system specification, Detailed Requirements Review (DRR) and architecture definition;
- Detailed design of the system, including the Preliminary Design Review (PDR) and finishing with the Critical Design Review (CDR);
- Development of a tactical RPAS system prototype.

The proposals shall also include any partial tests in order to support decision making during the design phase and reduce the development risks.
A detailed planning of the subsequent development phases shall be generated, including the identification of implementation priorities, according to operational needs of the Union and Member States. Subsequent phases up to operational readiness shall include prototype development.

Main high-level requirements

The following general requirements shall be fulfilled:

- The system shall belong to class II (category "tactical") of STANAG 4670 and shall comply with applicable civil and/or military airworthiness requirements;
- The system shall include:
  - The airborne platform including all necessary subsystems related to navigation, communications, ISR information capture and on-board processing;
  - A Ground Control Station (GCS) with human machine interfaces for the pilot and personnel executing the ISR mission;
  - A library to store and disseminate indexed ISR products over standardized interfaces for exploitation from other entities.
- The tactical RPAS system shall demonstrate low observability;
- The system shall incorporate economically viable self-protection measures, *i.e.* the cost of these measures shall have to be justifiable when compared to the risk and cost of the loss of a system. These may include threat detection systems, Infrared/Radiofrequency (IR/RF) countermeasures (jammers, decoys, chaffs), on-board control system redundancy as well as low observability coupled with the capability to operate from a distance to potential threats;
- The system shall support suitable interoperability standards for C2 data and ISR product exchange to be ready for integration into an overall information management infrastructure so that ISR products can be discovered, disseminated and exploited by multiple consumers and to enable net-centric operations;
- The system shall incorporate support for multiple, future-proof, reconfigurable, robust and secure wideband ad-hoc long range communication systems for both C2 data and ISR product exchange, so as to maximize the probability of a reliable connection between the aircraft and the ground;
- The system shall incorporate a navigation subsystem capable of operation in a GPS[4]-degraded environment;

[4] Global Positioning System.

- The system shall support autonomy modes to fly a predefined route without intervention from the pilot and deal with degraded performance of the aircraft, communication link or navigation equipment;
- The system shall have swarming capabilities targeted at improving ISR capabilities while maximizing system survivability;
- The system shall be easily deployable and recoverable;
- The system shall support versatile sensor payload configurations including yet not limited to electro-optical and IR sensors, laser range finder, Synthetic Aperture Radar (SAR), effectors and others;
- The system shall incorporate advanced on-board payload processing so as to reduce the amount of data to be conveyed to the GCS while extracting useful information;
- Cybersecurity by design principles shall be followed to develop a system resilient to cyber attacks, which could lead to hijacking of the aircraft and ISR information leakages.

The architecture of the tactical RPAS System shall take into consideration all necessary future elements, and in particular:

- Adoption of open architecture design principles with regards to the on-board processing and flight control subsystems so as to facilitate the incorporation of new payloads and advances in standards and protocols, especially those related to interoperability;
- Integration of new developments in the area of navigation systems capable of operation in GPS-degraded and denied environments.

Expected impact

- Decrease the risk of unmanned ISR missions through the drastic increase of the tactical RPAS survivability because of the adoption of low observability features and self-protection measures;
- Decrease the reaction time and improve the situation awareness of EU forces during tactical operations due to efficient generation and dissemination of the COP in near real time;
- Facilitate the integration of ISR provided by the tactical RPAS system with other sources of Member States, EU forces, NATO and civil agencies through the reinforcement of ISR product exchange interoperability;
- Maximize the capability of the tactical RPAS system to operate efficiently because of the incorporation of technological advances in radio communications, navigation and autonomy (including swarming) as well as its ease of use.

2.2.2. Topic EDIDP-ISR-DAA-2019 – European Detect and Avoid (DAA) function based on new sensors and processing for RPAS integration into air-traffic management

The 2018 Capability Development Plan (CDP) indicates that ensuring an effective and safe access to the airspace, notably in a Single European Sky context for existing and future manned and unmanned air capabilities in order to train for, and conduct, security and defence missions in peacetime, crisis and conflict is a priority in particular to facilitate the integration of military RPAS in non-segregated airspace.
This topic aims at the design and validation of a 100% European Detect And Avoid (DAA) solution for safe insertion of large military Remotely-Piloted Air Systems (RPAS) in the European air traffic with an objective of standardisation, interoperability and certification.

Specific challenge

While unmanned air systems (RPAS) have been used to support military missions since long, these assets are still limited to operate in segregated airspace. Current operations require special provisions that severely limit the use of these assets, in particular in dense European airspace. To overcome these limitations, RPAS need to be able to integrate into non-segregated airspace, safely flying along with manned aircraft, interoperable with both military and civil Air Traffic Management (ATM) system, including interaction with Air Traffic Control (ATC) where required. This capability, often referred to as Air Traffic Insertion (ATI), is a key enabler to allow significant expansion of RPAS operations. It is particularly useful for large RPAS (MALE[5] and tactical categories) which have range and endurance performances allowing them to address a large scope of missions, including flight operations in civil airspace in Europe.
The absence of a pilot on board means that technological and procedural enablers have to be put in place to allow RPAS operating like any other airspace user. This capability, referred to as Detect And Avoid (DAA), ensures that the RPAS will be able to safely handle collision hazards with any other air vehicles in the sky. For that purpose, it relies on a combination of sensors for traffic detection, and algorithms for collision risk assessment and avoidance manoeuvre. It also provides the remote pilot with a required view of the traffic, Situation Awareness (SA), in order to keep the RPAS away from collision hazard by the appropriate separation minima (remain well clear).
European cooperation (particularly the MIDCAS [6] project) has already addressed the definition of a DAA solution and the flight evaluation of a proof-of-concept demonstrator. Furthermore, the MIDCAS Standardisation Support Phase (MIDCAS SSP) is well into standardisation of DAA by working actively in the EUROCAE[7] WG[8]-105 development of required standards (OSED[9], MASPS[10] and MOPS[11]) for DAA. However major efforts remain

[5] Medium-Altitude Long-Endurance.
[6] Mid Air Collision Avoidance System.
[7] EURopean Organisation for Civil Aviation Equipment.
[8] Working Group.
[9] Operational Services and Environment Definitions.
[10] Minimum Aviation System Performance Standards.
[11] Minimum Operational Performance Standards.

to be made to reach higher maturity levels and to design an integrated and certifiable solution. The proposals will address the main remaining technical challenges (gaps) of DAA through two main streams of effort:

- Qualify the overall performance of a DAA solution and its compliance with safety objectives, for operations in both A-C airspace classes (cooperative traffic) and D-G airspace classes (cooperative and non-cooperative traffic);
- Increase the technological maturity level of non-cooperative sensors (visible, infrared and radar) up to TRL 6 through Size Weight & Power (SWAP) optimization and improvement of data processing.

Scope

Proposals shall address the development and validation of a 100% European DAA solution, which does not contain technology subject to control or restriction by a third country or by a third-country entity (in particular free of any control regime by third countries), able to operate worldwide, in all airspace classes, compliant with applicable regulation & standards, adaptable to a variety of RPAS/drones platforms (MALE, fixed-wing tactical RPAS, vertical take-off and landing RPAS), leveraging on available European background. The proposals should also cover the activities needed to increase the maturity level of non-cooperative sensors (*i.e.* visible, infrared and radar) through SWAP optimisation and improved robustness of data processing.

The proposals will address two main applications:

- IFR[12] flight operations insertion of RPAS in controlled airspace (A to C) with an initial emphasis on MALE;
- IFR flight operations in uncontrolled airspace classes (D to G) for application to large tactical RPAS.

With the above, the proposals shall provide operational capability supporting initial (IOC) integration of RPAS in the European (A-C) airspace using cooperative DAA, as well as taking necessary steps towards full integration in all airspace classes (A-G). These activities will be fully aligned with the RPAS 1 and RPAS 2 steps of the EU RPAS roadmap as well as the SESAR[13] European ATM master plan.

The proposals shall foresee a maximum reuse of building blocks and technologies already developed under European cooperation.

The proposals should also fully support the ongoing standardisation and regulatory work within EUROCAE WG-105, EASA[14], JARUS[15] and ICAO[16], as well as SESAR2020 and other relevant European programs (including EDA[17]-coordination DAA programs MIDCAS and MIDCAS-SSP).

[12] Instrument Flight Rules.
[13] Single European Sky ATM Research.
[14] European Aviation Safety Agency.
[15] Joint Authorities for Rulemaking on Unmanned Systems.
[16] International Civil Aviation Organisation.
[17] European Defence Agency.

The proposals should not address the insertion of small drones in the so-called U-Space and the operations in Very-Low Level airspace (VLL) but should consider the interoperability with U-space.

Targeted activities

The proposals shall cover the necessary activities for the design, and where required prototyping, testing and qualification, of a European DAA solution applicable to military RPAS and to various types of platforms (MALE, fixed-wing tactical and vertical take-off and landing RPAS).

The proposals shall cover at least the design activities (and possibly upstream and downstream activities) from the following overall programme of work:

- Design improvements of the detect function: sensors miniaturization (SWAP), robustness of sensor processing and fusion algorithms, adaptation to European platforms and related concept of operations;
- Design, prototyping and extensive testing of two DAA solutions:
    - For operations in A-C airspace classes (cooperative);
    - For operations in D-G airspace classes (non-cooperative).
- Design, testing and qualification (through extensive simulation) of a Collision Avoidance (CA) function according to European reference scenarios;
- Formal validation of safety case through extensive qualifying simulation programme using reference scenarios, models and conditions provided by Eurocontrol or Air Navigation Service Providers (ANSPs), completed by flight tests;
- Design and testing of a Remain Well Clear (RWC) function;
- Implementation and flight testing of a TRL 6/7 demonstrator.

The proposals shall cover a view of the complete programme of work up to the operational system with a detailed description of the remaining work to be performed.

Main high-level requirements

The system shall fulfil the following general requirements:

- Support safe integration of RPAS into controlled and uncontrolled airspaces, by assuring SA, RWC and CA functionalities with the applicable target level of safety for both cooperative and non-cooperative traffic;
- Enable RPAS operating IFR and Beyond Radio Line-of-Sight (BRLOS) with all capabilities needed for operation in all airspace classes;
- Embed cooperative (*e.g.* ADS-B [18] receiver or Bearing-less Active Surveillance (BLAS)) and non-cooperative sensors (visible, infrared and radar);
- Embed miniaturized non-cooperative sensors (visible, infrared and radar) allowing their integration in tactical RPAS. The sensors shall be compatible or compliant with draft MOPS RADAR (RTCA[19] and EUROCAE) and draft MOPS EO/IR[20] (RTCA and EUROCAE);

[18] Automatic Dependent Surveillance – Broadcast.
[19] Radio Technical Commission for Aeronautics.
[20] Electro-optical/Infrared.

- Embed automatic traffic detection using a combination of cooperative and non-cooperative sensors;
- Support integration of external systems data/information on fixed obstacles, weather hazards and no-fly zones;
- Be able to fulfil civil and military requirements for different categories of RPAS with initial focus on MALE and tactical systems;
- Be integrable (minimizing the customization process) in different categories of RPAS with initial emphasis on MALE and tactical UAS[21] (fixed-wing and vertical take-off and landing RPAS);
- Be in line with evolving European standards and regulatory framework as well as the future European ATM, as defined by SESAR;
- Comply with European R&D activities on RPAS Integration, *i.e.* SESAR OSED/SPR[22]/INTEROP documents on RPAS IFR integration (SESAR2020 PJ10.05 and Wave 2 developments when available);
- Comply with EUROCAE DAA OSED and draft DAA MASPS standards;
- Comply with risk-ratio defined in the DAA performance metrics defined by ICAO;
- Be interoperable with existing and future collision avoidance systems (TCAS[23], ACAS[24]-X, ACAS-Xu), by meeting interoperability standards for CA;
- Perform its intended functions in en-route and TMA[25] phases at any height above ground (take-off, landing and ground operations are not considered);
- Have system performances validated with European air traffic models and parameters.

Pure ground based DAA system is not considered feasible for long term evolution of the functionality, and therefore not recommended.

Expected impact

- Operational impact:
  - Provide military users with a flexible and safe use of RPAS everywhere, in all airspace classes and anytime;
  - Allow extension of military RPAS operations in European airspace for training purpose and security missions (border/maritime surveillance, law enforcement, homeland security, protection of major events…).
- Strategic impact and operational sovereignty:
  - To contribute to the Union strategic autonomy in particular through independence to operate military RPAS in worldwide operation;
  - Ensure the DAA solution does not contain technology subject to control or restriction by a third country or by a third-country entity, directly, or indirectly through one or more intermediate undertakings.
- Industrial impact: ensure European industrial capability and competiveness in a key technology area for RPAS/UAS and autonomous systems (military and civil);

[21] Unmanned Air Systems.
[22] Safety and Performance Requirements.
[23] Traffic Alert and Collision Avoidance System.
[24] Airborne Collision Avoidance System.
[25] Terminal Control Area.

- Programmatic impact:
    - Support European RPAS programs with DAA capability (such as but not limited to European MALE RPAS and on-going national tactical RPAS programmes);
    - Support implementation of the European ATM and drones/RPAS roadmaps, 2018 EU CDP;
    - Comply with and support SESAR2020, European standards (EUROCAE), European regulation (EASA), international standards (ICAO, JARUS).

2.2.3. Topic EDIDP-ISR-EHAPS-2019 – European High Altitude Platform Station (Euro-HAPS) solution for Union defence (surveillance of maritime zones, land borders or critical assets)

Surveillance of maritime zones, land borders or critical assets is key for European operations. Various solutions are currently used to perform the surveillance of maritime zones, land borders or critical assets, but no proper solution has been found at this time:

- Current observation satellites provide daily revisit frequency, upcoming constellations of small satellites will certainly propose a revisit time within the hour. However, this will still be too high to properly understand the behaviour of a terrestrial target, and to track it;
- Large Unmanned Air Vehicles (UAV) can provide permanence over an area but with a limited duration and a very high cost. No predictable near-future evolution is anticipated.

Recent advances in technology developments pushed by industry initiatives can be a solution to this issue. Since the 90's, international initiatives have been devoted to the application potentialities of the High Altitude Platform Stations (HAPS). With respect to terrestrial and satellite networks, technical advantages provided by HAPS are many, among which:

- Better propagation conditions for connectivity, lower latency, better image resolution;
- Ability to remain continuously and persistently on an area for a long period.

Specific challenge

HAPS, operating in the stratosphere, can provide an efficient solution to European defence forces, featuring simultaneously a capacity of permanence and endurance over a large area. HAPS can complement the terrestrial and satellite systems for the surveillance and monitoring services, *e.g.* keeping a stationary position (at a first approximation) with respect to the ground and thus acting like a fixed observation platform. They can be used to cover environmental "hotspots" providing almost continuous observations, with high spatial resolution, low costs and long duration, equipped with on-board visible, infrared, SAR[26] sensors. They can also be equipped to receive AIS[27] data and be used as relay for coast-ship communications, as well as broadband communication media for RPAS.

Main HAPS applications are:

- Surveillance missions, using radar, optical and Signal intelligence sensors;
- Accurate urban surveillance missions, especially in situations that require detailed mapping of impact on high value assets or frequent revisits;
- Telecommunication missions, embarking a powerful telecommunication relay.

The development of HAPS solutions necessitates solving specific technological, industrial and operational challenges:

[26] Synthetic Aperture Radar.
[27] Automatic Identification System.

- Maturity of the key technologies required to develop such platforms;
- Adaptation of the sensors and payloads to the stratosphere environment and high altitude position;
- Self-protection of the platform (and ground stations) to the electromagnetic/cyber threats;
- Industrial capacity and means to manufacture and integrate such large vehicles;
- Simple and autonomous command/control for low cost flight operations;
- Real time processing of the very large data flow, to derive actionable information for location based intelligence purposes, exploiting innovative artificial intelligence techniques and fusing data provided by HAPS with other multi-source and heterogeneous earth observation satellites and non earth observation data;
- Development of the concept of operation of such innovative assets, with specific operational capacities, together with operational and environmental constraints.

Scope

The proposed action should contribute to design, develop, manufacture and validate a HAPS solution and as such make a substantial contribution to European defence and security applications.

Benefiting from improvements in composite materials, low-power computing, battery technology and solar panels technologies, HAPS development projects lead by industry have recently reached more advanced stages of development, in particular in Europe.

