European Defence Fund (EDF)

Call for proposals

EDF-2022-RA

Version 1.0
09 June 2022

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	09.06.2022	– Initial version.	
		–	
		–	
		–	

EUROPEAN COMMISSION
Directorate-General for Defence Industry and Space

DEFIS.A – Defence Industry

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction

This is a call for proposals for EU **action grants** in the field of collaborative defence research and development under the **European Defence Fund (EDF)**.

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2018/1046 (EU Financial Regulation)
- the basic act (EDF Regulation 2021/697[1]).

The call is launched in accordance with the Work Programmes 2022 Part II[2] and 2023 Part I[3] and will be managed by the **European Commission, Directorate-General for Defence Industry and Space (DG DEFIS)**.

The call covers the following **12 topics**:

- **EDF-2022-RA-MCBRN-HICP: Diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel**
- **EDF-2022-RA-C4ISR-AIRC2: Single European Sky interoperability**
- **EDF-2022-RA-SENS-CSENS: Covert sensing**
- **EDF-2022-RA-SENS-ART: Advanced radar technologies**
- **EDF-2022-RA-SENS-ART: Advanced radar technologies**
- **EDF-2022-RA-SPACE-RSS: Responsive space system**
- **EDF-2022-RA-DIGIT-DBIR: Shared databases and integrated systems for image recognition**
- **EDF-2022-RA-ENERENV-CUW: Sustainable components for underwater applications**
- **EDF-2022-RA-MATCOMP-PACOMP: Packaging technologies for critical defence components**
- **EDF-2022-RA-PROTMOB-FMTC: Future mid-size tactical cargo aircraft**
- **EDF-2022-RA-UWW-UTS: Underwater manned-unmanned teaming and swarms**
- **EDF-2022-RA-UWW-ODAC: Underwater observation, detection, acquisition and communications**

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

[1] Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092 (OJ L 170, 12.5.2021).

[2] Commission Implementing Decision C(2022) 3403 final of 25/05/2022 on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2022 - Part II.

[3] Commission Implementing Decision C(2022) 3659 final of 07/06/2022 on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2023 - Part I.

We invite you to read the **call documentation** carefully, and in particular this Call Document, the Model Grant Agreement, the EU Funding & Tenders Portal Online Manual and the EU Grants AGA — Annotated Grant Agreement.

These documents provide clarifications and answers to questions you may have when preparing your application:

- the Call Document outlines the:
  - background, type of action and funding rate, objectives, scope and types of activities, functional requirements, expected impact and specific topic conditions (sections 1 and 2)
  - timetable and available budget (sections 3 and 4)
  - admissibility and eligibility conditions, including mandatory documents (sections 5 and 6)
  - criteria for financial and operational capacity and exclusion (section 7)
  - evaluation and award procedure (section 8)
  - award criteria (section 9)
  - legal and financial set-up of the Grant Agreements (section 10)
  - how to submit an application (section 11)
- the Online Manual outlines the:
  - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
  - recommendations for the preparation of the application
- the AGA — Annotated Grant Agreement contains:
  - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant *(including cost eligibility, payment schedule, accessory obligations, etc)*.

You are also encouraged to visit the DG DEFIS webpage to consult the list of projects funded previously.

1. Background

The European Defence Fund (EDF) fosters the competitiveness, efficiency and innovation capacity of the European defence technological and industrial base (EDTIB).

It contributes to the EU strategic autonomy and its freedom of action, by supporting collaborative actions and cross-border cooperation between legal entities throughout the Union, in particular SMEs and mid-caps, as well as by strengthening and improving the agility of both defence supply and value chains, widening cross-border cooperation between legal entities and fostering the better exploitation of the industrial potential of innovation, research and technological development, at each stage of the industrial lifecycle of defence products and technologies.

The EDF funds projects which are consistent with the defence capability priorities commonly agreed by EU Member States within the framework of the Common Foreign and Security Policy (CFSP), through:

- collaborative research that could significantly boost the performance of future capabilities, aiming to maximise innovation and introduce new defence products and technologies, including disruptive technologies for defence, and aiming to make the most efficient use of defence research spending in the EU

or

- collaborative development of defence products and technologies, thus contributing to the greater efficiency of defence spending in the EU, achieving greater economies of scale, reducing the risk of unnecessary duplication and thereby fostering the market uptake of European defence products and technologies and reducing the fragmentation of defence products and technologies, ultimately leading to an increase in the standardisation of defence systems and a greater interoperability between Member States' capabilities.

In line with the Work Programmes 2022 Part II and 2023 Part I, this call covers the thematic topics addressing research actions to be implemented through actual costs grants.

2. Type of action and funding rate — Objectives — Scope and types of activities — Functional requirements — Expected impact — Specific topic conditions

Type of action and funding rate

The topics under this call for proposals concern EDF Research Actions (RA).

Research Actions are reimbursed at a funding rate of 100%.

Specific topic conditions

- For all topic under this call, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply *(see section 6)*

- For all topic under this call, following reimbursement option for equipment costs applies: depreciation only *(see section 10)*

EDF-2022-RA-MCBRN-HICP: Diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel

Objectives

General objective

Research and development in detection, diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel (HICP) provides for new life-saving techniques, concepts and strategies for soldiers on the battlefield, including surgical robots, ultra-portable telemedicine devices and diagnostics sensors, Chemical Biological, Radiological and Nuclear (CBRN) containment systems, 'porter' or load- carrying Unmanned Vehicles (UVs) and battlefield casualty extraction devices. Battlefield logistics are a challenge regardless of the mission. Adversaries, terrain, and the environment all serve to complicate the process of delivering supplies to the wounded and sick. The medical support to a force must be capable of maintaining the necessary quality and quantity of supply, treatment and evacuation activities during peace, crisis, and conflict. This requires having on hand or in reserve appropriate medical equipment, supplies, integrated medical evacuation capabilities and remote casualty care capacity, as well as having the ability to resupply and to replace medical personnel on a continuous basis.

Specific objective

The limited ability to rescue HICP, while under fire or into a hazardous environment, is itself a major cause of poor outcome and death.

In the CBRN contaminated battlefield, combat-related injuries are "combined" – related to both, trauma and contamination. The time to aid a victim is crucial. This is even true for combination injuries. Hence there is a need to provide solutions for autonomous battlefield triage, safely extraction of HICP from the battlefield, providing instant availability information about vital signs, rapidly diagnosing life-threatening injuries, remote access of medical personnel to the casualty and delivering life-saving interventions. Extraction robots and dedicated evacuation vehicles may decrease the risk to the soldier and combat medic by life-saving robotic-assisted interventions, and by safely moving wounded soldiers out of the line of fire. Tele operated and autonomous surgical robots may deliver expert surgical care within the "golden hour" on the battlefield as well as during transport to military treatment facilities. In CBRN situations, notably under radiation exposure, further restrictions have to be dealt with such as limited accessibility of the affected areas and concerns regarding the safety of the rescuing personnel.