The proposals will include:

- Definition of the Concept of Operations (CONOPS) of HAPS solutions in their various missions, taking into account their specific operational capacities, together with operational and environmental constraints. Such CONOPS will be used to derive the scenarios to be executed by the demonstrator to demonstrate operational capacities for the European forces;
- Study of the current and foreseen technology status and identification of the road maps for each product involved. A definition of the demonstrator vehicle and mission chains should then be derived from such road maps;
- Design, development, qualification, manufacturing and industrialization of the HAPS platform demonstrator (including command/control ground segment);
- Design, development, qualification and manufacturing/procurement of the missions chains, its ground segment and payloads used for the demonstration, derived from existing products used on other systems;
- Design and development of HAPS mission data value added exploitation platform and service architecture according to the defined CONOPS;
- Design of maintenance program and logistic support;
- Certification activities;
- Execution of operational scenarios to validate the CONOPS and demonstrate the operational capabilities for the benefit of the European forces definition of future applications and services.

Targeted activities

The proposals shall cover the initial phases of the development of the platform and associated surveillance mission systems including in particular:

- Feasibility study, CONOPS definition, system specification, Detailed Requirements Review (DRR) and architecture definition;
- Detailed design of the system, including the Preliminary Design Review (PDR) and finishing with the Critical Design Review (CDR).

The proposals shall also include the development of technological demonstrators, in order to support decision making during the design phase.

A detailed planning of the subsequent development phases shall be generated, including the identification of implementation priorities, according to operational needs of the Union and Member States. Subsequent phases up to operational readiness shall include in particular prototype development, qualification and test activities, following a spiral approach, to reach incremental operational capabilities.

Main high-level requirements

Defence forces are looking for:

- High altitude of operation (typically 20 000 m);
- Permanence, necessary to detect critical threats;
- Endurance with an objective to stay in flight for one year. Ability to support operations without limitation during all its duration shall be investigated;
- No ground logistical impact on the operational theatre;
- A large payload capacity of several hundred kilograms and several thousand watts, that can embark large scope and long range sensors, such as powerful radars, optical or signal intelligence sensors, necessary for surveillance missions (terrestrial or maritime);
- Capacity to be repositioned or projected over foreign theatres;
- Long distance detection (typically 200 km), from a unique platform with optimized sensors:
    - Large radar coverage using a powerful radar;
    - Powerful optical (visible and infrared and/or hyperspectral) instrument;
    - Signal intelligence sensors.
- Applications for maritime and land (border) surveillance (air and sea);
- Applications for monitoring of migratory routes and flows in transit countries or at the EU external border;
- Applications for communication and electronic intelligence;
- Detection of objects usually hidden to low flying aircrafts or UAVs by mountains or buildings;
- Telecommunication applications, embarking a powerful telecommunication relay (as an option);
- Capacity to embark diverse payloads and sensors, according to the mission and to the user requirements, thanks to a modular design and a standardized interface (“plug and play”). Each Member State can define its own payload, based on its own sensors. This

capacity will be demonstrated by swapping payloads for diverse purposes and diverse origins;
- Ability to work as GNSS-pseudolite (Global Navigation Satellite System) shall be investigated;
- Ability to transfer imagery to reach back centres like processing, exploitation and dissemination cells, potentially with the help of artificial intelligence shall be investigated;
- Ability to be easily integrated in C2 systems;
- Electromagnetic and cyber resilient platform and payloads.

Expected impact

- Support of European critical defence and security solutions, through the development of innovative solutions in the domain of HAPS;
- Ensure secure and autonomous availability of high performance and trustable (re)configurable solution to military end-users;
- Contribute to strengthening the competitiveness of the Union industry and help improve its global position through the development of innovative technologies along a new European manufacturing value chain;
- Improve competitiveness of the European industry in and beyond the defence and security sector.

2.2.4. Topic EDIDP-ISR-PEO-2019 – Persistent earth observation from space with automated interpretation of data and information, including artificial intelligence, cloud solutions and real time on-board processing by sensors

The role of Earth observation (EO) and geo information within defence, security and intelligence operations is increasing both from a strategic and tactical point of view. High resolution EO data are undergoing an explosive growth, increasing complexity, like the diversity and higher dimensionality characteristic of the data. EO data are regarded as "big data" and their management requires techniques to solve data-intensive problems. Artificial Intelligence (AI) is key to cope with this challenge.

Specific challenge

The huge amount of available data sources requires new methodologies to assist the intelligence community streamline their processing and exploitation. The Activity Based Intelligence (ABI) complements the geo spatial activities by rapidly integrating data from multiple sources to discover relevant patterns, determine and identify changes, and characterize those patterns to drive collection and create decision advantage.

The challenge is to define and test a prototype of a system that implements the concept of ABI which is able, in particular, to:

- Extract entities (*e.g.* events, changes, features) from different data sources in an automated way;
- Derive insights from the aggregation, correlation and monitoring of such entities in terms of patterns and anomalies.

The challenge is then to provide the ABI system as a new means for ISR (Intelligence, Surveillance and Reconnaissance) to fulfil the command and control needs. This would be achieved by providing tools to analyse in an interactive way the ABI information linked to contextual intelligence information.

Scope

The already introduced ABI represents a new analysis methodology focused on the "time dimension" and aimed at discovering relevant patterns, detecting and characterising changes, analysing a target's behaviour and highlighting anomalies. Detected patterns feed a never-ending observation cycle by driving new collections and generating decision advantage.

Consequently, AI has evolved dramatically over the last years especially with the emergence of deep learning techniques. These techniques rely on the traditional neural network approach and, by exploiting hardware evolution (graphics processing unit availability and cloud), are able to reach unmatched accuracies in the traditional machine learning tasks, such as classification, detection, segmentation, *etc*. Deep learning is applicable to all the different data analysis needs of ABI, relevant to both EO data (Very High Resolution satellites (VHR), Synthetic Aperture Radar (SAR) satellites, constellation of micro-satellites, *etc*.) and un-conventional data sources (social network data, news feeds data, *etc*.).

The scope of this new system is to support the automated information extraction by applying AI techniques whenever possible and in particular for the extraction of entities such as:

- Events, extracted from news feeds and social networks using natural language processing and image analysis with deep learning techniques;
- Changes and features from satellite imagery "time series" using deep learning techniques such as CNN (Convolutional Neural Network).

After the extraction of information from heterogeneous sources, ABI includes the ability to aggregate entities and fuse them using spatio-temporal analysis (*e.g.* density maps of events over time) in order to create insights on different phenomena.

Targeted activities

The proposals shall cover the development of a prototype that implements the concepts of ABI and that includes in particular:

- Analysis of automated methods for entity extraction from EO and non-EO data;
- Design of the prototype system including the Preliminary Design Review (PDR) and the Critical Design Review (CDR);
- Development and demonstration of the prototype.

Main high-level requirements

The proposals shall fulfil the following general requirements:

- State-of-the-art for automated multi-SAR/optical and multi-platform data interpretation focused on time series analysis for ABI;
- Analysis of existing satellite missions to be exploited and fused for ABI tasks and definition of mission requirements to fill gaps in data availability;
- Support to the geospatial intelligence (GEOINT) analyst in the definition of the most suitable satellite and non-satellite data planning and data collection strategy to carry out ABI tasks. As an example, regarding the different sensor types, it is important to underline that:
    - SAR missions offer a primary source of information thanks to their reliability (no clouds or atmospheric effects), geo-location accuracy and capability to detect changes;
    - VHR optical missions and, above all, new missions based on constellations, offer the capability to classify and recognize targets with unprecedented revisit time;
    - MWIR (Medium Wave Infrared), TIR (Thermal Infrared) future missions are able to detect parameters such as heat as an indicator of activity over specific targets.
- Exploitation of innovative AI tools and methodologies (machine learning/deep learning) to support the extraction of relevant information and behaviour from large quantities of unstructured data;
- Extraction of motion information as a powerful activity indicator and for pattern-of-life analysis by exploiting:

  - The capabilities of SAR sensors to highlight moving targets and therefore provide information about "instantaneous activity" over a target area;
  - The capabilities of new missions to provide high definition videos, taken from space, lasting tens of seconds.
- Implementation of functionalities for entity extraction applicable to EO data based on deep learning techniques in order to detect changes and recognize entities;
- Implementation of functionalities for entity extraction applicable to non-EO data to overcome the limitation of data sources like social network and news feeds (*e.g.* data bias, geo-referencing, multi-language);
- Integration of multiple sources of information to derive insights, including remote sensing (satellite and airborne), local sensors and open source information such as social network data, properly organized, interpreted and analysed;
- Specification and implementation of unconventional data analysis methods on existing data. An example is the use of SAR images to detect and characterise signal from ground-based radars or other electromagnetic devices (interference analysis);
- Use of large-scale (both space and time wise) data filtering and analysis in order to develop an understanding by correlating heterogeneous data sets;
- Provision of specific workflow for ABI tasks for maritime and land application in order to support the GEOINT analysts work;
- Development of the system in a modular and expandable way to incorporate new data streams, new analysis methodologies and operational procedures.

Expected impact

- Enable the application of ABI for large scale, highly automated analysis of multi-source EO (including high revisit and/or high resolution constellations) and non-EO data;
- Use innovative and scalable methodologies to discover location based behaviours and activities relevant for intelligence purposes, taking advantage of the recent technological developments in EO, AI and ICT (Information and Communication Technologies) infrastructures for big data management;
- Enhance the European industry's capabilities and competiveness to provide operational ABI services exploiting state-of-the-art EO and non-EO data, platforms and methodologies;
- Foster the debate inside the user community about the requirements and challenges of ABI approach for GEOINT applications including, but not limited to, data sources availability and accessibility, data management tools, analysis methodologies, information confidentiality;
- Establish a proof-of-concept or a prototype, which can act as reference for the independent user assessment, in light of product extensions and service improvements and for the further technological developments;
- Provide tools and best practices for the operational application of ABI principles within the intelligence user community;

- Reduce operator workload for data preparation and information extraction in order to concentrate effort on GEOINT contextual analysis;
- Improve reaction time for decision making by leveraging continuous data streaming analysis;
- Implement information superiority.

2.3. Call EDIDP-CSAMN-2019 – Cyber situational awareness and defence capabilities, military networks and technologies for secure communication and information sharing

The Capability Development Plan (CDP) analysis points to an increasing risk of disruption through cyber attacks. It also underlines that cyber technologies, such as cyber situational awareness technologies and defensive cyber technologies are essential to counter cyber security threats faced by Member States, in particular the EU and Member States' command structures from tactical to strategic level.
The CDP also identifies the need to communicate and share information through deployable interoperable communication systems, data–sharing platforms (including data storage and sharing capabilities), and through *ad-hoc* and distributed networks.

Proposals are invited against any of the following topics

- **EDIDP-CSAMN-SDN-2019:** Modular and adaptive tactical network to control, change and manage network behaviour, including cyber security;
- **EDIDP-CSAMN-SSC-2019:** Software suite enabling real–time cyber defence situational awareness for military decision-making;
- **EDIDP-CSAMN-SSS-2019:** Software suite solution, enabling real-time cyber threat hunting and live incident response, based on shared cyber threat intelligence.

Budget

The Union is considering a contribution of up to EUR 17 700 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

2.3.1. Topic EDIDP-CSAMN-SDN-2019 – Modular and adaptive tactical network to control, change and manage network behaviour, including cyber security

Specific challenge

Software Defined Networking (SDN) is an evolving network architecture that focuses on the separation of control and data planes. SDN addresses the fact that the static architecture of conventional networks is not well-suited to today's high-bandwidth and very dynamic networking applications. SDN allows: (a) network behaviour to be controlled by software (programmability); (b) the creation of logically centralised network topologies which enable the intelligent control and management of resources; (c) the abstraction of services and applications from the underlying technologies; and (d) vendor-neutral networking infrastructure and openness.

SDN-enabled network architectures require reliable and high data rate communication between the network devices (SDN switches) and the SDN controller. Tactical networks on the other hand, may offer low rate and unreliable wireless links between highly mobile nodes. It is thus clear that, although SDN can offer significant benefits to tactical communications, a tactical network relying on SDN technologies will need to be very different from a typical civilian deployment as we know it today.

The main difficulties that a tactical SDN will need to overcome are:

- Highly mobile and heterogeneous end-nodes with no access to fixed network infrastructure;
- Unreliable and low data rate wireless links;
- Limited resources (power, bandwidth, data-storage, size and weight);
- Mission driven and frequent reconfiguration requirements;
- Strict physical and cyber security requirements (SDN controller may be a single point of failure) in a highly aggressive and insecure environment;
- Demanding logistics including backwards compatibility with legacy systems.

Scope

Proposals shall address the feasibility and design of SDN-enabled networks suitable for tactical use. All of the following areas should be covered:

- Network technologies, topologies and protocols suitable for tactical SDN-enabled networks;
- Requirements that should be applied to the corresponding tactical SDN controller;
- Use of Software Defined Radio (SDR) wireless nodes integrated in SDN-enabled tactical networks;
- Power, bandwidth and storage requirements and trade-offs of tactical SDN switches and controllers;
- Cyber security requirements, threats and counter-measures for tactical SDN-enabled networks;

- Demonstration of a SDN testbed that will allow the evaluation of SDN concepts in representative tactical scenarios from a technical and operational point of view. The testbed is expected to:
    - Rely on non-proprietary wireless technologies in order to facilitate ample testing, experimentation and evaluation from various actors;
    - Incorporate a limited number of heterogeneous mobile nodes;
    - Rely on existing SDN technologies and protocols that will be suitably integrated and/or modified and/or enhanced to facilitate the required validation setup.

Targeted activities

This proposal shall cover feasibility study and design, including the following activities:

- Collection and analysis of the end-users (armed forces) requirements at the tactical and tactical edge level with regard to existing networking SDN solutions;
- Definition of performance indicators to evaluate technical solutions versus the end-users requirements;
- Study of SDR and SDN interoperability requirements, constrains and consequences;
- Development of a tactical SDN testbed that will allow proof-of-concept;
- Definition and execution of extensive laboratory tests and cyber attacks under representative tactical scenarios;
- Collection and analysis of data for performance evaluation and insights provisioning;
- Suggestion of roadmaps for further development of tactical SDN R&T[28] efforts.

Main high-level requirements

The following general requirements shall be fulfilled by the SDN testbed:

- The testbed shall allow the experimentation with various technologies, network topologies and protocols suitable for tactical operations;
- The testbed shall allow the definition of representative tactical scenarios through the configuration of highly dynamic experimentation conditions;
- The testbed shall allow the evaluation of the communication performance, robustness and resilience in at least three cases: controller to controller, controller to switch, switch to switch;
- The testbed shall be able to demonstrate resource reallocation and policy enforcement on demand and produce the respective performance indicators;
- Cybersecurity enabling protocols and components shall be identified and tested including the elimination of single point of failures;
- SDN switches and controllers shall comply with realistic tactical Size, Weight and Power (SWaP) requirements.

Expected impact

[28] Research and Technology.

- Identify the necessary modifications to the existing SDN systems in order to make them suitable for tactical networks and operations;
- Assess the advantages and disadvantages of applying SDN technologies to tactical communication networks based on objective Key Performance Indicators (KPIs);
- Support the development, competitiveness, efficiency and strategic autonomy of the European industry in the field of SDN products and technologies;
- Enhance the interoperability of tactical communication systems of coalition forces;
- Create secure *ad-hoc* and distributed networks avoiding the existence of single points of failure.

2.3.2. Topic EDIDP-CSAMN-SSC-2019 – Software suite enabling real–time cyber defence situational awareness for military decision-making

Specific challenge

Cyber Situational Awareness (CSA) enables commanders to have a clear understanding of the threats landscape in order to manage cyber risks during the planning and conduct phases of a military operation. In 2013, Member States identified, within the EDA[29] cyber defence project team, the need for capabilities to enable military commanders to put in place measures to mitigate the risk of cyber attacks at all operational levels. An important prerequisite was to provide CSA for commanders and related staff.

The analysis of the state-of-the-art in CSA suggested that there are neither commercial nor open-source CSA solutions that appropriately match the full capabilities raised by military end users, as it was echoed by EDA. Although certain capabilities might be more mature than others, all-in-one solutions are not available yet. In order to overcome this shortcoming, the proposals against this sub-topic should be complementary to any ongoing EDA project.

Scope

Proposals submitted under this topic must bring support to the ongoing CSA capabilities of the Member States. In this way, they shall focus on providing operational prototypes of software suites for enabling real-time CSA that facilitate military decision-making. Contributions should introduce cognitive visualisation tools and integration with existing sensors. The system should be multi-tiered meaning information, which shall be aggregated according to the needs of the viewer at technical, operational or strategic level.

Targeted activities

Proposals shall cover the following activities related to design and system prototyping, not excluding upstream and downstream activities required for supporting the acquisition of CSA and incident response:

- Automatic data collection, normalization, aggregation, and fusion from various data sources, including, but not limited to, Network Operation Centers (NOC), Security Operation Centers (SOC), Cyber Threat Intelligence (CTI), conventional security sensors (*e.g.* firewalls, SIEMs[30], NIDS/NIPS[31], FPC[32], DPI[33], *etc.*), and Mission Planning Systems (MPS);
- Impact and risk calculation on assets and services held by computer information systems and missions, including those that support the instantiated CSA capabilities. This must cover at least alerts, warning, errors, anomalies and any other symptom of suspicious activities;
- Risk management and decision support capabilities aiming at enhancing the most suitable Courses of Action (CoA), which shall rely on simulating countermeasures,

[29] European Defence Agency.
[30] Security Information and Event Management.
[31] Network Intrusion Detection Systems / Network Intrusion Protection Systems.
[32] Full Packet Capture.
[33] Deep Packet Inspection.

constructing what-if scenarios and instantiating catalogues of predefined policy-driven actuations;
- Knowledge acquisition from the discovered symptoms, anticipation of the next steps of the attackers, and projection of the damage spreading throughout the protected environment;
- Graphical visualization of sensors, actuations, cyber risks and missions courses. The commander's view must provide any additional information for facilitating the acquisition of CSA, including CTI, geographical data, network status or risk level. It must display the suggested CoA and the predictions of the status of the monitoring environment.

Proposals could also include the development of small-scale testbeds for local validation and calibration of the capabilities to be developed. They include gathering up-to-date datasets and synthetic traffic/behaviours simulations.

Main high-level requirements

The following general requirements shall be fulfilled:

- The system shall implement modern and intuitive user interfaces supporting commanders and operators in all their operational, technical and training needs;
- Usability shall be the cornerstone of the system design, thus allowing rapid installation, administration, operation and training;
- Contributions shall be able to be reconfigured to be suitable to interface with different types of networks and to support different protocols;
- A foremost requirement to be developed is the security of the CSA capabilities themselves. The solution proposed shall present greater levels of availability, confidentiality and integrity than the protected environment;
- The selection of related technological solutions and standards shall have a strong focus on their obsolescence management and interoperability;
- The system shall be able to simultaneously operate on different security domains and to handle the information security requirements in order to properly control the information flows between these domains and external systems;
- The system shall provide dynamic, scalable and resilient solutions, which must be capable of easily integrating all the actors and nodes involved in each mission;
- The proposed solution shall be constructed and documented to satisfy minimum-security requirements according to NATO and EU security rules for processing classified information up to EU SECRET and equivalent NATO security level;
- The system shall generate an audit trail for the following operations carried out by users:
    - Security events on the system, like login attempts, successful logins, logouts, attacks detected (*e.g.* brute force attacks);
    - Administration tasks;
    - Security administration tasks.
- The proposed solution shall be adapted to the EU generated doctrine.

Expected impact

- Develop a critical enabler for CSDP (Common Security and Defence Policy) operations and missions;
- Improve situational awareness, resilience and security of EU and Member States operations;
- Support the development of Member States' cyber defence capabilities;
- Facilitate defensive cyber operations in any operational context;
- Facilitate military decision-making;
- Manage cyber risks during the planning and conduct phases of an operation;
- Enable military commanders at all operational levels to understand and manage the risk of cyber attacks;
- Provide a clear understanding of the cyber threat landscape including system vulnerabilities and attack vectors.

2.3.3. Topic EDIDP-CSAMN-SSS-2019 – Software suite solution, enabling real-time cyber threat hunting and live incident response, based on shared cyber threat intelligence

Development of cyber situational awareness technologies and defensive cyber technologies are essential to counter cyber security threats faced by Member States, in particular EU and Member States' command structures from tactical to strategic level.

Specific challenge

Cyber attacks continue to increase in frequency and sophistication, presenting significant challenges for public or private organizations that must defend their data and systems from capable cyber threat actors. These actors range from individual, autonomous attackers to well-resourced groups operating in a coordinated manner as part of a criminal organisation or on behalf of a nation-state. Threat actors can be persistent, motivated, and agile, and use a variety of Tactics, Techniques and Procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information.

In order to meet the EU CSDP military level of ambition, it is necessary to develop a cyber threat information sharing and Endpoint Detection - Response framework (EDR) with extensive cyber defence and incident response capabilities.

This framework should be capable of early detecting, mitigating, responding and sharing information related to known and unknown cyber threats targeting Member States, causing detrimental effects on civilian and military missions and operations.

Scope

Proposals shall address the feasibility, design and development of a system that is capable to provide cyber situation awareness through information sharing, combined with advanced cyber defence capabilities such as threat hunting, continuous monitoring and effective incident response to all Member States.

Targeted activities

Proposals shall cover the feasibility study and design of the system including, but not limited to:

- Feasibility study with a focus on the expected impact on the end-users;
- Concept of operations (CONOPS);
- System specification and architecture definition;
- Preliminary Design Review (PDR) and Critical Design Review (CDR).

Proposals shall also include the release of preliminary versions of the final deliverables to verify and test the functionality and detailed timelines and milestones to identify the progress priorities, according to operational needs of the Union and its Member States.

Main high-level requirements

The System shall fulfil the following high-level operational requirements:

- State-of-the-art system, with modern, intuitive user interface supporting military Computer Incident Response Centre (mCIRC) analysts in all their operational, technical and training needs. Usability shall be the cornerstone of the system design allowing rapid familiarization, administration, operation and training;
- Use of modern techniques and information handling approaches, including, but not limited to, artificial intelligence and machine learning;
- The proposed system shall be scalable and modular, focused on expanding and meeting the future operational capabilities and allowing other PESCO[34] or EU defence projects to be linked, integrated or implemented through this one;
- The proposed system shall be based on a modern service oriented architecture with an extensive use of open standards, allowing full compatibility with NATO and national systems, both military and civilian;
- The system shall be easily deployable in different environments according to the needs of each Member State;
- The system shall meet the highest information security requirements to properly control the information flows between Member States;
- The system shall be able to be deployed over a variety of datacentres and COTS IT[35] equipment and to operate in virtualized, capable and resilient environments. It shall also be capable of easily integrating all the actors and nodes environments in conjunction with specific security equipment, such as Information Exchange Gateways (IEGs), firewalls, Intrusion Detection and Prevention Systems (IDSs and IPSs), *etc.*;
- The system shall be able to support the mCIRC availability requirements providing an open, scalable, high availability and transparent failover architecture;
- The system shall be secured-by-design;
- The system shall be adapted to the EU generated doctrine.

The acknowledgement of cyberspace as an active operational domain implies an increasing need for cyber threats information sharing, in order to help Member States to efficiently cope with the constantly evolving cyber threat landscape.
The proposed system shall deliver a cyber threat and incident response information sharing technology with extended cyber threat hunting and defence capabilities (EDR).
More specifically, the system shall provide:

- Incident handling and response capability (both remote and onsite);
- Centralized access to massive endpoint data facilitating cyber defence analysts hunt for threats in real-time, as well as the conduct of in-depth investigations in case of incident;
- A platform agnostic architecture;
- Advanced information processing capabilities;
- Multi-layer access control (restrict access to users based on their roles);
- Data export features;

[34] Permanent Structured Cooperation.
[35] Commercial Off-The-Shelf Information Technologies.

- Built-in correlation of existing malicious TTPs;
- Advanced dashboards and visualizations to endorse decision-making process.

Expected impact

- Enhance the ability of the EU to conduct effective CSDP operations and missions in the cyberspace;
- Review, extend and optimize existing information sharing mechanisms and procedures among the Member States;
- Help the Member States build a cyber threat intelligence driven incident response culture (active defence – more proactive measures meaning pre-emptive actions – could be taken based on the quality of the threat intelligence);
- Build a common cyber awareness culture among Member States;
- Integrate CIS (Communication and Information Systems) and ISR (Intelligence, Surveillance and Reconnaissance) means provided by Member States, EU forces, NATO and civil agencies;
- Improve situational awareness, resilience and security of EU operations;
- Reinforce interoperability of Member States' armed forces;
- Reduce the cost of European military missions.

2.4. Call EDIDP-PNTSCC-2019 – Positioning, Navigation and Timing (PNT) and satellite communication capabilities

The Capability Development Plan (CDP) points to the need to develop EU military Positioning, Navigation and Timing (PNT) requirements and related capabilities and to promote the development of robust, secure and resilient EU military PNT capabilities. The CDP further highlights the need to develop capabilities to meet the increasing requirements for Satellite Communication (SATCOM). A comprehensive set of PNT and SATCOM capabilities should contribute to enhancing dissemination and must be capable of distributing timely data, information, intelligence and specialist and all-source analysis, in an appropriate and accessible form, across and between networks as required.

Proposals are invited against any of the following topics

- **EDIDP-PNTSCC-PNT-2019:** Development of European standardized and sovereign Galileo PRS[36] navigation receiver capabilities compatible with GPS/PRS solution for military purposes;
- **EDIDP-PNTSCC-SCC-2019:** Development of a European protected waveform to secure military satellite communications in peacetime, missions and operations.

Budget

The Union is considering a contribution of up to EUR 44 100 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay attention to the civil and dual-use on-going initiatives at Union level to avoid any duplication (especially with Galileo).

[36] Public Regulated Service of Galileo system.

2.4.1. Topic EDIDP-PNTSCC-PNT-2019 – Development of European standardized and sovereign Galileo PRS navigation receiver capabilities compatible with GPS/PRS solution for military purposes

This topic intends to develop European standardized Galileo Public Regulated Service (PRS) receiver technological capabilities, compatible with dual mode GPS/PRS GNSS[37] receiving equipment for military applications in air, land, naval and possibly space domains and achieving full compliance with the EU Common Minimum Standards (CMS).

Specific challenge

First satellite navigation systems, *e.g.* GPS, were designed under military requirements and budget to improve defence capabilities. They revolutionised military applications by providing accurate position, velocity and time/synchronisation information for all military assets worldwide, in all weather conditions, with a common time and geodetic reference frame supporting the essential interoperability requirement. Galileo has been developed to guarantee Europe's strategic autonomy in Satellite navigation. The Galileo PRS has been developed as a robust, secure and resilient PNT service even in case of denial of the other GNSS services. Interoperable and compatible with GPS, the PRS will provide the EU military users state-of-the-art satellite navigation performance, robustness and interoperability and, when combined with GPS, an even higher level of resilience for military use.

The CDP points to the need to promote the development of robust, secure and resilient EU military PNT capabilities. To achieve this objective in time (with regard to the Galileo PRS Full Orbital Capability (FOC) foreseen by 2023), operational EU military PRS receivers, associated to their antennas and key management facilities as well as service architectures and test and support facilities, need to be developed and those developments cannot be supported by the private sector, because of the high investment cost. In addition, the development of military standardized Galileo PRS receiver interfaces has been identified as an objective within the Permanent Structured Cooperation (PESCO). This standardisation will ensure the development of the EU market by facilitating the integration of PRS receivers into the armament systems. It will then increase the competitiveness and growth of the defence industry for those armament systems (the satellite navigation capabilities embedded are one of the criteria of choice for armament systems within the military market).

The EU activities supported so far have been feasibility studies, design activity and accreditation of one pre operational prototype.

Therefore, the challenge is to develop EU operational prototypes of PRS receivers with standardized interfaces, to be qualified and tested by FOC (2023) within at least one host platform. Testing in standardized and controllable test facilities as well as in a real environment with in-field demonstrations implementing real/realistic service architecture must be scheduled with the involvement of defence user communities.

Scope

[37] Global Navigation Satellite System.

Proposals shall address the development of European standardized and sovereign Galileo PRS navigation receiver capabilities compatible with GPS/PRS solution for military purposes in air, land, naval domains developed in full conformity with the EU Common Minimum Standards (CMS) from prototyping up to qualification or test. In this respect, the proposals shall cover:

- PRS security modules (SM);
- PRS receiver equipped with GPS/Galileo-compatible CRPA (Controlled Radiation Pattern Antennas);
- Anti-jamming and anti-spoofing capabilities/protection as applicable to the operational domain;
- Standardization of interface with military GPS and multi-GNSS fusion;
- Standardization of interface for PRS receivers;
- Key management, PRS security management and other PRS information management capability;
- Services architectures for test and support facilities;
- Security certification.

The tests shall be performed in standardized support facilities guaranteeing a controlled environment and afterwards in operational conditions with the operational Galileo system and real/realistic service architecture to demonstrate the real capability of the PRS receivers developed. The possibility to consider space domain may be addressed in the proposals.

Targeted activities

The proposals shall cover all the necessary activities for the prototyping, testing and qualification on different platforms (naval, land, airborne) of PRS receivers, encompassing in particular:

- Prototyping of:
    - PRS SMs including application-specific integrated circuit SMs;
    - PRS receivers as well as integration activities in host equipment and smart antennas (such as CRPA), *e.g.* navigation systems and platforms.
- Prototyping, testing and qualification of common infrastructure for testing, key management, PRS security management and other PRS information management;
- Standardization of the interfaces with military GPS and multi-GNSS fusion: those standardization documents shall be elaborated for PRS receivers and for host equipment embedding a PRS receiver, *e.g.* navigation systems and/or hosting platforms;
- Testing and qualification of resulting PRS receivers operational prototypes on a set of representative military applications including jamming and spoofing protection;
- Implementation of the security certification process of developed PRS products involving at least two Member States' civil aviation authorities in all the relevant steps.

Main high-level requirements

The following requirements shall be fulfilled:

- The PRS activity shall comply with PRS security rules defined by Decision No 1104/2011/EU [38] , by Commission delegated supplementing Decision No 1104/2011/EU as regards the Common Minimum Standards (CMS)[39], and by the referenced programme documents (classification guide, COMSEC[40] instructions…);
- Galileo PRS receiver functions shall be embedded in the form of standardised and generic PRS boards;
- At least two generic PRS boards and two SMs shall be prototyped, at least one of those SMs being an application-specific integrated circuit;
- The PRS receiver prototypes shall use technologies suitable for various types of platforms for land, maritime, air domains and timing & synchronisation;
- Standardisation activities shall consider dual mode Galileo PRS/GPS operational use;
- Standardization documents shall in particular define the functional and performances characteristics of the PRS receivers as well as the interfaces, including with GPS and multi-GNSS fusion;
- Standardized Form factors and interfaces of the generic PRS boards shall be chosen in order to facilitate integration for the EU defence industry;
- The standardisation activities shall prepare maximum reuse of building blocks and technologies already developed within the EU;
- Test with host platforms shall be defined from a broad range of representative applications such as tactical RPAS[41], ISTAR[42] vehicles, naval patrol boats (maritime surveillance capabilities), combat vehicles, land robotics, time keeping and network synchronization;
- Validation tests shall be performed in a common and standardized test environment to be developed and by demonstrations within European field test centres and/or, when possible, during operational test campaign in several Member States;
- The field test campaigns shall include the testing of the navigation capabilities in jamming and spoofing environments to validate in particular the achievement of a robust, secure and resilient EU military PNT capability for the EU;
- Each standardization activity shall produce, as deliverable, an interface control document.

Expected impact

- Contribute to the industrial autonomy of the European defence industry and to the security and defence interests of the Union;

[38] Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme, OJ 287/1, 4.11.2011.
[39] Commission delegated Decision C(2015)6123 of 15.9.2015 supplementing Decision No 1104/2011/EU of the European Parliament and of the Council as regards the common minimum standards to be complied with by the competent PRS authorities.
[40] Communication Security.
[41] Remotely Piloted Aircraft System.
[42] Intelligence, Surveillance, Target Acquisition and Reconnaissance.

- Promote and facilitate the uptake of the Galileo PRS service, developed under EU funding, to cover EU defence applications and provide significant advantages over existing defence products or technologies;
- Provide the EU industry with an equal playing field in the defence market where embedded GNSS solution is a competitive advantage (with currently no embedded EU GNSS solution);
- Guarantee an access to all Member States to PRS equipment and services with the availability of common innovative qualified PRS technologies;
- Providing EU owned standards for the interfaces for Galileo PRS receivers;
- Provide essential technologies for EU defence interoperability;
- Create a critical mass for PRS equipment and incentivize joint procurement and maintenance leading to price reduction/cost savings;
- Ensure PRS user equipment technology readiness across the whole value chain, enabling EU military forces equipment at PRS FOC declaration;
- Consolidate the credibility of the PRS EU approach during the on-going international PRS negotiations (currently with Norway and the United States).

2.4.2. Topic EDIDP-PNTSCC-SCC-2019 – Development of a European protected waveform to secure military satellite communications in peacetime, missions and operations

Specific challenge

In today's military applications supported by satellite communications, security, information assurance and link efficiency technologies are inextricably linked. Military operations are becoming more complex as conflict areas grow more dispersed on a global scale, with a growing need to support a diversity of on-the-move, on-the-pause and fixed platforms. At the same time, cyber security threats are becoming more apparent, raising concerns that nations, terrorist groups, criminals and individual hackers can jam, interrupt and endanger military operations.