Scope and types of activities

Scope

Proposals must address extraction, treatment, and evacuation systems, including detection, diagnostics, integrated life-support systems and transport of HICP. Proposals must in particular address:

- design of a dedicated CBRN casualty extraction device and/or adaptation and integration of existing capabilities, 'porter' or load- carrying UV/RGP[4] capable to locate, lift (scoop) and rescue, operating in hazardous and uneven/rough conditions,

- patient on-board life support and containment system supported by automated recording of vital signs to perform preliminary diagnostics and movement of casualties, containing ventilator, defibrillator, in-/out protection, and devices to monitor the physiological status of the patient to perform preliminary diagnostics,

- decontamination technologies for safe treatment and/or transport of HICP,

- robotics-assisted life-saving intervention, such as automated administration of anti-dots and/or haemostats or tourniquets,

- solutions for quick location of casualties and initial diagnosis, including triage, in case of CBRN events, for example based on wearable (bio)sensors or other sensor solutions.

In addition, proposals should also address:

- methods and concepts for seamless interoperability and complementarity of CBRN casualty extraction devices, whereas casualties could be evacuated by unmanned vehicles and robotic platforms and transported to medical treatment facilities,

[4] Unmanned vehicle/Robotic ground platform

- compatibility between transport types with plug & transport solutions leading to an enhanced responsiveness and resilience. E.g., by a modular platform system as a basis for multiple (unmanned) aerial or ground vehicles: (roll-on / roll-off platform system),

- integration of CBRN casualty extraction devices into health monitoring platforms and/or CBRN DIM[5] systems,

- harmonization of the different concepts of operation (interoperability) fostering the collaboration of EU Member States and associated countries with a standardized solution,

- investigation of new possibilities to transport and assist HICP,

- semi-autonomous or 'supervised' surgical capabilities, concepts for material, structure design, ventilation and medical supply logistics for the safe transport and assistance (including treatment) of contaminated or contagious casualties in CBRN hazard area,

- evaluate the designated materials, the components and the final system during transport and assistance of contaminated/contagious casualties,

- selection of material and components, and evaluation according to suitable simulation and testing procedures.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional (see Article 10(3) EDF Regulation):

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping[6]** of a defence product, tangible or intangible component or technology	No

[5] Detection, identification, monitoring

[6] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[7] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[8] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must substantiate synergies and complementarity with foreseen, ongoing or completed activities in the field of MEDEVAC[9] and RSS[10], notably those performed or foreseen in the context of EDIDP, EDF 2021, Horizon 2020 and Horizon Europe.

Moreover, projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them).

Functional requirements

The proposed activities should address technologies to provide the following functional requirements:

- adaptable UxV evacuation vehicle and/or platforms for different operations (for example short/medium/long range transport of HCIP);
- air filtration system with air quality monitoring capability to be applied during transport, which would be adaptable for different CBRN conditions – HICP with different agents;
- option for transport of casualty/patient required ICU[11];
- integrated decontamination system/capabilities;
- operate in extreme environments (including hazardous environments) and provide combat casualty care as close as possible to the point and time of injury;
- robust, light and small as possible, resisting fog, mud or dust and extreme temperatures, in order to assure a correct service in hostile environments and over debris surfaces;
- track, record, transmit and act upon continuous near-real-time measurement of physiological/health data rendered by wearable biosensors;

7 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.
8 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.
9 Medical evacuation.
10 Reconnaissance and surveillance services.
11 Intensive care unit.

- locate and evacuate HICP from the battlefield using UxV evacuation platforms;
- carry / integrate a payload of medical supplies including a life support and surgical system capable to perform automated and/or robotic assisted lifesaving interventions, e.g., administer CBRN medical countermeasures using a robotic arm;
- (semi-) autonomous deployable surgical platform, including miniaturized surgical devices for robotic surgery to fit in casualty extraction UxV;
- integration of diagnostic, imaging and therapeutic capabilities (e.g., digital x-ray, portable ultrasound, intubation);
- smart textile sensor integration and wearable biosensors;
- carry / integrate into CBRN DIM system to provide early information as to the possible toxic hazards in the environment;
- remote assistance, including tele-medicine, such as technologies to communicate with a reach-back human medical team, imaging technologies and/or augmented reality technologies;
- protect the HICP during transport;
- for design of platforms, a manual with all tested and evaluated procedures should be prepared.

Expected impact

- Provide substantial improvements to the CBRN / medical defence domain for Member States and Norway armed forces that can revolutionize battlefield care by safely extracting casualties and patients from harm's way, rapidly diagnosing life-threatening injuries, delivering life-saving interventions and ensuring their safe transport (short-medium or long range) to dedicated medical facilities;
- Facilitate the development of CBRN / medical defence capabilities that each Member State, associated country, individual government or industry cannot face alone;
- Strengthen European sovereignty and contribute to the EU strategic autonomy;
- Develop EU autonomous industrial segments.

EDF-2022-RA-C4ISR-AIRC2: Single European Sky interoperability

Objectives

General objective

In order to cope with sustained air traffic growth and operations over Europe, the Single European Sky (SES) initiative has been running since 2004. It intends to improve the performance of Air Traffic Management (ATM) in terms of safety, capacity, cost-efficiency and the environment. It hence paves the way for a European airspace that is used optimally, embraces emerging disruptive technologies, facilitates the integration of "new entrants" such as all types of drones, High Altitude Platform Systems (HAPS) to super- and hyper-sonic aircraft, trans-atmospheric and suborbital

vehicles, and complies with emerging challenges. This modernisation of the civil aviation sector does not directly apply to military operations and training. However, civil and military aviation activities are closely interlinked, as they share the same airspace considered as a continuum. Therefore, SES implies a necessary coordinated modernisation of the different Air Command and Control (C2) systems, which are furthermore to collaborate at national and EU levels. Indeed, in this context, concomitant with a more hostile security environment, the timely sharing of correct and consistent information covering all phases of flight, between civil and military parties is a must.

Specific objective

The evolving SES regulations based on the harmonisation of the coordination and interoperability operational concepts or technical standards introduces in front of the military ATM stakeholder several new challenges which might be converted in opportunities for a more complete, optimized and performant Air C2 missions.

The introduction of the 4D Trajectory based management of the Air traffic and the new technical standards on the harmonisation of automatic ATM data exchanges need to be implemented in the Air C2 centres and systems.