Member States are increasingly pooling and sharing their defence efforts to increase their strategic autonomy in a geopolitical context, overcome new security risks with enhanced military capabilities, and create a more competitive and integrated defence industry.

In satellite communications, most individual nations cannot generate significant capabilities by themselves. Instead, European nations can generate increased capabilities through cooperation and collaboration. Several pooling and sharing initiatives have already been kicked off in the European defence context to face challenges related to the fragmentation of supply and demand, the assured secure access to satellite communications and the changing environment.

The complexity of dispersed operations translates into requirements to have access to complex global satellite communication networks with a mix of different satellite types and services to support a wide variety of military applications. Security is the key feature belonging to all those requirements that in addition need to be met in the most efficient way.

However, these wide-ranging requirements face an increased risk of ill-intentioned acts and cyber attacks against military satellite communication networks such as jamming, signal spoofing and interception attempts.

A key element to reply to this security challenge is the satellite communication waveform, which needs to be as protected and secure as possible.

Different initiatives to make satellite communications more secure and reliable through the creation of (proprietary) protected waveforms have already been undertaken and/or are ongoing within the military context. Yet the results of those initiatives are used only in sovereign national satellite networks of some major nations, driven and supported by big international industrial players.

The great majority of Member States do not have independent access to secure satellite communication waveforms, although they also engage in military operations in a national or multinational (EU, NATO, UN peacekeeping, *etc.*) context. The investment for developing a protected waveform cannot be carried out by a single nation alone and requires a multi-national development approach in a European context with the aim to establish a European Protected Waveform (EPW).

Scope

The EPW shall be able to operate in this complex military operational environment and bring a solution to the challenges described.
Proposals should address feasibility, design and development of an EPW for satellite communications that can be used by different EU nations individually or together in a joint operational context (EU, NATO, multi-nation missions) with five key considerations in mind.

- **European autonomy and cooperation between Member States**

The EPW shall be capable of increasing the autonomy of Europe and of reducing the dependence on non-European satellite communication technology for military operations with mission critical and sensitive information. At the same time, it shall allow for interoperability between EU nations in a joint operational context in order to exchange mission critical information and improve the efficiency of the operations.

- **Affordable and efficient satellite services**

The EPW shall be affordable and include the latest efficiency satellite communication waveform, networking and equipment technologies to save OPEX[43] (reduce bandwidth costs, need for less resources for planning) and CAPEX[44] (reduce equipment cost) compared to current existing expensive (proprietary) military satellite modems.
The EPW shall include already available innovative Commercial Off-The-Shelf (COTS) satellite communication technologies (*e.g.* DVB-S2X[45] waveform standard) in combination with the latest security technology. There shall no longer be a trade-off between the efficiency of the waveform and security. As such, high throughput demands shall be achieved even with small terminals using a limited amount of satellite bandwidth.

- **Flexibility and scalability**

The EPW shall be portable on different modems with different form factors (board, modem, terminal), different platforms (fixed, on-the-move, on-the-pause) and be used across multiple types of satellite communication networks, different types of satellite constellations (LEO[46], MEO[47], GEO[48], high-throughput systems, spot beams, regional and global beams) and different network architectures (VSAT[49], SCPC[50], mesh). At the same time, the EPW shall be operational in different satellite frequency bands (at least C-band, X-band, Ku-band and Ka-band) and exchange, broadcast, multicast, unicast or relay a large range of satellite services and applications from low to very high data rates.

- **Innovation**

The EPW development shall not just be a copy and paste of existing solutions, licenses and technologies. The EPW proposal shall be ambitious and innovative, combining the individual

[43] Operational expenditure.
[44] Capital expenditure.
[45] Extension to Digital Video Broadcasting – Satellite Second generation standard.
[46] Low Earth Orbit.
[47] Medium Earth Orbit.
[48] Geostationary Equatorial Orbit.
[49] Very Small Aperture Terminal.
[50] Single Channel Per Carrier.

strengths of different nations and different members in the European satellite communication industry. The EPW program shall be open to support future requirements and capabilities needed.

- **Security and resilience**

The main feature of the EPW shall be the increase in protection and resilience of the waveform to ensure secure information exchange over satellite for mission critical communications. Based on different threat analysis and Concept of Operations (CONOPS) definitions, the EPW development shall focus on building satellite links that are resistant to cyber attacks such as jamming, signal spoofing, eavesdropping and interception attempts. In addition, satellite link outages caused by rain fade, atmospheric conditions or on-the-move communication challenges shall be reduced to a minimum. The EPW activity shall investigate how different security levels can be offered towards different government and defence end-users depending on their security requirements, their daily operations and the budgets available.

Targeted activities

The proposals shall cover the initial phases of the development of the EPW including in particular:

- Feasibility study, threat analysis, CONOPS definition, system specification, Detailed Requirements Review (DRR) and architecture definition;
- Detailed design of the system, including the Preliminary Design Review (PDR) and finishing with the Critical Design Review (CDR);
- The development of small-scale technological demonstrators with military end-users in an operational environment, in order to support decision making during the design phase.

The end state shall be an EPW standard for satellite communication (comparable to other communication waveform standards) that can be implemented by nations or industry on their individual baseband solutions.

Main high-level requirements

The EPW development shall fulfil requirements at the level of both the waveform and the satellite baseband equipment (terminals, modems, hubs, networks). The demarcation point is the edge router of the satellite network which connects the hubs, gateways and modems with outside networks or the internet.

- **Baseband equipment requirements:**
    - The right implementation of the terminal will determine the success of the EPW. The flexibility and the affordability of the terminal are key considerations. Hence the preference for Software Defined Radio (SDR) type of equipment;

- The baseband infrastructure (hubs and modems) needs to cover multiple architecture types of networks (point-to-point, point-to-multipoint, mesh) and satellite (wideband, spot beam, mix of both) architectures;
- The EPW shall operate on SDR hardware from different vendors that will be selected by nations, government and defence agencies or institutions, depending on their preference or acquisition processes;
- The EPW shall include the ability to receive and transmit various modulation methods using a common set of hardware. A modem could also run the EPW and a proprietary or DVB standard waveform on the same platform and switch waveforms, if needed;
- The EPW shall be future-proof and easy to upgrade – the ability to alter functionality by downloading and running new software at will, in order to repurpose the modem for a new application;
- The EPW shall be affordable and include the latest efficiency satellite waveform, networking and equipment technologies to save OPEX (reduce bandwidth costs, save resources for planning) and CAPEX (save on equipment cost) compared to existing expensive military satellite modems;
- The EPW shall consider Size, Weight and Power (SWaP) constraints for on-the-pause and on-the-move platforms and shall be easy to transport;
- The EPW shall be deployable in different environment conditions and on different platforms (land, sea or air);
- The EPW shall be available in different form factors (OEM[51] cards, rack units or rugged terminals);
- The EPW shall be license-based to cater for different level of users;
- The EPW shall be transparent for national encryption standards and externally encrypted data, and capable of integrating on-board encryption technology;
- The EPW shall be capable of introducing dedicated authentication certificates;
- The EPW shall be reliable to ensure continuity of operations;
- The EPW shall have performances considering the throughput demands of today and the future;
- The EPW shall support pooling and sharing service models of both waveform and equipment that can be implemented for different operations.

- **Protected waveform requirements**

  The EPW shall:
  - Be defined as a standard to enable interoperability. Multiple terminal vendors must be able to support the EPW and be compatible, even on a minimum basis;
  - Be affordable, based on the best practices of COTS and government or military-grade waveforms;
  - Implement the latest SATCOM efficiency technology to obtain the best performance out of a satellite link;

[51] Original Equipment Manufacturer.

- Support a range of different satellite constellations (HTS[52], wideband, military, commercial, government, GEO, MEO, LEO), satellite architectures (pure transponder, partially or fully processed) and frequency bands (C-band, X-band, Ku-band, Ka-band);
- Be easy to port on other SDR modems or hubs;
- Flexible to support multiple governmental and defence applications that require different levels of security;
- Consider a growing amount of on-the-move and on-the-pause platforms connected over the satellite with a need for mobility features (Doppler compensations, spreading modulation, small and flat antenna support, beam switching, beam hopping, *etc.*);
- Operate in GPS-denied environments;
- Provide adequate protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping;
- Consider a wide range of throughput requirements and satellite bandwidth sizes (symbol rates);
- Offer seamless and resilient satellite links against fading effects, interference (intentional and unintentional), shadowing effects and jamming (fixed and sweeping);
- Be capable of supporting different service models such as pooling and sharing.

Expected impact

- Availability of a critical enabler for CSDP operations and missions in providing scalable secure and resilient communications in peacetime and during operations with protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping;
- Full interoperability between different demanders and suppliers of satellite communication in support of military operations and missions;
- Secure, guaranteed and affordable access to satellite communications for all Member States;
- Strongly increased European autonomy in satellite communication for defence users and no longer dependency on support from outside the EU for the transmission and exchange of mission critical and sensitive information;
- State-of-the-art technological solution in line with the latest satellite innovations and initiatives such as 5G, small LEO/MEO satellites, connected vehicles and Internet of things.

[52] High Throughput Satellites.

2.5. Call EDIDP-ESC2S-2019 – European Command and Control (C2) system from strategic to tactical level

Development of a strategic C2 capability according to the needs of a future fully operational EU headquarter. This call for proposals intends to complement existing European External Action Service (EEAS) C2 and Communication and Information Systems (CIS), to enhance and further develop the Military Planning and Conduct Capability (MPCC) of the EEAS towards a true strategic EU headquarter, covering all kinds of military operations, both executive and non-executive.

Proposals are invited against the following topic

EDIDP-ESC2S-2019: Capabilities and equipment needed for establishing C2 system from strategic to tactical level, complementing existing European External Action Services systems.

Specific challenge

The Global Strategy for the European Union's Foreign and Security Policy[53] defines an integrated approach to conflicts "*at all stages of the conflict cycle, acting promptly on prevention, responding responsibly and decisively to crises, investing in stabilization and avoiding premature disengagement when a new crisis erupts*".

The Capability Development Plan (CDP) analysis also highlights that resilient C2 capabilities are critical enablers for Common Security and Defence Policy (CSDP) operations and missions.

Specific shortfalls concerning the fulfilment of the EU CSDP military level of ambition are a consequence of EU strategic Command, Control and Coordination (C3) at military level. This EU strategic C3 should be capable of directing, coordinating and controlling all EU CSDP actions, missions and operations, as well as civilian and military actors and forces in an integrated approach, in the full spectrum of crises – before, during and after conflicts – by managing its development, stopping ongoing conflicts and contributing to consolidating stability in the post-conflict situation.

Scope

Proposals shall address the feasibility and design of a system that includes, in particular, the capability to conduct several simultaneous operations, with all kinds of forces, anywhere in the world, either independently or in cooperation with NATO. The Strategic C2 must integrate all kinds of Communication and Information Systems (CIS) and Intelligence Surveillance and Reconnaissance (ISR) means and shall be able to interoperate with Member States, EU forces, NATO and civil agencies. The size, duration and number of simultaneous operations and deployments to be planned and conducted must be based on the EU level of ambition for CSDP missions and operations established by the Council for the MPCC.

The strategic C2 system shall support a large staff working simultaneously over multiple operations, with a scalable C2 structure that could be adapted to each mission.

[53] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy (http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf).

The architecture of the strategic C2 system should also consider integrating and complementing the tactical and operational levels.
The strategic C2 system shall support all operational phases:

- Planning:
  - Supporting the capabilities demanded by Joint C2, including personnel, intelligence, operations, logistics, plans, CIS and Civil-Military Cooperation (CIMIC);
  - Integrating planning information from all domains (air space management, naval operations, ground deployments, cyber situational awareness, *etc.*). and external systems;
  - Allowing the European Union Military Staff (EUMS) to effectively task its own staff and other supporting armies.
- Pre-deployment:
  - Supporting force projection tasks in complex scenarios (infrastructures databases, *etc.*).
- Deployment:
  - Monitoring deployment tasks;
  - Supporting the quick establishment of communications and command posts upon initial entry.
- Mission conduct:
  - Generating real time common operational picture;
  - Integrating many systems for multiple domains;
  - Segmenting the information in the most automated way per mission;
  - With a strict control on the information dissemination.
- Re-deployment.

Target activities

The proposals shall cover the initial phases of the development of the strategic C2 system including in particular:

- Preliminary studies: analysis of existing MPCC capabilities and systems and their potential evolution. Analysis of the existing systems that the strategic C2 system may potentially be required to be interoperable with (NATO, national, others). Dialogue with EUMS / MPCC to capture requirements, experience and lessons learned applicable to the future system;
- Feasibility study, definition of Concept of Operations (CONOPS), system specification, Detailed Requirements Review (DRR) and architecture definition;
- Detailed design of the system, including the Preliminary Design Review (PDR) and including up to the Critical Design Review (CDR).

The project could also include the development of small-scale technological demonstrators, in order to support decision making during the design phase.
A detailed planning of the subsequent project phases shall be generated, including the identification of implementation priorities, according to the operational needs of the EU and its Member States. Subsequent phases up to operational readiness shall include in particular

prototype development, qualification and test activities, following a spiral approach, to reach incremental operational capabilities.

Main high-level requirements

The system shall fulfil the following general requirements:

- State-of-the-art system, with modern, intuitive user interfaces supporting MPCC operators in all their operational, technical and training needs. Usability shall be the cornerstone of the system design allowing rapid installation, administration, operation and training;
- Selection of technological solutions with a strong focus on obsolescence management;
- The system architecture shall be designed in accordance with the modularity principle in order to be expandable to future operational capabilities and to integrate modules and tools coming from multiple sources, allowing other PESCO[54] projects to be linked, integrated or implemented through this one;
- The proposed system shall be based on a modern service-oriented architecture with an extensive use of open standards, allowing full compatibility with NATO and national systems, both military and civilian. Specifically the system must be interoperable with a federated mission network;
- Effective use of communications, covering also tactical levels. The system shall operate in a full IP[55] communication network that shall be able to integrate different transmission mechanisms (WAN[56] segments, SATCOM, *etc.*). The system shall be able to seamlessly use the available transmission mechanisms and adapt the information flows to their specific characteristics;
- The system shall be able to work simultaneously in different security domains and handle the information security requirements to properly control the information flows between these domains and the integrated external systems;
- Dynamic, scalable and resilient, capable of easily integrating all the actors and nodes for each mission;
- The system shall be able to be deployed over a fixed C2 centre, which will host the MPCC operators and in deployable centres. The system will be deployable over COTS IT[57] equipment and will be able to operate in virtualized environments in conjunction with specific security equipment, such as Information Exchange Gateways (IEGs), Firewalls, Intrusion Detection and Prevention Systems (IDSs and IPSs), *etc.* Specifically the feasibility of an architecture based on cloud concepts (either private or hybrid) must be analysed;
- The system shall be able to support the MPCC availability requirements providing an open, scalable, high availability and transparent failover architecture;

[54] Permanent Structured Cooperation.
[55] Internet Protocol.
[56] Wide Area Network.
[57] Commercial Off-The-Shelf Information Technologies.

- Cybersecurity aspects must be taken into account along all project phases, from requirements capture to system design and implementation, in order to ensure adequate resilience, survivability and information protection;
- The system shall be adapted to the EU generated doctrine.

The architecture of the strategic C2 system shall take into consideration all necessary future elements, and in particular:

- Communication equipment and infrastructure, in order to be able to exchange information between the EU headquarter and the Member States' C2 centres and information systems. This may require the use of dedicated terrestrial networks and satellite links, hub infrastructure and terminals;
- The infrastructure to setup a dedicated C2 centre, including facilities for operators, data centres, and all the associated equipment (operators' equipment, voice / video communications, local communications, *etc.*);
- Deployable C2 centres, based on shelters and providing operator posts, a deployable data centre, communications and the required infrastructure;
- Architecture designed for security accreditation and cyber defence in order to prevent cyber attacks and to protect the information.

Budget

The Union is considering an EDIDP funding of up to EUR 20 000 000 to support proposals addressing the above-mentioned topic and its specific challenge, scope, targeted activities and main high-level requirements.

Expected impact

- Develop critical enablers for CSDP operations and missions;
- Reduce the minimum reaction time for deployment of European military missions;
- Integrate all CIS and ISR means provided by Member States, EU forces, NATO and civil agencies;
- Improve situational awareness, resilience and security of EU operations;
- Create a reference Strategic C2 System that will improve the capabilities of the European defence industry to develop and supply state-of-the-art C2 systems;
- Reinforce interoperability of Member States' armed forces;
- Reduce the cost of European military missions.

2.6. Call EDIDP-NGPSC-2019 – Upgrade of current and development of next generation ground-based precision strike capabilities

The availability of mobile precision systems able to provide the necessary high degree of accuracy and efficiency, when the use of the force is required, avoiding widespread collateral damage, and reducing exposure of friendly forces is a priority for Member States' armed forces. The Capability Development Plan (CDP) analysis identifies the need for the upgrade of current and development of next generation of direct and indirect fire support capabilities for precision and high efficiency strikes, including ammunition and fire control systems.

Proposals are invited against the following topic

EDIDP-NGPSC-2019: European Beyond Line Of Sight (BLOS) anti-tank capabilities.

Introduction

The ground combat is one of the eleven EU capability priorities identified as part of the revised 2018 CDP. This assessment acknowledges the necessity to further develop existing land battlefield missile systems.

Moreover, the development of an EU new generation medium range Beyond Line Of Sight (BLOS) land battlefield missile systems family has been identified as an objective within the EU BLOS Land Battlefield Missile Systems project of the Permanent Structured Cooperation (PESCO). There is a need to develop a capability providing a high degree of accuracy while avoiding widespread collateral damage, and reducing exposure of friendly forces.

The EU is facing increasing geopolitical instability and a complex set of conventional and new threats. Therefore, the armed forces of the Member States need the ability to operate autonomously or, as a valuable contributor, within an *ad-hoc* coalition. They have to intervene in a high intensity and in asymmetric engagement, facing a wide range of threats including potential technically advanced adversaries. Moreover, some requirements are becoming increasingly important:

- Providing the land combat units with the ability to defeat at medium range, with a high degree of accuracy and reliability, selected threats that are not always clearly identified and visible, especially in a urban environment, or defeat targets that may mask or unmask at the last moment;
- Reducing exposure to enemy fire;
- Avoiding widespread collateral damage;
- Allowing concentrating fires without concentrating means, providing autonomy, reactivity and freedom of action on the battlefield.

Specific challenge

In this context, the European BLOS capability will bring a significant operational differentiator to the armed forces of the Member States. Such a capability can be mounted or dismounted on manned and unmanned land platforms, in consistence with the CDP long term analysis which identifies the need to deploy automated effectors to reduce the danger on human personnel or manned platforms.

Several products and technologies currently exist or are under development in Europe but they need to be integrated in order to achieve this BLOS capability:

- A land battlefield missile system, BLOS native with a full Lock-On After Launch (LOAL) capability, and providing Man-In-The-Loop (MITL) through a seeker back-image for over watch and control during the whole flight of the missile;
- A turret system to support and set up the missile using an Unmanned Aerial Vehicle (UAV) for target designation;
- A land platform;
- A UAV providing a cyber-secured target location.

In order to guarantee freedom of operational use, capacity to implement further evolutions over time, and standardization of those interfaces with other EU land battle systems, the European BLOS capability has to be built without restraints and restriction from third country or third country entity, in particular regarding IPR and know-how, and must be free of any third party control regime.

Scope

The scope of this action includes:

- The analysis of the operational requirements for a small unit able to deliver autonomously both LOS and BLOS firings, and proposal of operational concept of use through dedicated scenarios;
- The realisation of a full-scale demonstration.

The proposals shall include an analysis of the operational needs and of the different technical contributors of the BLOS capacity. The concept of use shall be illustrated by scenarios (timescales, level of performances, cooperation scheme, concept of operations, cybersecurity) which shall involve the platform equipped with the missile and demonstrate the operational interest of the BLOS capability with a stand-alone target designation.

The demonstration of the BLOS capability shall be based on the realisation of one of the proposed scenarios, showing the different technologies involved. Those technologies shall include at least:

- Designation of the target, in terms of coordinates and image, using a UAV adapted to this mission: the flight and functions of the UAV shall be controlled by a specific base, positioned on the battlefield, and related to the platform. The UAV system can use a digital terrain model;
- Transmission of the target coordinates and image by the UAV control base through a cyber-secured data link to the platform (equipped with the missile system and turret) which is not in direct view of the target;
- Reception of the information on the platform which controls the turret in the direction of the target;
- Set up of the missile on the platform, using the target coordinates;
- Firing of the missile;

- Lock on the target by the operator when the missile is in flight, using the image transmitted and the MITL capacity through seeker back-image.

Targeted activities

This proposal shall cover testing, including the following activities:

- Analysis of the different contributors of the BLOS capacity, leading to specify the operational requirements and man-machine interfaces, taking also into account the availability of the associated technologies and products on the market;
- Realisation of interviews with skilled actors of the battlefield: the discussions shall be based on the operational needs and constraints and shall be illustrated using a dedicated missile system simulation environment with MITL and seeker back-image functionality;
- Proposal of a concept of use, illustrated with different scenarios demonstrating the operational advantage brought by the BLOS capacity.
- Choice of the demonstration scenario among those proposed and defined previously;
- Preparation of the scenario in the selected test centre, and associated safety studies;
- Preparation of the platform (vehicle);
- Adaptation and prototyping of the missile system to the platform (turret);
- Adaptation of the UAV, in particular interfaces for data transmission;
- Functional validation of the whole system;
- Availability of two missiles (one spare);
- Realization of the demonstration with a live firing.

Main high-level requirements

The main operational requirements for this action are the following:

- The system shall have the capacity to be operable day and night;
- The system shall have an operational range up to 5 km;
- The system shall be easily adapted to allow the firing demonstration;
- The UAV shall have the capability to design a target, in terms of coordinates in the referential common to the platform with the required accuracy;
- The UAV shall be independent, as an objective, from a GNSS[58] system;
- The UAV data link shall be cyber robust (to its control base), the cyber aspects being fully controlled by Member States;
- The missile shall have the capability to fire on visible and non-visible targets using target coordinates and associated image;
- The missile shall have a back-image capability to lock on the target during flight on operator action in the platform;
- The technologies and components of the system shall be built with a European design authority, must not contain any IPR generated outside Europe and must be free of any third party control regime;

[58] Global Navigation Satellite System.

- The firing demonstration shall be carried out in suitable European Union test centre, allowing for proving the BLOS capability with the stand-alone target designation[59] of the system;
- The system shall be able to fulfil the firing range's safety requirements;
- The experimental devices associated to the firing demonstration shall be able to record the relevant characteristics of the firing / engagement sequences (data links communications between the different units, impact precision of the missile on target, back image from the missile seeker through data link, *etc.*);
- The live firings results shall be compared with the simulation of the missile system with MITL capability.

Budget

The Union is considering an EDIDP funding of up to EUR 6 500 000 to support proposals addressing the above-mentioned topic and its specific challenge, scope, targeted activities and main high-level requirements.

Expected impact

The expected impact of this action for the Member States should be:

- Contribution to excellence with the demonstration of a significant advantage over existing defence products or technologies;
- Contribution to innovation through the application of technologies or concepts previously not applied in the defence sector;
- Contribution to competitiveness by creating new market opportunities;
- Contribution to the security and defence interests of Europe and to industrial autonomy;
- Contribution to increased interoperability and potential European standards.

[59] The target designation is made by the operator of the missile system.

2.7. Call EDIDP-ACC-2019 – Air combat capabilities

Air superiority is a key factor for European armed forces to defend European territory and citizens as well as to respond in more remote geographical areas. The Capability Development Plan (CDP) analysis highlights the importance of developing the suppression of enemy air defence capability, the need to integrate and combine manned and unmanned platforms in a larger operational system, the need for airborne electronic attack capabilities, the ability to carry out deep strikes as well as upgrading or developing next generation attack helicopters, including self-protection systems for fixed and rotary wing aircraft. The CDP long-term capability analysis also identifies the need to ensure overmatch in air-to-air engagements, including against fully autonomous Unmanned Combat Air Vehicles (UCAVs) and to penetrate adversary-controlled airspace to achieve the desired air supremacy.

Proposals are invited against any of the following topics

- **EDIDP-ACC-AEAC-2019:** Airborne electronic attack capability;
- **EDIDP-ACC-CJTP-2019:** Combat jet training platforms;

Budget

The Union is considering contribution of up to EUR 12 000 000 to support proposals addressing any of the above-mentioned topics and their associated specific challenge, scope, targeted activities and main high-level requirements.

Several actions, addressing different topics, may be funded under this call.

2.7.1. Topic EDIDP-ACC-AEAC-2019 – Airborne electronic attack capability

This topic intends to develop a system in pod to be used by EU air platforms in contested electromagnetic environment. Interoperability and cross-domain operations shall be part of the solution.

Specific challenge

The proliferation of advanced long-range Integrated Air Defence Systems (IADS), incorporating threats that can operate across different frequency bands and attack aircraft at ranges up to 400 km, could create Anti Access/Area Denial (A2/AD) areas. In such A2/AD areas, air power cannot operate or be projected in case of conflict. In particular, access to large swaths of territory over EU nation's airspace could be denied in case of a conflict. The only effective way for Europe to counteract these air defence means is to have a capability of Airborne Electronic Attack (AEA), able to create a safe bubble around the formation of aircrafts.

From the operational perspective, the AEA capability must find, locate and track Electro Magnetic (EM) threats and deliver high power jamming signals in the full Radio Frequency (RF) spectrum used in military operations.

Currently the EU capability in countering these threats is limited to few platforms and, when needed, most of the required capability is provided by NATO allies. The EU Capability Development Plan (CDP) also identifies electronic attack as one of the priority areas for development.

EU therefore needs to catch up with emerging Electronic Warfare (EW) technologies to enable aircrafts to operate into the danger zones created by advanced air defence systems, in order to operate its air power from within its own territories as well as in vital geographical areas.

The EU industries have traditionally been developing advanced capabilities in the field of EW, but not at the level required by an electronic attack system, limiting the strategic autonomy of Europe for this critical capability.

Scope

This topic invites to launch the development a European electronic attack system that will remove the above-mentioned limitations. This capability will allow European and NATO air forces to safely operate within EU territories and to safely project force in other potential areas of operations. The system shall be interoperable with the existing and planned Member States assets and in cross-domain operations.

Proposals shall address design, development and testing of an escort/modified escort-jamming capability that will be based on state-of-the-art existing technological cores at European industries level.

The system should follow a modular development approach, being pod mounted in order to be compatible with different aircrafts of interest for the Member States (manned and unmanned).

The Electronic Attack pod mounted system shall implement a highly efficient phased array based jamming system with powerful, efficient and wideband Gallium-Nitride (GaN) technology.

The goal of the system is to enable a platform for Airborne Electronic Attack (AEA) missions that could adapt to the latest in EW requirements, which include (soft) suppression of enemy air defences, escort/modified-escort role, non-traditional electronic attack, self-protected/time-critical strike support, and continuous capability enhancement.
Such features shall rely on the ability to locate, record, replay, and jam hostile communications while tracking across an extremely broad frequency range. Maintaining the ability to communicate with allied forces while operating jamming electronics is another critical requirement.
The escort system would be able to mask an entire fleet of airships from a medium to long range.
The system shall be designed to break the acquisition cycle of radar installations since the search or early-warning phase of detection. S-band radar installations are the threat most often considered, as they are used in most Surface-to-Air Missile (SAM) systems and other Anti-Access/Area Denial (A2/AD) systems.
The presence of threats in the Ultra-High-Frequency (UHF) to X-band range, and their spread in operational frequency and instantaneous bandwidth shall also be considered.

Targeted activities

The proposals shall cover at least:

- Concept of operations (CONOPS) definition, system specification, Detailed Requirements Review (DRR) and architecture definition.
- Detailed design of the pod air system, including the Preliminary Design Review (PDR) and Critical Design Review (CDR).

The proposals could also include the development of small-scale technological demonstrators in order to support decision making during the design phase.
The project will take into account specific requirements from Member States associated to each of the selected air vehicle platforms, in order to perform a design compatible with them, up to the maximum extent possible.
A detailed planning of the subsequent project phases shall be generated, including the identification of implementation priorities according to operational needs of the Union and Member States. Subsequent phases up to operational readiness shall include in particular: prototypes development, qualification and test activities, to reach incremental operational capabilities.

Main high-level requirements

The proposed system shall be based on a phased array architecture with full 360° EW support capability. The system will use the electronic scan nature of this architecture to contend with numerous radar systems.
The proposed system shall have very high ERP[60] effective in all radar polarizations to perform standoff jamming and escort jamming. The frequency coverage shall be valid for electronic attack against air surveillance, target tracker, target indication airborne or ground radars.

[60] Effective Radiated Power.

The waveforms generation by the system shall be able to perform any radar waveform including continuous wave signals.
The system shall be able to detect and perform tracking passively against any radar emission.
The system shall be able to generate waveforms to perform deception to these radars. Specifically, the system will focus in the capability of reprogramming waveforms to adapt to existing and future threats. An effective air operation can need the use of close-in jamming actions by means of UAV (RPAS) swarms. The system shall be able to control the electronic attack operation of the swarm so performing coordinated electronic attacks. The capability to deliver cyber payload shall also be taken into consideration.
At the same time, the system will increase back-end system capability with highly sophisticated computer control along with rapid re-programmability and all EW managing functions.
The system shall offer additional unconventional functionalities: coordinated electronic attack (*i.e.* cooperative jamming) and precise geolocation and targeting.

Expected impact

- To develop a European electronic attack capability at system level operable from air vehicles. This capability would allow EU air forces to conduct operations in contested EM environment, to deal with low-frequency radars and to counter new sophisticated threats;
- To identify and assure that all key strategic components for this capability are under the sovereignty of EU industry;
- To contribute to the development and competitiveness of EU industries worldwide by incorporating key EW components and systems currently leaded in the market by non-EU industries. To minimize the design and development efforts that would need to be spent separately by EU industries and, consequently, to allow these industries to sooner reach the market and satisfy the requirements of Member States' armed forces in the field of electronic attack;
- To increase commonality on EW systems, in the area of electronic attack, along the Member States' armed forces, by joining efforts on this area.

2.7.2. Topic EDIDP-ACC-CJTP-2019 – Combat Jet Training Platforms

This topic intends to develop the next generation of Combat Jet Training Platforms (CJTP).

Specific challenge

Air forces are currently using several training platforms. EU based jet pilot training is a key condition to ensure high-level combat-operational readiness within Member States using the latest and cost-effective training systems.

The development of a joint combat jet training platform with at least two Member States will retain EU independence, reduce cost and training lead time of the next generation of European jet pilots.

Scope

Proposals shall address the development of a modern and effective trainer designed as a unified, comprehensive training system for modern air forces. Proposals shall in particular cover:

- Development of Integrated Training Solution (ITS);
- Application of the latest technologies and equipment especially widely applied simulation technologies;
- Elaboration of a new jet pilot training concept;
- Contribution to the enhancement of Member States' TAFs air offensive and defensive operational capabilities by providing better quality of training from the very beginning;
- Development of the aircraft in order to ensure the capability to operate as light combat aircraft as secondary role.

Targeted activities

The proposals shall cover the following phases of the development of the Combat Jet Training Platforms (CJTP):

- Development of next generation CJTP;
- Development of the Integrated Training System (ITS);
- Testing, qualification and certification.

Main high-level requirements

- Development of synthetic ground based training (including full mission simulator and part task trainer);
- Development of computer based training with support of augmented reality;
- Development of integrated environment for mission planning and learning management system;
- Development of Live, Virtual, and Constructive (LVC) training environment;
- Development of the aircraft in order to ensure the capability to operate as light combat aircraft as secondary role;
- Development of fuel management system;

- Development of flight control system;
- Development of On-Board Oxygen Generating System (OBOGS);
- Flight testing system integration;
- Flight testing virtual training system;
- Flight testing aircraft weapons system integration.

Expected impact

- State-of-the-art and cost-effective joint European military jet pilot training;
- Faster and smooth jet pilot adaptation for current and future generation military aircraft;
- More effective training of all air forces personnel, including GSI (Ground Surveillance Intercept), FAC (Forward Air Controllers);
- Training for all training phases from basic up to LIFT (Lead In Fighter Training);
- Strong involvement of Member States, SMEs and midcaps.

2.8. Call EDIDP-FNPRT-2019 – Future naval platforms and related technologies

Naval power superiority is a key factor for the European armed forces to defend European territory and citizens as well as to enable power projection in more remote geographical areas. Evolving operational environment and threats require the development of the next generation naval platforms and their related systems. As such, ensuring surface superiority is a priority in the Capability Development Plan (CDP). The increasing diversity and evolution of operational threats (such as asymmetric warfare, swarming, surface and/or high speed air threats, wider proliferation of anti-ship missiles) as well as new threats (like hypersonic weapons or anti-ship ballistic missiles), require new naval defence capabilities supported by risk assessment. Additionally, the expanding operational environment (*e.g.* the Arctic) as well as environmental legislation require the development of the next generation naval systems and tactics to ensure surface superiority in the Anti-Air Warfare (AAW), Anti-Surface Warfare (ASuW) and Anti-Submarine Warfare (ASW) domains.