The latest version of the European ATM Master Plan demonstrates the necessity to transform the ATM architecture due to several observed concerns that will have to be improved and optimised. These concerns are mainly the following ones:

- a steady increase of conventional traffic since 2014, even if the current sanitary crisis has drastically reduced the traffic, it is most probably a temporary situation;

- the growing environmental concerns raised by the aviation sector to demonstrate its capacity to contribute to the EU's environmental objectives;

- the appearance of new entrants into the airspace with the expected large number and heterogeneous nature of drones together with the emerging interest for operating vehicles at very high altitudes;

Against this background, Member States and Norway must be prepared from a military perspective to:

- Safeguard the military ambition to be trained for and to execute missions as required and more specifically to continue performing Air Surveillance and Control in the changing context of civil aviation sector (digitalization, automation, dynamic airspace management, new data format, resilience and cybersecurity issues), facing the density and diversity increase of air traffic,

- Ensure the interoperability and data exchange between civil and military control centres, including data sharing between classified and non-classified environment, permitting an efficient, secured and safe ATC[12] (e.g., for military airports providing Air Traffic Services for civilian flights) and to support the planning, tasking.

[12] Air traffic control.

Scope and types of activities

Scope

Military airspace users' main challenges are to continue to provide, and further improve, defence and security missions, with needs of high degree of flexibility and reactiveness, into an airspace shared with civil airspace users, without prejudice to the safety of civil air traffic, and considering, to the maximum extent possible, the performance and environmental objectives of the civil aviation sector.

In order to do so, the scope of the activity consists in increasing interoperability of military Air C2 systems against SES rules via an interoperability demonstration. The activity must focus on identifying technical solutions for information and data exchanges between cross border military C2 systems and cooperating civil – military ATC systems based on new challenges generated by the evolution of the SES harmonisation deployment regulation and new possibilities offered by information technologies.

In particular, the implementation and assessment of new rules of Interoperability (IOP) for surveillance and control of the European air traffic from a military perspective are the main objectives of this call. Several technical standards must be implemented, and solutions developed to ensure the harmonized, efficient and secure data exchanges between relevant civil and military stakeholders:

- Technical interoperability for real time flight and airspace management data exchanges (with relation to ability to exchange, exploit and fill Flight Objects, etc.);
- Security aspects to ensure cross-domain exchanges (with regards to secure gateway or procedures to limit dissemination of sensitive military information, facilitating sharing of military information to enhance civil situational awareness, etc.);
- Assessment of resulting ATM safety levels as any ATC civil-military interoperability system.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)

(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[13] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[14] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[15] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must substantiate synergies and complementarity with SES, including SESAR, activities.

Functional requirements

The technical solutions for information and data exchanges between cross border military C2 systems and cooperating civil – military ATC systems should meet the following functional requirements:

(1) Situational Awareness establishment and exploitation

- Improve surveillance and flight identification data capacity
- Improve situational awareness and operational flexibility
- Identify better conditions to accommodate the mission-specific requirements derived from the introduction of new generations of military manned and unmanned aircraft and systems.

(2) Coordination and IOP assessment

- Improve flight information automatic exchange for coordination purposes
- Facilitate hand-over of aircraft control
- Identify and develop a military solution of common interest for European forces and compliant with SES regulation for the ATM civil-military, and military-military exchanges

[13] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[14] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[15] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Integrate data compliant with SES technical standards used for IOP exchange between civil-military ATC systems or military Air C2 systems of cross-border countries

- Implement Operational Air Traffic (OAT)/General Air Traffic (GAT) rules.

(3) Cross-domain connectivity establishment and services provision

- Assess the impact of the new pan-European network service (NewPENS) and the system-wide information management (SWIM) service-oriented architecture, including SWIM Nodes (for military operation system) access procedure, based on available standard interfaces to the military infrastructure and services delivery architecture (SWIM Blue for the interoperability)

- Identify the level of performance/quality of service requirements as the basis to select the applicable SWIM-TI (technical infrastructure) profile

- Develop interfacing and IP (internet protocol) networking approaches supporting SWIM-TI accessibility

- Comply with NewPENS and SWIM services, including related standardization rules

- Identify proprietary/local interoperability options outside the context of SWIM to ensure service continuity and redundancy and diversity of connections for military systems

- Design and develop an evolving, scalable cross-domain solution supporting the information exchanges between ATM civil-military and military-military centres

- Validate end-to-end information exchanges via the SWIM TI, between ATM military centres from European forces and between ATM civil and military centres in accordance with the regulation of the SES and national security rules.

Expected impact

This collective work should provide individual and mutual benefits, for European Member States, Norway and the industry, in different fields as follows:

- European Technology
    - Reinforcement and security improvement of data exchange between cross domain (classified and unclassified environments)
    - Improvement of air surveillance performances and flight's safety
    - Improvement of Dynamic Airspace Management
    - Capitalisation of on field proven Research & Development (R&D) process and ensure limited in time project
    - Production of consolidated R&D data for further industrialization phase
- European Autonomy
    - Contribution to the enhancement of sensible data sharing between ATM stakeholders

  - Maintenance and enhancement of autonomous control of the European defence capabilities
  - Protection of the environment of the European citizen
- European Security
  - Participation to the improvement of the airspace surveillance and control, and air policing missions
  - Facilitation of military forces projection and intervention
  - Enhancement of cooperation between Member States and Norway for defence matters.

EDF-2022-RA-SENS-CSENS: Covert sensing

Objectives

Due to the current geopolitical instability, European military forces will be obliged to participate in demanding military multi – domain operations like securing air superiority, land and sea control, border surveillance, traffic management, security of critical infrastructures, etc. Military information superiority is key to these operations, because they are relying on the best possible battlefield awareness, which is created by the exploitation of data acquired by modern sensors, integrated both in a range of platform and in a range of concepts of use enabled by the digital transformation of the battlefield.General objective.

General objective

Given the sensors' technological progress, the European military forces may encounter potential adversaries capable of obtaining a robust situational awareness by using advanced active and passive sensor capabilities, able to accurately locate and identify forces and their sensors in the three-dimensional battlespace (land, sea and air). For efficient Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) missions, armed forces therefore need to have sensors that reliably allow detection, classification and tracking of targets while being themselves difficult to detect, track and intercept. The capability to sense covertly allows unhindered operation without exposing location and identity to the enemy surveillance activities, thus lowering the vulnerability of own forces and conferring a key advantage in military conflicts.

In the modern operational environment, there are targets with properties resulting in low probability of detection, due to their low signature or manoeuvring characteristics (very fast or very slow, up to hovering). Targets can also be difficult to detect due to the operation conditions (such as in urban scenarios, under foliage, underground or underwater operation or operating at low altitude) leading to strong clutter or a degraded visual environment. Recent advances in computing power, digital data and signal processing, together with the drastic reduction of size, weight and overall dimensions of equipment due to the advancement of microelectronics technology, have paved the way for better sensors, with increased sensitivity and better detection characteristics.