Proposals are invited against the following topic

EDIDP-FNPRT-2019: Naval platform technologies for defence purposes, including those able to operate in extreme climates and geographical environments.

Specific challenges

The fast-changing geo-political situation, as well as the evolving operational context, drives future capability needs. In addition to the past decade's focus on peacekeeping, anti-piracy and patrol operation, navies will also have to operate again in the upper end of the spectrum in terms of threat and intensity, to sail in more remote and extended areas and reduce the need of highly skilled embedded crews. This translates into:

- Stronger emphasis on detectability, survivability, perseverance and battle hardening;
- Capabilities to sail and operate in more demanding conditions, in particular extreme climates both tropic and arctic;
- Worldwide operation and permanent protection of the exploitation of marine resources and sea lines of communication against all kind of threats;
- Sea-basing at a large scale;
- Increased adaptability to different mission-profiles both in a solo role or as part of a flotilla;
- Reduced crew ship operation through autonomy and automation;
- Increased operational availability of naval assets;
- Emphasis on emission reductions and energy efficiency improvements;
- Integration of new weapon systems against new short or long-range threats and targets.

The first challenge in developing a new generation of naval vessels is not the concept itself but the development of technologies that once integrated form the essence of the concept. This requires common feasibility studies to evaluate the state-of-the-art, the potential and the impact of integrating such technologies on a platform and its payload.

With several Member States currently undergoing replacement programmes for their navies, the results of the study should lay ground for the development of recommendations about potential building blocks within the European Defence Fund and/or at national level.

Scope

To address these challenges, the study should be structured around the investigation of the potential impact of a number of existing as well as future systems and technologies on the performance of a naval platform, in a high-level threat environment (surface and subsurface).
New development are relevant, such as those having a high impact on capabilities to conduct missions and to increase adaptability to different mission-profiles; detectability; survivability against modern threats; ship-motion control; electric power generation and storage; capability to operate in extreme climates; increased autonomy & automation and connectivity to sea port.
The feasibility study should recommend a number of game-changing developments in the framework of EDF, to bring the TRL[61] and SRL[62] level of the block to its maximum.

Targeted activities

The proposals shall cover a study over a period of maximum 30 months.

Main high-level requirements

Based on the CDP recommendation, the feasibility study shall address the following issues:

- **Lower detectability**

The level at which a naval platform is detectable by adversaries is a major consideration when confronted by those adversaries.
The study shall address to what extent ship signatures can be further reduced or augmented compared to today's levels and/or camouflaged in order both to minimize detectability and improve effectiveness of own sensors and soft kill measures. Signature management in off-design conditions shall be addressed too.
Solutions to make the vessel invisible for radar (RCS[63]), to mitigate the effect of the earth magnetic field, radiated noise, infrared and other energy sources shall be studied as well as measures to improve the stealth capability against interrogating acoustic, electromagnetic and hydrodynamic sensor systems. Solutions for signature modelling shall be studied as well.

- **Higher survivability against modern surface and subsurface threats including against high-speed threats and swarming threats**

Ultimately, the cheapest way to strengthen our defence is to prolong the use and survivability of a naval weapon-system in a confrontation. A focus on technologies also applicable for on service ships will be specifically considered
The study shall look into solutions for:

  - Improved redundancy, protection and damage containment;

[61] Technology Readiness Level.
[62] System Readiness Level.
[63] Radar Cross Section.

- Blast and shock tolerant structures;
- Capability to recover lost fighting / sailing / floating capabilities (reconfiguration, self-mending / healing systems);
- New advanced and light weight armoured materials (active armouring, ceramic armouring, protection against RPG7-like anti-tank rocket-propelled grenade launcher, in particular for bridge protection);
- Innovative lay-outs;

The study shall also take into account the latest developments in future weapon systems and sensors including the effect it will have on the development of the platform solutions.

- **Reduction of ship motions**

Operations with helicopters, UAV/USV[64] and UUV[65] systems are limited to a window set by ship motions. Solutions are multi-faceted and offer a lot of potential improvements.
New developments offer new opportunities to control ship motion in all direction and thus extend the use of the above-mentioned systems. The following developments shall be addressed:

- Naval architecture: identify architecture options for hull shapes and appendages, allowing gains in sea keeping and minimizing vertical accelerations;
- Improvement of stabilization: new stabilization modes (mobile mass, active foils...);
- Operation in higher sea states;
- Use of prediction: measuring and calculating waves in advance and evaluating their impact, motion sensors;
- Interactions with other systems: UxS[66], aircraft, small vessels;
- Human factors: improve crew working condition to operate the ship (aided system for environment perception like artificial horizon, systems reducing impact of motion, *etc*.).

The study shall investigate the potential of these (combined) developments for frigate sized platforms and formulate required further steps.

- **Improved electric power generation and storage**

Innovative solutions to cater for a new generation of energy-demanding weapons such as laser and electro-magnetic guns, as well as to comply with the requirements of environmental legislation, will be necessary.
The study shall look into the potential of energy efficiency improvements, and their impacts and integration challenges of the use and development of alternative fuels, fuel cells, batteries, supercapacitors, sustainable sources, LED [67] sources smart electric power distribution: "NAVAL GRID" (modelling – simulation), new power to thrust conversion systems and new materials / improved yields.

[64] Unmanned Air Vehicle/Unmanned Surface vehicle.
[65] Unmanned Underwater Vehicle.
[66] Unmanned Systems.
[67] Light-Emitting Diode.

- **Capability to operate in extreme climates**

Taking into account the changing political importance of remote geographical areas as well as the effects caused by climate change in terms of more extreme weather conditions and the access to so far closed-off areas (artic, ant-artic) future naval systems design will face additional requirements such as:

  - Ice strengthening;
  - More stringent requirements for on-board platform systems : air-conditioning, lower operating temperatures, *etc*.;
  - Insulation.

- **Topside**

The purpose is to study topside technologies in order to cover permanently around 360° and to use simultaneously all integrated sensors and radiating effectors. The main topics are:

  - Analyse and evaluate innovative antenna technologies (meta materials, ferro fluid, plasma…);
  - Identify and evaluate design and validation EMC[68] tools for integrated topside;
  - Feasibility study for topside functional and physical integration (interface standardization);
  - Analyse the feasibility of topside functional ship wall.

- **Increased autonomy and automation**

To enable further crew reduction and autonomy at system level, the study shall also address the technologies and systems relevant to damage control, firefighting, replenishment at sea, close proximity manoeuvres.

Budget

The Union is considering a contribution of up to EUR 14 500 000 to support proposals addressing the above-mentioned topic and its specific challenges, scope, targeted activities and main high-level requirements.

Expected impact

The feasibility study results shall:

- Set up a common definition to identify future naval systems and technologies;
- Define the state-of-the-art of the identified naval systems and technologies;
- Deliver an analysis of the potential improvements, impacts and related cost of their integration into a surface or subsurface platform;
- Develop concrete requirement to enable further development and their successful integration on-board future naval platforms;
- Elaborate concrete recommendation and proposals for further development programmes, within the EU or national frameworks.

[68] Electromagnetic Compatibility.

2.9. Call EDIDP-SME-2019 – Innovative and future-oriented defence solutions

The development of innovative and future-oriented defence products and technologies relies on the innovation capacity of Small and Medium-sized Enterprises (SMEs). This call for proposals targets innovative defence products, solutions and technologies and is devoted to SMEs.

Proposals are invited against the following topic

EDIDP-SME-2019: Innovative defence products, solutions, materials and technologies, including those that can create a disruptive effect and improve readiness, deployability, reliability, safety and sustainability of EU forces in all spectrum of tasks and missions, for example in terms of operations, equipment, infrastructure, basing, energy solutions, new surveillance systems

Specific challenge

This category encourages the driving role of SMEs in bringing forward innovation, agility and ability to adapt technologies from civil to defence applications, to turn technology and research results into products in a fast and cost-efficient way.

Scope

Proposals shall address innovative defence products, solutions and technologies, including those that can create a disruptive effect and improve readiness, deployability and sustainability of EU forces in all spectrum of tasks and missions, for example in terms of operations, equipment, basing, energy solutions, new surveillance systems. Proposals could address any subject of interest for defence, such as, but not limited to, the following:

- Cybersecurity solutions for the protection of the future security and defence systems (command and control, logistics, embedded systems, distributed simulation…);
- Future compounds/smart basing technologies development;
- Development of innovative methods or methodologies for comprehensive technical requirements setting such as concurrent design;
- Future Mine Counter Measures (MCM) capabilities operating autonomous underwater systems, coping with current capability gaps in securing Sea Lines of Communication;
- Integrated maritime surveillance system, combining legacy assets with new, innovative solutions;
- Portable bacteriological and chemical future detection systems;
- Future soldier CBRN (Chemical, Biological, Radiological and Nuclear) protection equipment and integration;
- Innovative intelligence tools for early warning and countermeasure deployment support to counter CBRN threats;
- Wearable orthosis equipment and exoskeletons to increase strength capabilities and minimize stress of future soldiers;

- Autonomous and remote-controlled unmanned systems for safe medical evacuation of injured soldiers during military operations;
- End-to-end solutions for artificial intelligence in defence & security key strategic issues;
- Command and control systems designated for individual soldier-squad up to brigade Command, post logistic information system for maintenance, transport, medical, management;
- Armoured medium and light vehicle;
- Tactical logistic trucks;
- Protected, cooled and connected shelter solutions for fixed and mobile command post for EU operations;
- Future effective and collective CBRN protection capacity to civil population, military and their equipment;
- Mobility support deployable solution for amphibious and airmobile (helicopter) operations;
- Innovative battery for future infantry portable system (radio set, optronic, *etc.*) and for weapon system (missile) ignition;
- Innovative solutions (bio-based) for fuel production from organic waste to support military operations and energy self-sufficiency in remote areas;
- Innovative passive systems (solar-tracking) systems for energy production based on renewable sources to support military operations in remote areas;
- Innovative software systems for processing of aerial images and videos through hyperspectral imaging (for metadata/telemetry information extraction and exploitation in C2 systems);
- Integrated management system for assets and services required in emergency situations in the framework of UE defence operations, in order to increase sustainability of EU forces;
- Nanomodified composite materials and related production processes and design procedures for reinforcement of existing armours of military vehicles;
- Development of a minefields mapping system using unmanned aircraft;
- High capacity communications for UAVs (Unmanned Air Vehicles) in beyond line-of-sight applications;
- Medical virtual reality training simulator;
- Unmanned semi-fixed sea platforms;
- Additive manufacturing enhancing the logistic performance by provide to military end-users possibilities to produce spare parts using additive manufacturing solutions, particularly in the context of overseas operations;
- European glider operational and oceanographic data acquisition Centre: Establishing a proof of concept of an underwater oceanographic data assembly centre;
- Development of counter-UAS (Unmanned Air System) capability based on mini-UAS swarms;

- Secure high capacity communications for UAVs in beyond line-of-sight applications;
- Augmented-reality combat helmet featuring night-vision and ally or enemy position display, including artificial intelligence functionalities;
- Intelligent, dynamic and robust control of the quality of service in hybrid satellite-terrestrial telecommunication networks.

Targeted activities

Proposals shall cover any kind of activities listed in Article 6(1) of the EDIDP regulation:

- Study;
- Design;
- System prototyping;
- Testing;
- Qualification;
- Certification;
- Development of technologies or assets increasing efficiency across the life cycle of defence products and technologies.

Given the importance of time-to-market for SMEs, proposals are expected to cover more than only studies or design.

Budget

The Union is considering a contribution of up to EUR 7 500 000 to support proposals addressing any subject of interest for defence.

Several actions, addressing different defence products, solutions, materials and technologies, may be funded under this call.

Expected impact

- Innovative, rapid and cost-effective solutions for defence applications;
- Ground-breaking or novel concepts and approaches, new promising future technological improvements or the application of technologies or concepts previously not applied in the defence sector;
- Building innovation capacity across Europe by involvement of SMEs that can make a difference in the future;
- Potential for future market creation for SMEs.

3. Conditions for the calls

The following section provides all the necessary conditions to submit proposals in response to the calls described in section 2.

3.1. Opening dates, final date for submission and indicative budgets[69]

Calls	Topics	Budgets in EUR (2019)	Opening date	Final date for submission
EDIDP-MUGS-2019	EDIDP-MUGS-2019	Up to 30 600 000	4 April 2019	29 August 2019
EDIDP-ISR-2019	EDIDP-ISR-TRPAS-2019	Up to 43 700 000	4 April 2019	29 August 2019
	EDIDP-ISR-DAA-2019			
	EDIDP-ISR-EHAPS-2019			
	EDIDP-ISR-PEO-2019			
EDIDP-CSAMN-2019	EDIDP-CSAMN-SDN-2019	Up to 17 700 000	4 April 2019	29 August 2019
	EDIDP-CSAMN-SSC-2019			
	EDIDP-CSAMN-SSS-2019			
EDIDP-PNTSCC-2019	EDIDP-PNTSCC-PNT-2019	Up to 44 100 000	4 April 2019	29 August 2019
	EDIDP-PNTSCC-SCC-2019			
EDIDP-ESC2S-2019	EDIDP-ESC2S-2019	Up to 20 000 000	4 April 2019	29 August 2019
EDIDP-NGPSC-2019	EDIDP-NGPSC-2019	Up to 6 500 000	4 April 2019	29 August 2019
EDIDP-ACC-2019	EDIDP-ACC-AEAC-2019	Up to 12 000 000	4 April 2019	29 August 2019
	EDIDP-ACC-CJTP-2019			
EDIDP-FNPRT-2019	EDIDP-FNPRT-2019	Up to 14 500 000	4 April 2019	29 August 2019
EDIDP-SME-2019	EDIDP-SME-2019	Up to 7 500 000	4 April 2019	29 August 2019

[69] The authorising officer by delegation responsible for the call may decide to open the call up to one month after the envisaged opening date.
The authorising officer by delegation responsible for the call may delay the final date for submission by up to two months.
All deadlines are at 12:00:00 Brussels local time.

3.2. Admissibility conditions

The proposals submitted following the call for proposals shall fulfil the following admissibility conditions:

- Applicants shall submit their proposal in one of the official languages of the Union (English language is encouraged), using the submission form template available here.
- The submission form shall be duly completed. *Applicants may usefully refer to the guide for applicants (available here) to do so.*
- One proposal shall only be submitted against one topic.
    - Where a call is covering several topics (EDIDP-ISR-2019, EDIDP-CSAMN-2019, EDIDP-PNTSCC-2019 and EDIDP-ACC-2019), one proposal shall only address one topic of this call.
    - Proposals in response to the call EDIDP-SME-2019 shall address one clearly identified product, solution, material or technology which is of interest for defence. The provided list of subjects inside the call text is only indicative.
- All proposals shall be provided in an electronic version in a searchable[70] pdf format on a USB stick or a CD-ROM. In addition to this electronic version, applicants are allowed to submit a paper copy. In case of discrepancies between the electronic and paper copies, the electronic copy will be the reference.
- All proposals shall be readable, accessible and printable.
- Proposals shall be submitted before the final date for submission (evidence of timely delivery) specified in the table above.
- Proposals shall be submitted according to one of the following options:
    - Option a: **sent by registered mail** (date of postmark serving as evidence of timely delivery) to the following address:

European Commission *Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs* *EDIDP Call 2019* *Unit I.4* *Office address: BREY 09/028* *B-1049 Brussels, Belgium*

    - Option b: **sent by courier services** (date of deposit slip serving as evidence of timely delivery) to the same address as in option c.
    - Option c: **delivered by hand,** in person or by an authorised representative (date of acknowledgement of receipt by the Commission serving as evidence of timely delivery) to the following address:

European Commission *Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs* *EDIDP Call 2019* *Unit I.4* *Office address: BREY 09/028* *Service central de réception du courrier*

[70] Scan pdf is also accepted for signed supporting documents.

Avenue du Bourget, 1-3 *B-1140 Bruxelles, Belgique*

Failure to comply with those conditions will lead to rejection of the proposal.

If the applicants deem necessary to include classified information in their proposal, they shall contact the Commission at the following email address (EC-EDIDP-proposals@ec.europa.eu) well before the final date for submission of the call, in order to arrange the delivery of their proposal.

3.3. Duration of the action

Duration of the proposed action shall not exceed six years. Duration of the proposed action is not expected to exceed four years, unless duly justified in the proposal.

3.4. Evaluation procedure and conditions

The admissible proposals will be evaluated by the Commission on the basis of the procedure and conditions described below.

3.4.1. Procedure

The evaluation of the proposals will be performed by the Commission following a multi-stage procedure:

- Stage 1 will consist in determining if the proposal falls under exclusion grounds.
  Proposals which fall under exclusion grounds will be rejected.
- Stage 2 will consist in assessing the proposal against eligibility criteria:
  - Eligibility of the proposed action;
  - Eligibility of the entities involved in the action.

  Proposals which fail to meet any of the eligibility criteria will be rejected.
- Stage 3 will consist in assessing the proposal against selection criteria:
  - Financial capacity of the applicants;
  - Operational capacity of the applicants.

  Proposals which fail to meet any of the selection criteria will be rejected.
- Stage 4, for which the Commission will be assisted by independent experts, will consist in an assessment of the proposal against the award criteria, resulting in a scoring of the proposal.
- Stage 5 will consist in establishing a ranking list (selected proposals and reserve list) of the assessed proposals for each call, and request the positive opinion of the Programme Committee of Member States on the selected proposals.
- Stage 6 will consist in the adoption of the award decision by the Commission, following the positive opinion of the Programme Committee of Member States.

- Stage 7 will consist in inviting coordinators of winning consortia to start the grant agreement reparation: negotiation and signature of the grant agreement by or in the name and on behalf of the Commission.

3.4.2. Indicative timetable for evaluation and grant agreement signature

Information on the outcome of the evaluation: maximum six months from the final date for submission.
Indicative date for the signing of grant agreements: maximum three months from the date of informing successful applicants.

3.4.3. Exclusion criteria

The objective of the exclusion criteria is to specify the cases in which applicants shall be excluded from participating in the call procedure or from being awarded a grant.
These situations are described in Article 136 of the Financial Regulation. They include bankruptcy, grave professional misconduct, non-compliance with social or tax obligations, involvement in a criminal organisation, money laundering or any other illegal activity.
Applicants shall declare on their honour that they are not in one of the situations of exclusion referred to above. To this effect, a declaration on honour shall be included in the grant application to be signed by all applicants.
Depending on a risk assessment, the successful applicants may be requested to provide further evidence to demonstrate that they do not fall under the exclusion criteria.
However, the authorising officer responsible shall waive the obligation for an applicant to submit evidence, when such evidence has already been submitted for the purposes of another grant or procurement procedure, provided that the documents are not more than one year old and the applicant confirms that they are still valid.

3.4.4. Eligibility criteria

Assessment against eligibility criteria will be performed based on evidence the applicants shall provide at the time of the submission of their proposal (*see relevant section of the guide for applicants for example of expected evidence against each criteria*).
The eligibility criteria fall into two types:

- Eligibility criteria for the proposed action;
- Eligibility criteria for the entities involved in the action.

The eligibility criteria are listed below.

Proposals that will fail to meet any of these eligibility criteria will be rejected.

In the event of a change during the carrying out of the action which might put into question the fulfilment of the eligibility criteria, the undertaking shall inform the Commission, which shall assess whether the eligibility criteria continue to be met and shall address the potential impact on the funding of the action.

a. Eligibility criteria for the proposed action

- The action shall address the development phase of new defence products and technologies and/or the upgrade of existing products and technologies;
- Where addressing upgrade, the use of pre-existing information needed to carry out the action shall not be subject to a restriction by a third country or by a third-country entity, directly, or indirectly through one or more intermediary undertakings;
- The action shall only address one or more of the following activities:

  (a) studies, such as feasibility studies, and other accompanying measures;

  (b) the design of a defence product, tangible or intangible component or technology as well as the technical specifications on which such design has been developed, including partial tests for risk reduction in an industrial or representative environment;

  (c) the system prototyping of a defence product, tangible or intangible component or technology;

  (d) the testing of a defence product, tangible or intangible component or technology;

  (e) the qualification of a defence product, tangible or intangible component or technology;

  (f) the certification of a defence product, tangible or intangible component or technology;

  (g) the development of technologies or assets increasing efficiency across the life cycle of defence products and technologies.
- The action shall be carried out by undertakings cooperating within a consortium of at least three eligible entities which are established in at least three different Member States.
- At least three of those eligible entities established in at least two different Member States shall not be controlled, directly or indirectly, by the same entity or shall not control each other.
- The above-mentioned consortium shall offer proof of viability by demonstrating that the costs of the action that are not covered by Union support are to be covered by other means of financing, such as by Member States' contributions.
- With regard to actions addressing activities (c), (d), (e), (f) or (g), the consortium shall provide proof of their contribution to the competitiveness of the European defence industry by demonstrating that at least two Member States intend to procure the final product or to use the technology in a coordinated way, including through joint procurement where applicable.
- Actions addressing activity (b) shall be based on common requirements jointly agreed by at least two Member States.
- Actions addressing activities (c), (d), (e), (f) or (g), shall be based on common technical specifications jointly agreed by the Member States that are to co-finance or that intend to jointly procure the final product or to jointly use the technology, as referred above, thereby strengthening the standardisation and interoperability of systems.

- Actions for the development of products and technologies the use, development or production of which is prohibited by international law shall not be eligible for funding.
- A proposal will only be considered eligible if its content corresponds to the topic description against which it is submitted.
- The results of actions which receive funding under the Programme shall not be subject to control or restriction by a third country or by a third-country entity, directly, or indirectly through one or more intermediate undertakings, including in terms of technology transfer.

b. Eligibility criteria for the entities involved in the action

In this sub-section, 'subcontractors involved in the action' refers to subcontractors with a direct contractual relationship to a beneficiary, other subcontractors to which at least 10 % of the total eligible cost of the action is allocated, as well as subcontractors which may require access to classified information in order to carry out the contract.

- Beneficiaries and subcontractors involved in the action shall be public or private undertakings established in the Union.
- The infrastructure, facilities, assets and resources of the beneficiaries and subcontractors involved in the action which are used for the purposes of the actions funded under the Programme shall be located on the territory of the Union for the entire duration of the action, and their executive management structures shall be established in the Union.
- Where no competitive substitutes are readily available in the Union, beneficiaries and subcontractors involved in the action may use their assets, infrastructure, facilities and resources located or held outside the territory of Member States provided that that usage does not contravene the security and defence interests of the Union and its Member States, is consistent with the objectives of EDIDP (Article 3 of the EDIDP Regulation) and the provisions on ownership and intellectual property rights (Article 12 of the EDIDP Regulation). **The costs related to those activities will not be eligible for funding under the Programme.**
- For the purposes of the actions funded, the beneficiaries and subcontractors involved in the action shall not be subject to control by a third country or by a third-country entity.
    - By derogation from this condition, an undertaking established in the Union and controlled by a third country or by a third-country entity shall be eligible as a beneficiary or subcontractor involved in the action only if guarantees approved by the Member State in which it is established in accordance with its national procedures are made available to the Commission. Those guarantees may refer to the undertaking's executive management structure established in the Union. If deemed to be appropriate by the Member State in which the undertaking is established, those guarantees may also refer to specific governmental rights in the control over the undertaking. The guarantees shall provide the assurances that the involvement in an action of such an undertaking would not contravene the security and defence interests of the Union and its Member States, as established in the framework of the Common Foreign and Security Policy pursuant to Title V of the TEU, or the objectives set out in Article 3 of the

EDIDP Regulation. The guarantees shall also comply with the provisions on ownership and intellectual property rights (Article 12 of the EDIDP Regulation). The guarantees shall in particular substantiate that, for the purpose of the action, measures are in place to ensure that:

- control over the undertaking is not exercised in a manner that restrains or restricts its ability to carry out the action and to deliver results, that imposes restrictions concerning its infrastructure, facilities, assets, resources, intellectual property or know-how needed for the purpose of the action, or that undermines its capabilities and standards necessary to carry out the action;
- access by a third country or by a third-country entity to sensitive information relating to the action is prevented and the employees or other persons involved in the action have national security clearances, where appropriate;
- ownership of the intellectual property arising from, and the results of, the action remain within the beneficiary during and after completion of the action, are not subject to control or restriction by a third country or by a third-country entity, and are not exported outside the Union nor is access to them from outside the Union granted without the approval of the Member State in which the undertaking is established and in accordance with the objectives set out in Article 3 of the EDIDP Regulation.

If deemed to be appropriate by the Member State in which the undertaking is established, additional guarantees may be provided.

- When carrying out an eligible action, beneficiaries and subcontractors involved in the action may also cooperate with undertakings established outside the territory of Member States or controlled by a third country or by a third-country entity, including by using the assets, infrastructure, facilities and resources of such undertakings, provided that this does not contravene the security and defence interests of the Union and its Member States. Such cooperation shall be consistent with the objectives of EDIDP (Article 3 of the EDIDP Regulation) and shall be fully in line with the provisions on ownership and intellectual property rights (Article 12 of the EDIDP Regulation). There shall be no unauthorised access by a third country or other third-country entity to classified information relating to the carrying out of the action and potential negative effects over security of supply of inputs critical to the action shall be avoided. **The costs related to those activities will not be eligible for funding under the Programme.**

3.4.5. Selection criteria

Selection criteria are intended to assess the applicant's ability to complete the proposed action. Only proposals by applicants who satisfy the selection criteria may be considered for a grant. The necessary ability of the applicants will be assessed under both financial capacity and operational capacity. Proposals which fail to meet the selection criteria will be rejected.

Financial capacity: the applicants shall demonstrate that they have stable and sufficient sources of funding to maintain their activity throughout the duration of the grant and to participate in the funding of the action. This capacity will be verified in particular on the basis of the following supporting documents:

- balance sheet and profit & loss account for the last financial year for which the accounts were closed;
- audit report produced by an approved external auditor certifying the above-mentioned accounts for applicants requesting more than EUR 750 000 of Union financial support.

Where a statutory audit is required by EU or national law, it shall always be submitted. The audit report shall certify the accounts for up to the last three available financial years. Where a statutory audit is not required, the applicant shall provide a self-declaration signed by its authorised representative certifying the validity of its accounts for up to the last three financial years available.

The authorising officer responsible may, depending on a risk assessment, waive the obligation to produce the audit report for education and training establishments. The waiver is also possible in case of agreements with a number of beneficiaries who have accepted joint and several liabilities or who do not bear any financial responsibility.
In particular, supporting documents will not be requested for:

(a) natural persons in receipt of education support;
(b) natural persons most in need and in receipt of direct support;
(c) public bodies including Member State organisations;
(d) international organisations;
(e) persons or entities applying for interest rate rebates and guarantee fee subsidies where the objective of those rebates and subsidies is to reinforce the financial capacity of a beneficiary or to generate an income.

Operational capacity: the applicants shall demonstrate that they have the professional competencies and qualifications required to complete the proposed action. This capacity will be assessed on the basis of information about specific qualifications, professional experience and references in the field concerned, to be provided with the proposal.
Applicants shall in particular provide a declaration on honour as well as the following documents:

- a list of previous projects and activities performed in the area;
- description of the technical equipment, tools or facilities and patents at the disposal of the applicant.

3.4.6. Award criteria and scoring

Each proposal which complies with the admissibility, exclusion, eligibility and selection criteria will be assessed and scored by the Commission, which will be assisted by at least three independent experts against five (for actions covering only feasibility studies and/or design) or six award criteria (for all other actions). The award criteria and the associated

specific items that will be looked at by the experts are listed below and reflected in the submission form.

Criterion 1. Contribution to excellence, in particular by showing that the proposal presents significant advantages over existing defence products or technologies

1.1 Objectives and relation to the call for proposals

- To what extent does the proposal address the specific challenge, scope, targeted activities, main high-level requirements, and expected impact as set out in the call for proposals?
- Are the overall and specific objectives of the proposal, clear, measurable, realistic and achievable within the proposed duration?

1.2 Contribution to excellence

- To what extent does the proposal aim at state-of-the-art solutions and broadens the existing expertise in the domain?
- To what extent does the expected outcome of the action differ from and represent (or will represent in combination with other technologies) an advantage over existing defence products or technologies?
- What is the strategic, technological or operational added value of the expected outcome?

1.3 Contribution to increasing efficiency across the life cycle

- Where relevant, what is the contribution to increasing efficiency across the lifecycle of the expected outcome, including cost-effectiveness (*e.g.* lower production, operational, maintenance, repair and overhaul or disposal costs) and the potential for synergies in the procurement and maintenance process?

1.4 Quality of implementation, organisation and resources

To what extent have the following aspects been taken into account?

- Quality and effectiveness of the work plan, including the extent to which the resources assigned to work packages are in line with their objectives and deliverables;
- Appropriateness of the management structures and procedures, including risk management (identification and mitigation measures envisaged);
- Complementarity of the participants and extent to which the consortium as a whole brings together the necessary expertise and can perform the work with a high level of effectiveness and efficiency;
- Appropriateness of the allocation of tasks, ensuring that all participants have a valid role and adequate resources in the project to fulfil that role.

Criterion 2. Contribution to innovation, in particular by showing that the proposal includes ground-breaking or novel concepts and approaches, new promising future technological improvements or the application of technologies or concepts previously not applied in the defence sector

2.1 Contribution to innovation

- To what extent will the key innovative aspects of the proposal contribute to improving the innovation capacity of the European defence industry? From the European and non-European perspective, does the proposal contain ground-breaking or novel concepts and approaches, new promising future technological improvements or the application of technologies or concepts previously not applied in the defence sector?
- Which are the patents the proposal relies on and which patents are expected to be deposited during the project?

2.2 Potential spin-offs of the technologies

- To what extent could the innovations/technologies to be developed in the proposal spin-off to other defence capabilities?

2.3 Contribution to increasing efficiency across the life cycle

- Where relevant, what is the contribution to increasing efficiency across the lifecycle of the expected outcome, including cost-effectiveness (e.g. lower production, operational, maintenance, repair and overhaul or disposal costs) and the potential for synergies in the procurement and maintenance process?

Criterion 3. Contribution to the competitiveness and growth of defence undertakings throughout the Union, in particular by creating new market opportunities

3.1 Contribution to the competitiveness and growth

- To what extent will the proposal contribute to the improvement of the competitiveness of the European Defence Technological Industrial Base (EDTIB)?
- What impact will the project have on the employment, turnover and investments in the EDTIB?
- To what extent will the products proposed to be developed have a competitive advantage vis-a-vis existing or planned products both within and outside of the Union?

3.2 Market opportunities

- What is the size and the growth potential of the market the proposal addresses?

3.3 Contribution to increasing efficiency across the life cycle

- Where relevant, what is the contribution to increasing efficiency across the lifecycle of the expected outcome, including cost-effectiveness (e.g. lower production, operational, maintenance, repair and overhaul or disposal costs) and the potential for synergies in the procurement and maintenance process?

Criterion 4. Contribution to the industrial autonomy of the European defence industry and to the security and defence interests of the Union by enhancing defence products or technologies in line with defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy, particularly in the context

of the Capability Development Plan, and, where appropriate, regional and international priorities provided that they serve the Union's security and defence interests and do not exclude the possibility of participation of any Member State

4.1 Contribution to the industrial autonomy of the European defence industry and defence interests of the Union

- To what extent will the proposed development of the technologies/capabilities decrease EU industrial and technological dependence from third countries?
- What impact would the proposed activities have on the European security of supply?

4.2 Contribution to the security and defence interests of the Union

- To what extent is the proposal in line with the defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy, particularly in the context of the Capability Development Plan?
- To what extent does the proposal address a regional or an international priority that contributes to the Union's security and defence interests and does not exclude the possibility of participation of any Member State?

Criterion 5. The proportion of the overall budget of the action to be allocated to the participation of SMEs established in the Union bringing industrial or technological added value, as members of the consortium, as subcontractors or as other undertakings in the supply chain, and in particular the proportion of the overall budget of the action to be allocated to SMEs which are established in Member States other than those where the undertakings in the consortium which are not SMEs are established
For the SME category, maximum points for this criterion shall be given.

5.1 Participation of SMEs

- What is the share of the total eligible costs allocated to SMEs (cross-border and non-cross-border) bringing technological added value?
  What is the share of the total eligible costs assigned to cross-border SMEs (SMEs which are established in Member States other than those where the undertakings in the consortium which are not SMEs are established) bringing technological added value?

Criterion 6. For actions covering:

- **the system prototyping of a defence product, tangible or intangible component or technology, or;**
- **the testing of a defence product, tangible or intangible component or technology, or;**
- **the qualification of a defence product, tangible or intangible component or technology, or;**
- **the certification of a defence product, tangible or intangible component or technology, or;**

contribution to the further integration of the European defence industry through the demonstration by the beneficiaries that Member States have committed to jointly use, own or maintain the final product or technology.
This criterion shall be disregarded for actions covering only feasibility studies and/or design.

6.1 Joint commitment of Member States and contribution to the integration of the EU market

- How many Member States have committed to jointly use, own or maintain the final product or technology?
- To what extent do these commitments contribute to further integrating the EU market and increasing the cooperation potential between Member States?