Examples of use-cases, where covert sensing of difficult targets is of particular importance include:

- counter-battery fire;

- detection of sea surface targets (drones, periscopes, wooden boats, communication buoys…);

- air defence and detection, recognition, identification and tracking of aerial targets (including low flying, slow, small drones);

- detection of fast manoeuvring and fast-moving targets with up to hypersonic speeds, like tactical ballistic missiles and anti-ship missiles;

Specific objective

Modern surveillance sensors have to comply with operational requirements such as:

- To provide steady and reliable surveillance (detection, tracking, classification, identification), at various environmental conditions – for all battlespace dimensions, with guaranteed low probability of false alarms

- To detect and track targets that are difficult to detect in complex environments, like rural, coastal and mountainous areas with complex relief, semi-urban and urban environments, etc.

- To operate covertly, exhibiting low (for passive sensors) or reduced (for active sensors) signature to enemy counter- intelligence, surveillance and reconnaissance (ISR) assets, thus reducing the possibility of being intercepted and countered,

- To be capable of supporting target acquisition in all mission phases and to support target engagement on the move, in particular by continuing interpretation and processing of data while the sensor and / or the target are moving or changing position.

- To have improve sustainability under harsh operational conditions in full battlespace dimensions (sea, air and land)

- To provide robustness in contested environments, with scenarios that are becoming more and more dynamic with highly agile targets.

- To be able to be integrated in various types of static and moving platforms (ground-based, shipborne, airborne, space-based), both manned and unmanned;

Covert sensing concepts can in principle include:

- Passive sensors that are less traceable and are hard to target and

- Active sensors with very low probability of intercept, in particular when used in specific configuration (multi-static configurations...)

Such sensors can be based on different types of physical phenomena (to detect different electromagnetic wavelength, acoustic waves, photons…) and on different working principle.

To use the advantage of a multi-sensor and multi-spectral approach, the sensors may need to be integrated into a network of multiple heterogeneous sensors and provide data that can be merged with data from other sources.

Scope and types of activities

Scope

This topic aims at enhancing detection performance (such as range, sensitivity, resolution) of sensor systems to detect low signature targets, in the modern three-dimensional operational environment while maintaining covert operation, without exposing presence, identity and location. It encompasses innovative concepts of sensor use, in particular the combination of multiple, heterogeneous sensors, potentially on different platforms.

Considered sensors may be electro-optical/infrared, radiofrequency and/or acoustic sensors, not excluding innovative sensor concepts. They must be passive or low-observable active. The topic covers the enhancement of individual sensors as well as their interplay.

The sensors' integration and interoperability with other sensors (networks) and connection to battlefield management systems must be addressed, e.g., through standardized data formats and interfaces or data processing (up to data fusion) on the sensor level.

Proposals should address the optimization of available sensor resources in order to achieve optimum surveillance results. Proposals should also address aspects of efficient data exploitation and data fusion close to the data source.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[16] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No

[16] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

(g)	**Qualification**[17] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[18] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The following tasks may be performed as part of the optional activities of the project:

- Generating knowledge:
  - Research on low-signature active sensors as well as very high sensitivity passive sensors
  - Activities aiming at improving the ability of sensors to operate in difficult conditions
- Integrating knowledge:
  - Activities aiming at improving communication and connection between sensors

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activities of the project:

- Studies
  - Definition of relevant targets and operational conditions
  - Definition of performance evaluation techniques and parameters for detection and classification solutions.
  - Study and modelling of relevant signatures of targets and of complex environments, e.g., rural, coastal and mountainous areas with complex reliefs, semi-urban and urban environments, etc., and under different weather conditions.
  - Study on enhancing performance robustness when dealing with different platform dynamics, stability, and manoeuvring conditions, different targets and environments.
  - Study of data fusion techniques for improving detection and classification performances in different sensors configurations
  - Study on interfaces and data exchange formats to provide efficient data fusion and exploitation, taking into account standards used by the EU Member States and Norway armed forces.

[17] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[18] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Design
    - Design of a system of passive or low-observable active sensors to detect targets of interest
    - Demonstration of the performance of the system in a simulated environment, if possible, including real data where relevant to improve modelling and demonstration
    - Demonstration of the performance of the system in a laboratory environment

Functional requirements

Proposals should address technologies and solutions that:

- significantly increase detection performance with respect to new and challenging targets in harsh operational environment;
- significantly increase performance robustness against changes of the environment and the target characteristics;
- are adaptable to different and complex scenarios (e.g., electromagnetically congested, dynamic, with degraded visibility and rapidly changing), enabling multi-mission and multi-platform applications (maritime, land and air);
- have reduced size, weight and power consumption, for scalable integration on differently sized manned or unmanned platforms;
- are compatible with modular and scalable architectures;
- are compatible with multi-sensor and multi-spectral approaches;
- ensure interoperability with other systems by providing standardized interfaces and data exchange formats used by the EU Member States and Norway armed forces;
- simulate and automatically configure sensor configurations to carry out data fusion while optimizing the available resources and achieving the optimum surveillance results;
- allow efficient exploitation and data fusion from multiple static or deployed sensors;
- are capable of executing data processing and analytics close to the data source to decrease the capacity needs to transfer sensor data;

Expected impact

- New knowledge in the field of covert sensors, sensor systems and their interplay, thereby strengthening the European technological and industrial base.
- Future EU critical land, naval and air ISTAR capabilities in highly dynamic scenarios, especially regarding challenging targets, increasing situational awareness, early warning, decision making and action planning capabilities.

- State of the art, covert sensing capability that increases survivability of units/platforms.

- Increase of interoperability and efficient use of sensor systems thereby facilitating joint operations among armed forces of the EU Member States and Norway.

EDF-2022-RA-SENS-ART: Advanced radar technologies

Objectives

General objective

Passive and active radio-frequency (RF) systems in general and surveillance radar systems in particular remain vital assets for supporting multi-domain operations: incl. air and air defence missions, as well as ground/maritime operations.

Management of the electromagnetic spectrum has increased in importance. Radar operation must be compatible with other communication and control systems running concurrently. Management of emission and sensing in both space and frequency increases the systems covertness. It also improves the system's ability to discriminate reliably signals coming from passive and civilian sources as well as active disturbances such as jammers and decoys.

Emerging technologies lead to the increased appearance of threats that are difficult to detect and track due to their low radar cross-section (RCS) (e.g., stealth technologies), manoeuvring characteristics (e.g., hypersonic weapon systems, slow-moving airborne units) or saturation attack tactics. Facing such a wide spectrum of threats (in terms of variation of speed, angle of approach and altitude), existing surveillance systems are reaching their limits in terms of detection range, angular domain coverage, and tracking capabilities. Specific operating modes (e.g., multistatic configurations) can improve detection and tracking performance. They however lead to an increased requirement on multiple beams forming. Proper detection, recognition and classification of different targets in a variety of operational conditions also requires a finely tuneable band.