Experts will attribute up to 5 points for each award criterion (half-points will be allowed):

0	The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
1	Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.
2	Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.
3	Good. The proposal addresses the criterion well, but a number of shortcomings are present.
4	Very Good. The proposal addresses the criterion very well, but a small number of shortcomings are present.
5	Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

The score of a proposal will be determined by summing the scores against relevant award criteria, and dividing it by the number of award criteria taken into consideration, meaning that the individual score of a proposal will range from 0 to 5. No weighting will apply.
The final assessment and score of a proposal will result from a consensus of the different experts' outputs. Proposals that will get a final consensus score beneath 3,3 points will be rejected.

3.4.7. Ranking mechanism and award decision

For each call, assessed proposals will be ranked according to their final consensus score.

The proposal with the highest rank will be awarded.
Where a call mentions that several actions may be funded, the next proposals on the ranking list will also be awarded subject to the availability of budget and provided that these proposals address different topics (or different defence products, solutions, materials or technologies for the call EDIDP-SME-2019) from those already awarded.

The following approach will be applied successively for every group of ex aequo proposals requiring prioritisation, starting with the highest scored group, and continuing in descending order:

- Proposals that address topics not otherwise covered by more highly ranked proposals, will be considered to have the highest priority;
- These proposals will themselves be prioritised according to the scores they have been awarded for criterion 1 (contribution to excellence). When these scores are equal, priority will be based on scores for criterion 2 (contribution to innovation).

The Commission will adopt an award decision based on the ranking list (awarded proposals and reserve list) after having consulted the Member States through the EDIDP Programme Committee. The adoption of the award decision will be the starting point for informing the successful applicants and entering into grant agreement preparation (GAP) with the Commission.

For the highest ranked proposals on the reserve list, coordinators will be informed that their proposal may receive funding should budget still be available at the end of the GAP. In such case, they will be invited for negotiation on the scope and budget of their proposal.

3.5. Funding rates

The maximum Union financial support will be calculated according to the mechanism described below. The Union financial support to an awarded proposal in response to one call cannot exceed the indicative budget allocated to this call.

3.5.1. Calculation mechanism

Union funding will be calculated based on the total eligible costs provided and justified by the applicants at the time of submission of the proposal.
Indirect eligible costs shall be determined by applying a flat rate of 25% of the total direct eligible costs, excluding direct eligible costs for subcontracting.
The costs listed in points a) to d) of paragraph 4 of Article 186 of the Financial Regulation will also be considered as eligible.
For more details and definitions of eligible costs, direct and indirect costs and subcontracting, please refer to the relevant sections of the guide for applicants.

The calculation will be performed for each type of activity covered by the proposal (study, design, prototyping, testing…), applying the baseline funding rates as described in Table 1 below and, where conditions are met, the increase (bonus) of the baseline funding rates as described in Table 2 below.
For that purpose, the applicants shall provide and justify eligible costs for each activity, while respecting the following rules:

- an activity may be broken down into several work packages;
- a work package shall only cover one type of activity;

- for horizontal workpackages, if any (*e.g.* maganement), an allocation of the related costs to the different activities shall be provided.

Applicants are invited to refer to the relevant section of the guide for applicants for more details about the information that needs to be provided.

The total Union funding for the awarded action will be determined by adding up the Union funding calculated for each type of activity covered by the action.

3.5.2. Table 1. Funding rates

Activity	Baseline funding rate
Studies, such as feasibility studies, and other accompanying measures	Up to 90% of eligible costs
The design of a defence product, tangible or intangible component or technology as well as the technical specifications on which such design has been developed, including partial tests for risk reduction in an industrial or representative environment	Up to 65% of eligible costs
The system prototyping of a defence product, tangible or intangible component or technology	Up to 20% of eligible costs
The testing of a defence product, tangible or intangible component or technology	Up to 65% of eligible costs
The qualification of a defence product, tangible or intangible component or technology	Up to 65% of eligible costs
The certification of a defence product, tangible or intangible component or technology	Up to 65% of eligible costs
The development of technologies or assets increasing efficiency across the life cycle of defence products and technologies	Up to 65% of eligible costs

3.5.3. Table 2. Cumulative increases in the funding rates listed in Table 1

The overall increase in the funding rate of an action following the application of the increase of funding rates listed in Table 2 shall not exceed 35%. The financial assistance of the Union provided under the Programme including the increased funding rates shall not cover more than 100% of the eligible cost of the action.

Condition to be fulfilled to get the corresponding increase in funding rate	Increase in funding rate
Action developed in the context of the permanent structured cooperation (PESCO)	+ 10%
EU-established SME participation $\frac{\sum Eligible\ Costs\ of\ EU\ SME}{Total\ Eligible\ Costs} \geq 10\%$	$+\frac{\sum Eligible\ Costs\ of\ EU\ non\ crossborder\ SME}{Total\ Eligible\ Costs} * 100\%$ (up to an additional 5%) and $+\frac{\sum Eligible\ Costs\ of\ EU\ crossborder\ SME}{Total\ Eligible\ Costs} * 200\%$
EU-established Mid-cap participation $\frac{\sum Eligible\ Costs\ of\ EU\ MidCap}{Total\ Eligible\ Costs} \geq 15\%$	+ 10%

For the definition of SME, applicants shall refer to EU Recommendation 2003/361[71] or visit the following website:
http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en.

'EU cross-border SMEs' shall be understood as SMEs established in Member States other than those in which the undertakings in the consortium that are not SMEs are established.
'EU non cross-border SMEs' are SMEs established in the Member States in which the undertakings in the consortium that are not SMEs are established.
'Middle-capitalisation company' or 'Mid-cap' means an enterprise that is not a SME and that has up to 3 000 employees, where the staff headcount is calculated in accordance with Articles 3 to 6 of the Annex to Recommendation 2003/361.

The applicability of the bonuses for SME/cross-border SME and mid-cap participation will be determined on the basis of the information provided in Annex I to the submission form.

[71] Commission Recommendation C(2003) 1422 of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124, 20.5.2003, p. 36–41.

3.6. Consortium

Applicants shall set up a consortium and appoint one of them to act as coordinator. The coordinator shall be the principal point of contact between the members of the consortium in relations with the Commission. The coordinator will be identified in the grant agreement.
The members of a consortium participating in an action shall conclude an internal agreement establishing their rights and obligations with respect to the carrying out of the action in accordance with the grant agreement. The internal agreement shall also include arrangements regarding the intellectual property rights relating to the products and technologies developed.

3.7. Grant agreement

For each proposal selected for award, the coordinator of the consortium will be invited to enter grant agreement preparations with the Commission. A model grant agreement is available here.
The Commission may request additional information for the conclusion of the grant, such as those related to financial capacity, costs or legal status of future beneficiaries.
The attention of the applicants is drawn on the following points:

- Where Member States have appointed a project manager to lead the work related to the action that will received Union funding, the Commission shall consult the project manager on the progress achieved in connection with the action before executing the payment to the eligible beneficiaries.
    - In addition to the deliverables identified by the applicants in their proposal, specific periodic reports and a final report will be requested to the consortium in the grant agreement for the purpose of managing the grant. These reports shall include a dedicated chapter containing data necessary for the monitoring and the evaluation of the Programme. The final report shall in particular contain data necessary for the preparation of the evaluation report that the Commission is required to produce in line with the provisions of Article 17(2) of the EDIDP Regulation. This will include, for instance, data on cross-border participation, including of SMEs and mid-caps, in actions carried out under the Programme, as well as the integration of SMEs and mid-caps in the global value chain, information on the countries of origin of the beneficiaries and, where possible, the distribution of the generated intellectual property rights.

3.8. Actions involving the handling of classified information[72]

Pursuant to Commission Decision (EU) 2019/513 of 26 March 2019 on the security framework for the European Defence Industrial Development Programme, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries are established shall decide on the originatorship of the classified foreground information generated in the performance of an action. For that purpose, those Member States may decide on a specific security framework for the protection and

[72] Restricted and above.

handling of classified information relating to the action and shall inform the Commission thereof. Such a security framework shall be without prejudice to the possibility for the Commission to have access to necessary information for the implementation of the action.
If no such specific security framework is set up by those Member States, the security framework will be put in place by the granting authority in accordance with Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information ('Decision 2015/444'). Further details are provided in the Annex to this document.
The applicable security framework for the action has to be in place at the latest before the signature of the grant agreement.

3.9. Additional conditions for the Topic EDIDP-PNTSCC-2019

Under the topic EDIDP-PNTSCC-PNT-2019, applicants shall:

- Be authorised by the Security Accreditation Board in accordance with Article 11(2) of Regulation (EU) No 912/2010; and
- Comply with the decisions of the Security Accreditation Board and with the Commission delegated decision C(2015)6123.

For this purpose, the applicants shall provide a confirmation of authorisation and of compliance issued by their Competent PRS Authority as provided under Article 5(1) of the Decision No 1104/2011/EU.

3.10. Additional conditions for the call EDIDP-SME-2019

The consortium applying for funding under call EDIDP-SME-2019 shall be composed of small and medium-sized enterprises (SMEs) only. SMEs shall be understood as defined in EU Recommendation 2003/361.
Applicants who want to know if they are SMEs according to this Recommendation are invited to visit the following website:
http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en.

Non-SMEs can participate in the action but cannot be part of the consortium.
Please refer to the relevant section of the guide for applicants for more details.

SMEs members of the consortium shall all be considered as cross-border SMEs.

3.11. List of eligible countries

Public or private undertakings established in the following countries will be eligible to receive funding (*i.e.* become beneficiaries) through EDIDP grants:

- The Member States (MS) of the European Union (EU), including their outermost regions;

The attention of the applicant is drawn on the existence of other eligibility criteria (please refer to section 3.4.4).

Applicants are invited to read carefully the guide for applicants (available here) which provides additional guidance on how to fill the submission form and to prepare proposals.

Any remaining questions regarding the calls can be submitted by email no later than 31 May 2019 at EC-EDIDP-proposals@ec.europa.eu. The Commission may reply to received questions on the "Funding and tenders portal" website no later than 28 June 2019. Any questions or replies do not constitute any ground to claim any expectation concerning the selection of the proposal or the award of the grant.

4. Annex – Security aspects

4.1. Introduction

This Annex issued by the European Commission – DG for Internal Market, Industry, Entrepreneurship and SMEs – mentions the main Security Aspects to complement the EDIDP call for proposals for 2019.
It establishes the general requirements for the performance of the tasks identified in the calls, which may involve the handling of classified information.
The beneficiary's National Security Authority (NSAs) is responsible for ensuring that the beneficiaries under their jurisdiction comply with the applicable security provisions for the protection of classified information.

4.2. Definitions

ACTION means, in the light of Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry, the project selected under the Programme which the Consortium is to carry out.
BENEFICIARY is an individual or legal entity possessing the legal capacity to receive funding through a grant in the EDIDP and which has been selected by the Programme to receive the grant.
CLASSIFIED INFORMATION means any information or material designated by a security classification, the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or more of the Participants or any other State or international organisation with which the Participants have concluded a security of information agreement. Its classification level, and therefore the level of protection to be afforded to it by the recipient of the classified information, is indicated by a classification marking as detailed in the Appendix to this Annex.
CONSORTIUM means a collaborative grouping of undertakings constituted to carry out an action under this Programme.
DESIGNATED SECURITY AUTHORITY (DSA) is a state authority responsible to the National Security Authority (NSA) of a participant which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority in that Participant state.
EU CLASSIFIED INFORMATION (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.
FACILITY SECURITY CLEARANCE (FSC) means an administrative determination by a NSA, DSA or competent Security Authority that, a facility can afford an adequate level of protection to classified information to a specified security classification level.

FOREGROUND INFORMATION is classified information generated in the performance of the Action.
GRANTING AUTHORITY is the Commission department responsible for the Programme, which prepares, awards, cancels or modifies grant agreements.
NATIONAL SECURITY AUTHORITY (NSA) is a government authority with ultimate responsibility for the security of Classified Information in that country.
PERSONNEL SECURITY CLEARANCE (PSC) means a statement by a competent authority of a Participant state, which is made following completion of a security investigation conducted by a competent authority of a Participant state and which certifies that an individual is cleared to have access to Classified Information.
SECURED AREA is a physically protected area with a visibly defined and protected perimeter through which all entry and exit is controlled by means of a pass or personal recognition system, where unescorted access is granted only to individuals who are security cleared and are specifically authorised to enter the area on the basis of their need-to-know, and where all other individuals are escorted at all times or are subject to equivalent controls.
SECURITY ASPECTS LETTER (SAL) is a set of special contractual conditions, issued by the Contracting or Granting Authority, which forms an integral part of a Classified Contract or Classified Grant involving access to or generation of Classified Information, that identifies the security requirements or those elements of the contract or grant requiring security protection.
SUB-CONTRACTOR is a legal entity awarded a sub-contract under the Action.

4.3. General conditions

Pursuant to Commission Decision (EU) 2019/513 of 26 March 2019 on the security framework for the European Defence Industrial Development Programme, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries are established shall decide on the originatorship of the classified foreground information generated in the performance of an action. For that purpose, those Member States may decide on a specific security framework for the protection and handling of classified information relating to the action and shall inform the Commission thereof. Such a security framework shall be without prejudice to the possibility for the Commission to have access to necessary information for the implementation of the action.
If no such specific security framework is set up by those Member States, the security framework will be put in place by the granting authority in accordance with Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information (‘Decision 2015/444’).
The applicable security framework for the action has to be in place at the latest before the signature of the grant agreement.

The applicable security framework will be detailed in the Security Aspect Letter (SAL) which will be integral part of the Grant Agreement.

4.4. Access to classified information

All entities participating in grants which involve creation or access to information classified CONFIDENTIAL or SECRET, or at RESTRICTED level where requested by national rules, at the consortium's premises, shall ensure that a valid Facility Security Clearance (FSC) at the appropriate level exists for the premises. This FSC must be granted by the National Security Authority (NSA/DSA) of the entity involved.
The involved entities must hold a duly confirmed FSC at the appropriate level. Until a Secured Area is in place and accredited by national NSAs, handling of classified information above RESTRICTED level shall not be possible in their premises.
Access to and handling of classified information for the purposes of the Action shall be limited to individuals with a need-to-know in possession of a valid Security Clearance.

Upon termination of the grant agreement when EUCI is no longer required for the performance of the grant, the Beneficiary shall return any EUCI they hold to the contracting authority immediately. Where the Consortium is authorised to retain EUCI after termination or conclusion of the grant, the EUCI must continue to be protected in accordance with Commission Decision (EU, Euratom) 2015/444.

4.5. Marking of classified information

Classified information generated for the performance of the grant agreement shall be marked in accordance with the applicable security instructions of the Action.
Grant agreements shall not involve information classified ‘TRES SECRET UE/EU TOP SECRET’ or an equivalent classification.

4.6. Other provisions

Where a beneficiary has awarded a classified subcontract, the security provisions of the grant agreement shall apply *mutatis mutandis* to the subcontractor(s) and their personnel. In such case, it is the responsibility of the Beneficiaries to ensure that all subcontractors apply these principles to their own subcontracting arrangements.
All security breaches related to classified information shall be investigated by the relevant security authority.

Appendix to Annex - Table of equivalent security classification markings

Participant	Secret	Confidential	Restricted
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	SECRET (Loi du 11 Dec 1998) or GEHEIM (Wet van 11 Dec 1998)	CONFIDENTIEL (Loi du 11 Dec 1998) or VERTROUWELIJK (Wet van 11 Dec 1998)	DIFFUSION RESTREINTE or BEPERKTE VERSPREIDING *(Note, see below)*
Bulgaria	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Croatia	TAJNO	POVJERLJIVO	OGRANIČENO
Cyprus	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Czech Republic	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG
France	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	*(Note, see below)*
Germany *(Note, see below)*	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
Ireland	SECRET	CONFIDENTIAL	RESTRICTED

Participant	Secret	Confidential	Restricted
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET	KUNFIDENZJALI	RISTRETT
Netherlands	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Poland	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	SECRETO	CONFIDENCIAL	RESERVADO
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG or HEMLIG/SECRET or HEMLIG	HEMLIG or HEMLIG/CONFIDENTIAL	HEMLIG or HEMLIG/RESTRICTED
United Kingdom	UK SECRET	No equivalent *(Note: see below)*	UK OFFICIAL - SENSITIVE

Notes:

Belgium and France: Both Participants handle and protect classified information bearing the marking "RESTRICTED" or equivalent according to its national laws and regulations in force for the protective level "DIFFUSION RESTREINTE" (also "BEPERKTE VERSPREIDING" in the case of Belgium) or the standards defined in the present document whichever is higher. The other Participants will handle and protect information marked "DIFFUSION RESTREINTE" (also "BEPERKTE VERSPREIDING" in the case of Belgium) according to their national laws and regulations in force for the level "RESTRICTED" or equivalent or according to the standards defined in the present document whichever is higher.

Germany: VS = Verschlusssache.

United Kingdom: The UK handles and protects classified information marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.