Specific objective

Those operational and technical challenges can be met by future systems with:

- agile digital beamforming to optimise observation time, volume coverage and detection reliability

- System characteristics such as wide or ultra-wide band coverage, low noise, high coherence

- Software defined waveforms with high degree of flexibility and use of multiple bands

- Data processing functions to enhance detection performance, target recognition and classification, notably with respect to new threats

In order to be operated in various conditions and to be integrated in various platform, specific requirements moreover apply to the dimensions, weight and energy consumption of the radar modules (e.g., through miniaturization or grouping of functions in small electronic units) as well as their materials and electronics design to ensure optimal operability in harsh conditions. Efforts are also aiming at integrating multiple functions (radar, communication, electronic warfare) in a single radio frequency system for multi-role systems (e.g., see call PADR-EMS-03-2019).

Scope and types of activities

Scope

Recent research and development efforts in the field of radar and electronic warfare systems have the goal to create more flexible and adaptive systems in terms of modes of operation and beamforming. At the same time, new technologies offer possibilities to explore different frequency (or bandwidth) ranges while maintaining a high signal-to-noise ratio. A further objective is to integrate more functions, including internal computing capacities, while responding to the operational restrictions in terms of size, weight and power consumption and cost (SWaP-C).

The scope of this call topic focusses on electronic components and their integration that help to accomplish the above-mentioned goals by achieving:

- improved size/weight/power ratios through miniaturisation and system integration
- integration of new technologies to increase the system's adaptability to environments and operational scenarios.
- demonstration of agile and precise radar beam steering and detection performance.

The following enabling technologies serve as examples for the improvement and integration scope of this topic, without excluding other relevant technologies:

- direct sampling technologies able to perform data conversion in any radar frequency band, reducing the RF front-end complexity and maximizing the miniaturisation;
- hardware and software components for digital beamforming, including using photonic components, that enable generic and reconfigurable digital beamforming, especially with true-time delay, broadband characteristics, multi-beam capability;
- hardware and software that would allow real time signal and data processing coming from digitized received signals at radiating element level in order to extract and store the information on targets including detection, tracking and classification;
- components that enable the generation of extremely stable radio-frequency signals
- antenna components that emit in a broad frequency band with low spurious emissions to adapt to the environment, e.g., by exploring fully polarimetric active electronically scanned array (AESA) antennas which are more robust against interferences and can enable enhanced performance in terms of detection and classification.

Proposals should target a substantial technological advancement in order to bring the considered components to a maturity level corresponding to laboratory testing or higher (technology readiness level TRL> 4).

Furthermore, proposals may include complementary aspects on:

- application of artificial intelligence as a means of enhancing target detection, classification and identification performance, notably with regards to new threats, including to enable cognitive radar concepts

- integration aspects (such as interfaces with other sub-subsystems and data exchange formats) including high data rate transfer to other sub-systems (software and/or hardware aspects), in particular enabling distributed radar setup and Command and Control integration

This topic complements past and ongoing research and technology efforts supported by the EU, e.g., through the calls PADR-EMS-03-2019, PADR-EDT-02-2018 and the calls EDF-2021-SENS-R-RADAR, EDF-2021-MATCOMP-R-RF as well as Member States' and Norway's efforts, including in the EDA framework.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (mandatory)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[19] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[20] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[21] of a defence product, tangible or intangible component or technology	No

19 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

20 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

21 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activities of the project:

- Generating knowledge:
  - Research on software and hardware solutions for processing digital signals collected after RF direct sampling for sensors
  - Investigation of technologies and components for wideband or multiband direct sampling
  - Exploration of innovative antenna design
  - Investigate cognitive approaches that enables adaptability of the system to the environment and the scenario.
  - Investigation of technologies and components for ultra-low phase noise oscillators
  - Investigation of improvement of SWaP-C for the considered components.

  The proposal may also address optionally the following tasks under this activity:

  - Prepare suitable model of targets, threats and environment for training artificial intelligence (AI) -based algorithms;
- Integrating knowledge:
  - Explore scenarios and algorithms to improve the performance in scenarios including low RCS targets and highly manoeuvring targets such as hypersonic ones.
  - Explore the applicability or adoption of components and technologies from civil applications to defence designs

  The proposal should moreover address the following tasks under this activity:

  - Investigation of solutions, such as algorithms, to increase system resilience against Cyber Electro Magnetic Activities (CEMA) and similar threats
  - Investigate "secure by design" technologies that can be used to increase system resilience in case of cyber-attacks;
- Studies
  - Selection of relevant operational scenarios
  - Exploitation of numerical simulations, e.g., based on digital twins, for testing new hardware and software solutions

- Study of advanced antenna architectures, including innovative thermal management solutions and material, reducing size, weight and power consumption (acceptable SWaP for airborne applications) while providing enhanced surveillance and tracking capabilities;

The proposal may address the following tasks under this activity:

- Study on technology for sharing and distributing classified data from RF sensor systems;

- Study on the use of AI techniques for system design and concept

- Design

  - Design of digital beamforming and testing in a laboratory environment

  - Design on-board computing solutions for deployment of signal and data processing algorithms enabling enhanced and real-time computing capabilities and demonstration of performance in a laboratory environment;

  - Design of digital twins for testing of new hardware and software solutions and demonstration in a laboratory environment;

  - Design of advanced antenna architectures, including innovative thermal management solutions and material, reducing size, weight and power consumption (acceptable SWaP for airborne applications) and demonstration in a laboratory environment;

  - Validation of the adaptive capabilities of the system by tests in a simulated environment and in a controlled environment.

Functional requirements

Proposals should address technologies and solutions that:

- Integrating wide bandwidth components and building blocks for achieving better detection, tracking and, classification performances of radio-frequency sensor systems, including for challenging threats;

- Enabling versatility and reconfigurability with respect to system functions and operational modes (e.g., tracking modes, imaging modes, beam modes, waveforms)

- Enabling adaptability to the scenario and the operational conditions

- Supporting innovative antenna design (e.g., ubiquitous approach decoupling the observed area from the physical antenna position, conformal arrays)

- Enabling operation in multi-static radio-frequency system architectures, especially taking into account synchronisation issues;

- Capable of coping with increased data rate and volume with respect to signal acquisition and data processing

- Demonstrating modular and scalable architecture with suitable weight, size and power consumption (SWaP) to be implemented over a variety of platforms (including airborne applications as well as unmanned vehicles)

- Ensuring compatibility with simultaneously operated civil systems (including telecommunication applications) and defence systems;

- Ensuring interoperable interfaces and data formats with other military and civil sensor systems.

Expected impact

- Contribution to the capacity and the technological autonomy of technological and industrial actors in the EU Member States and Norway to develop new radio-frequency systems.

- Building capability to define, develop and operate radio-frequency systems for surveillance, detection, tracking and classification of objects that are difficult to detect and track in increasingly difficult environments and operating conditions.

- Increased flexibility of radio-frequency systems to create multifunctional, fully digital systems, able to adapt to the situation and the environment.

- Enhancement of the integration of radio-frequency systems in distributed control and surveillance platforms.

EDF-2022-RA-CYBER-CSACE: Adapting cyber situational awareness for evolving computing environments

Objectives

General objective

An increasing number of malicious actions targeting governmental and strategic systems occur in cyber space. New or improved solutions, technologies and applications for enhanced cyber situational awareness (CSA) are essential to counter these threats. To address evolving and more complicated activities in cyberspace, including challenges that arise due to the ongoing evolution of battlefield network and systems, decision makers and Security Operation Centre (SOC) operators need the most updated CSA related to cyber threats, in real time, gathering internal and external cyber information. CSA denotes the capability for a decision-maker to know what is going on in the cyber domain in order to be able to make informed decisions and adequately respond to incidents.

Specific objective

CSA needs to be supported by technology to collect, correlate and fuse the several sources of data as well as their different nature (e.g., network, mission, open-source intelligence, structured and unstructured threat awareness) to provide the necessary information so that human decision-makers can assimilate the situation. Cyber threats continue to grow in complexity and scope, new and evolving threats arising from advancing adversary campaigns and tactics and at the same time the volume and diversity of cyber threat intelligence grows all the time. It poses challenges to human operators to visualise and comprehend the variety and volumes of information produced by dynamic and fragmented networks and systems in a battlefield context. The evolving computing challenges will require improved mission awareness capabilities through Cyber Threat Intelligence (CTI) establishing interfaces with sources of information considered relevant for the planning and conduct phases of an operation in order to provide real time mission information at the correct level of granularity to the common operational picture (COP).

Scope and types of activities

Scope

The overall goal is to explore novel concepts and operational opportunities for providing to the Commander essential intelligence about the adversary, their capabilities and objectives while operating in and through cyberspace. CTI enhanced with a Semantic Threat Enrichment module able to analyse both data coming from public repositories and the dark web to generate Indicators of Compromise (IoCs) and Indicators of Attacks (IoAs) will support Cyberspace Operations.

The proposals are expected to develop novel solutions leveraging full-spectrum cyber defence (physical, logical, cyber persona) under an adversarial-focused perspective. The proposals are expected to aim at CSA-supporting technology with a view to provide the necessary technical information elements that are needed to process the vast amounts of information in order to produce from tactical to COPs, as well as other technical artifacts to be used by decision-makers in need of CSA. This includes creation of graphics like timelines, histograms or relationship graphs, personalized dashboards, and reports according to the responsibilities of each user. Special attention shall be paid to the interoperability and collaboration with existing solutions at Security Operations Centre (SOC), Network Operations Centre (NOC) and Computer Emergency Response Team (CERT) level, where duplication of effort is to be avoided.

The proposals are expected to cover state of the art technologies. Enhanced situational awareness information handling and visualisation systems are expected to have a capability to present overarching views of the battlefield environment through COPs via data exportable modules of logic information to be interoperable with other operational pictures be at land, sea, air or space, taking into account ongoing evolution of the C2 military systems towards the Internet of the Military Things (IOMT) scenario which poses additional complexity, and sustain against a massive attack to critical battlefield system.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)

(e)	**System prototyping**[22] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[23] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[24] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must include studies and design. The proposal may include generating knowledge and integrating knowledge activities.

The following tasks must be performed as part of the required activities:

- Development of a number of typical user scenarios based on stakeholder needs. Entails analysis of battlefield IOMT technology requirement and their impact on the collection, correlation and presentation of information. It will include advances in terms of organisational, leadership and human training capability aspects. These will take into consideration human-machine interphases and performance optimisation in e.g., cyber SOCs.

- The use of the digital twin concept and human factors analysis to improve operator information acquisition and processing through enhancing the current COP artefact technologies. Digital twins can allow to overcome operational technology (OT) constraints due to the need to be continuously operational and the fact they often provide only limited in-depth analysis capabilities. Digital twins can run in parallel to their physical counterparts and allow inspection of their behaviour without the risk of disrupting operational services.

- Development of different hierarchical models to support IOMT mission awareness. These should establish means of aggregating dependency information to propagate only mission relevant, abstracted information rather than entire network configurations. Moreover, these systems must be able to exchange dependency information between and across federated IoT systems from different organisations/trust domains.

- Design of an AI multi-stage (i.e., multi kill chain steps) attack detection architecture that maps AI-based anomaly detection models onto the distributed enterprise infrastructure. This will enable efficient temporal and spatial correlations of the event streams from different endpoints. This is expected to exceed the performance of conventional centralized security systems through improved detection of cross-network attacks and greatly reduced data communication. Moreover, it is essential to integrate threat

[22] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[23] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[24] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

modelling and sharing with attack detection to achieve efficient real-tie detection using AI.

- The use of federated learning to create a collaborative intrusion detection system (CIDS) to enhance the inter-domain sharing of mission-oriented CTI as well as remove many of the trust and privacy issues associated with CTI sharing. In this approach no actual alerts are shared, rather the AI model parameters are shared. This will ensure that there is no leakage of sensitive network, organisational or personal information. Moreover, the CIDS pattern can be implemented within a single organisation through judicious partitioning.

- The use of digital ledger technologies to facilitate more dynamic and incentivised mission-oriented CTI sharing analysis between organisations well as increasing trust in sharing of intrusion model parameters between cross-domain federated learning entities will be investigated.

The following tasks may be performed as part of the eligible activities:

- linking observed tactics and techniques to specific Advanced Persistent Threat (APT) behaviour, which may assist with adversary characterization and identification;

- use of deception technologies, including decoys, both for monitoring the threat landscape and attackers' behaviour, and for intrusion detection. Particular attention should be on making the data from such systems can be presented in useful ways, and integrated with other sources of information;

- use of machine learning technology.

The proposals must substantiate synergies and complementarity and avoiding unnecessary duplication with projects awarded under EDIDP calls for proposals.

Functional requirements

Proposals should meet the following functional requirements:

- Definition of a number of use-case scenarios to test the concept.

- Development of proof-of-concept implementations to verify the operation.

- Design of a cyber-range-based environment simulation to both generate representative data sets to validate the AI models and to provide a testbed to evaluate the overall concept.

Expected impact

The outcome is expected to contribute to:

- Better understanding of how CTI along with future technology will be able to support an analyst's build-up and conservation of a high level of CSA.

- Improved visualisation metaphors and information handling processes arising from IOMT scenarios.

- Improved CSA management through simulation capabilities provided by digital twins.

- Improved mission-to-asset awareness for IOMT supported mission infrastructures.

- Increased CTI sharing due to use of federated learning to prevent leakage or need to share sensitive information.

- Better understanding on the use of distributed anomaly detection in both single organisation constituencies as well as the effectiveness of collaborative intrusions on improving attack detection.

EDF-2022-RA-SPACE-RSS: Responsive space system

Objectives

General objective

The general objective of this research topic is to pave the way towards a future European responsive space system able to place small satellites in various types of orbits within a short notice in order to address specific operational needs, including tactical ones, and capability gaps stemming from shortage, failures and damages of existing space assets. This is particularly relevant in the field of intelligence, surveillance and reconnaissance (ISR) and satellite communication (SATCOM) where space assets have to be continuously operational and available to monitor and react to risks and events.

Such a responsive space system will enhance the resilience and autonomy of the Member States, Norway and of the European Union in the fields of 'access to space' and 'space capabilities for defence applications.

Specific objective

The specific objective of this topic is to define the concept of operations (CONOPS) of such a responsive space system and to identify and compare suitable and affordable architectures and solutions for the end-to-end system. In order to be able to provide mission critical responsiveness in terms of reconstitution, replenishment or augmentation of space assets, the responsive solutions need to be considered within a broader space defence ecosystem. In this respect, the multiple logistical challenges required by an end-to-end system that needs to operate at a tactical pace should also be taken into account.

Scope and types of activities

Scope

Project proposals must address collaborative defence research on the CONOPS and architecture of a responsive space system composed of a launch infrastructure (including fixed sites and/or mobile carriers), launch vehicles and spacecraft (satellite platforms and payloads) concepts as well as the ground segments and stations needed to operate the launcher and the satellite/payload. Project proposals must consider various options for each component of the system based on existing solutions, adapted solutions and/or new developments. In particular, terrestrial, maritime or airborne launch solutions must be considered.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (optional)
(e)	**System prototyping**[25] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[26] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[27] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The following tasks must be performed as part of the mandatory activities (studies) of the project:

- consolidation of CONOPS from end-users, from user request for launch and preparation of the launch to ground and space segment interaction during launch and orbital phases;
- identification of main mission use cases for the responsive space system;
- preliminary analysis of the applicable regulatory framework (*e.g.,* compliance with NOTAM[28]/NOTMAR[29] requirements, launch security and safety requirements including stage re-entry, mission abort…);

25 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.
26 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.
27 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.
28 Notice to air missions.
29 Notice to mariners.

- definition of the overall conceptual architecture for the end-to-end system and associated high level requirements; the system must include the following subsystems:
    - the launch infrastructure ensuring the purposes of launch preparation, launch pad and launch range (including fixed sites and/or mobile carriers);
    - the launch vehicle (rocket);
    - the spacecraft composed of satellite platforms and of a family of sensors dedicated to missions;
    - ground segments for the launcher, the spacecraft, including fixed/mobile ground stations for space data reception and the necessary means of encryption;
- identification of high-level requirements for the launch infrastructure and of suitable launch zones to launch terrestrial, maritime or airborne systems on short notice:
    - identification of suitable starting points (where the carrier departs) and launch areas (where the launch vehicle departs). Starting points must consider terrestrial, maritime or airborne mobile carriers;
    - this must include an overview and comparison of all existing and new planned launch sites having assembly, integration and test (AIT) and storage facilities and possibility to host mobile carriers in the EU or associated countries with their individual pros and cons (*e.g.* vertical, horizontal, maritime launch and airborne launch concepts; safety und ecological implications; suitability for one or more launch providers; reachability by truck, airplane, train;; reachable orbits; security measures to handle defence systems);
    - this task must consider phases from pre-flight to mission preparation and execution (including management of prepositioned payloads, propellant loading systems, *etc.*);
- identification of high-level requirements for the launch vehicle:
    - including volume under fairing, standardization requirements (including fairing interface), propulsion type, injection precision and required deltaV, operational life expectancy;
- identification of high-level requirements for the spacecraft:
    - types and related performances (minimum standards);
    - standardisation, affordability and modularity/flexibility should be part of the analysis;
    - ability to be merged with the orbital upper stage should be looked at;
- identification of high-level requirements and definition for the ground segments and stations needed to operate the launcher and the satellite mission (platform and payload);

  - this task should include analysis of security requirements (encryption);

  - this task should also include a preliminary analysis of the sharing and booking mechanism for the system;

- identification and analysis of existing solutions able to meet the requirements and of needs for adaptations or for new research and development actions with their associated roadmap;

- costs vs benefits analysis (informed by CONOPS and architecture definitions) of the different options identified;

  - comparison of the proposed options in terms of costs / coverage of use cases and associated performances / safety constraints / logistics constraints / other implementation constraints / potential of evolution (*e.g.,* reachable orbits, increased mass…);

  - the analysis must take into account the lifecycle cost including launch infrastructure, launch vehicle, spacecraft (satellite platforms and payloads), ground segments, including all required ground facilities for prepositioned payloads, pre-flight operations including propellant loading, cryogenic (if needed) storage solutions, safety storage facilities for solid, hybrid or liquid propulsion, end-to-end maintenance, repair and operations;

  - the analysis must also take into account the logistical aspects and include preliminary technical and logistical trade-offs between propulsion solutions;

- preliminary requirements review (PRR) guided by the end-users (from Members States and Norway).

The following tasks may be performed as part of optional activities (design) of the project:

- simulation of the achievable responsiveness (end-to-end performances) of selected options for selected mission use cases / scenarios;

- preliminary design of selected sub-systems (to be proposed by the applicants).

Functional requirements

The responsive space system is expected to meet the following requirements:

- time between request for launch and positioning into orbit should be less than 72 hours including flight range safety measures. Time to operational data delivery can be shorter, depending on the precision of orbit injection, the type of orbital propulsion, the type of sensors and related calibration in space;

- ability to reach any low earth orbital plane, from equatorial to sun-synchronous polar orbits, while minimizing the operating and logistical constraints (operable from various types of areas);

- ability to place a satellite between 20 kg and 200 kg into an orbit of at least 400 km.

Expected impact

The action should produce the following expected impacts:

- set the basis for the development of a responsive space capability not yet available at European level;
- creation of a sovereign supply chain in Europe for defence capabilities in the domain of responsive space systems;
- leveraging the European defence technological and industrial base in the domains of launch infrastructure (including mobile carriers), rockets and satellite platforms and sensors;
- extension of EU launch solutions portfolio and strengthening of the EU autonomy in this field.

EDF-2022-RA-DIGIT-DBIR: Shared databases and integrated systems for image recognition

Objectives

Image recognition technologies become essential for defence applications. There is in particular an increasing need for forces to analyse their environment more efficiently in order to enhance decision-making, responsiveness and survivability while ensuring the observation function effectively. This need is reinforced by the emergence of new forms of threats such as hypersonic, swarming, miniaturised or stealth weapons, which require increased speed, sensitivity or accuracy of the recognition systems. This need applies to manned and unmanned platforms as well as to wide-area or long-lasting surveillance.

Besides, databases are essential for training, testing and certifying artificial intelligence (AI) systems such as image recognition systems. However, collecting data that is both representative of military operational scenarios and sharable for AI system development is a complex task. Furthermore, data annotation (e.g., definition of regions in images, labelling…) and curation need significant efforts that are often underestimated. The lack of specialised entities missioned to serve the community by actively creating representative and sharable databases further hinders the creation of such databases. These issues are often a bottleneck in system development. Frameworks should be developed that enable or facilitate cooperation and sharing of image databases for defence.

In addition, new high-resolution sensor technologies provide larger amounts of information that are difficult to transmit in their entirety in real time. Automatic processing located near the sensor is needed to reduce the information flow. This requires joint optimisation of software and hardware and can involve trade-offs between recognition performances and integration constraints.

Scope and types of activities

Scope

Proposals should address the development and objective testing of image recognition systems for defence, the creation of the needed new databases, and the integration of the developed image recognition technologies near the sensors and objective testing of these integrated systems. Any relevant types of images and sensors (visible, infrared, multiband, hyperspectral…) and any well-defined types of recognition tasks (detection and classification for well-defined classes of objects, detection and identification of known objects, tracking…) can be considered.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (mandatory)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (optional)
(e)	**System prototyping**[30] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[31] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[32] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must address in particular the following:

- Creation and sharing of annotated image databases, and development of appropriate frameworks for that purpose
- Development of software image recognition systems
- Integration of such software systems on customised hardware near sensors (integrated technology demonstrators)

30 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

31 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

32 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Objective evaluation of the performances of the software and integrated systems

Functional requirements

The proposed solutions should fulfil the following requirements.

- A limited number of well-defined use cases should be addressed (possibly one).

- For each use case addressed:

  - The use case should address well-identified military operational needs and scenarios.

  - The use case should be defined by clear evaluation data, metrics and protocols described in the proposal. Evaluation raw data should be real images directly acquired through sensors. However, if real images do not yet exist (for instance for future threats) but hybrid or synthetic images can be expected to be representative of the anticipated threats, such images may be used.

  - Several approaches should be explored by different research teams (while being evaluated in a comparable way using the above-mentioned data, metrics and protocols). The proposed techniques should be presented in the proposal.

  - The state-of-the-art should be described in the proposal, relying as much as possible on past objective and quantitative evaluation results. The expected progress beyond the state-of-the-art should also be described, taking into account the foreseen amount of new training data and/or the ability to make a better use of existing data through innovative learning techniques, and a possible roadmap toward technological maturity beyond the project should be provided.

  - The needed image data should be collected, relying on dedicated trials and measurement campaigns as needed. Images should be annotated using documented annotation guidelines. The resulting databases should be shared at least with the project partners who need them in the framework of the project.

  - The possibility to share and reuse these databases beyond the project should be anticipated, including where they would be classified. The organisational and technical framework for data production and sharing should be described in the proposal. In particular, the entity in charge of curating and distributing the databases should be clearly identified and the conditions for sharing should be described. If hybrid or synthetic images are needed for system evaluation, the possibility to share the tools used to generate these images should be anticipated in the same conditions.

  - Setting up a framework for data production and sharing that can be reused beyond the project is encouraged. Synergies with similar efforts at the European level should be sought.

  - Training and evaluation data should be representative of the use case and cover the various conditions encountered in real-life scenarios

(e.g., various climate, weather or lighting conditions, various types of background landscapes…).

- If representative data that can be collected by users during operations is deemed needed to reach the expected system performance, machine-learning techniques to learn continuously from user supervision (user-driven adaptation) should be considered.

- Software recognition systems should be optimised to offer the best possible recognition performance (e.g., high probability of correct detection and low false alarm rates, high area under the ROC[33] curve…).

- Integrated recognition systems should maintain the recognition performance of software systems as much as possible while taking into account size, weight, power and cost constraints.

- Both software and integrated systems should be benchmarked using the agreed-upon evaluation data, metrics and protocols.

Expected impact

The expected impacts are:

- Shareable databases for image recognition
- Established frameworks easing the production and sharing of databases, creation or reinforcement of entities producing sharable databases
- Availability of new integrated image processing products
- Enhanced decision-making and responsiveness, reduction of cognitive load of soldiers during operations
- Enhanced situational awareness
- Enhanced safety, resilience and survivability
- Reduction of fratricides and collateral damages
- Enhanced unmanned system autonomy

EDF-2022-RA-ENERENV-CUW: Sustainable components for underwater applications

Objectives

Piezoelectric materials used for military applications, especially in underwater acoustics, are to a very large extent based on ceramics, more specifically, on lead titano-zirconate Pb1-xZrxTiO3 (PZT). Civilian and military users now face challenges with European regulations regarding lead and its derivatives identified in the Candidate List of the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) regulation from 2012, with the risk of its inclusion in the Annex XIV (substances under authorization) in the coming years. This is a concern for sonar systems used in underwater applications utilising piezoelectric ceramics. In addition to

[33] Receiver Operating Characteristic.

the REACH regulations, other global regulations, such as the Restriction of Hazardous Substances (RoHS) or Waste Electrical and Electronic Equipment (WEEE), require the elimination of lead and its salts from consumer goods and industrial devices. These constraints and regulations stimulate the need for an increased technological and industrial maturity of piezoelectric material alternatives to PZT. As an example, the recent update of the European RoHS directive has precluded the use of PZT ceramics from July 2021 for civil applications.

General objective

The general objective is to replace existing PZT based ceramics with alternative technologies, such as lead-free piezoelectric materials (aspiring to have no reduction in performance levels with even the potential for a gain), which will be suitable for military underwater applications, including the most demanding, which is a passive hydrophone and active transducer for sonar and underwater communications. The overarching goal is to have the emergence of at least one European lead-free piezoceramic supply chain, which will soon be mandatory with regarding the European REACH regulations. The patenting of new formulations and processes would be of use for sonar applications.

PZT ceramics are used in most acoustic sensors for underwater military applications: hydrophones, sonobuoys, dipping sonars, variable depth and hull mounted sonars, torpedoes, towed arrays. With the launch of major fleet renewal programs, which are currently entering the implementation phase, the R&D of the naval sector has the challenge to control the environmental impact and the safety of ships, while preserving acoustic performance.

Since the renewal of scientific work on the replacement of PZT, started around 2000, considerable research has been conducted in studying substitution ceramics, with promising results. Research on demonstrators integrating lead-free piezoelectric ceramics and crystals based on BT[34], KNN[35], KN[36], BCTZ[37] has been published in scientific literature. However, gathering all the properties of PZT materials to alternative lead-free piezo-electric materials has never been done, and this is the reason academic research is still extremely active in this sector. In addition, reproducibility and process up-scale raise numerous issues.

Apart from military sectors, civilian markets are very broad and extend to several domains (non-destructive control sensors, medical echography apparatus, automotive, printing, energy harvesting). Even if civilian markets are very broad and potentially less demanding in terms of physical and piezoelectric properties than military domains, very few lead-free piezoelectric materials are proposed at industrial level and their physical and piezoelectric properties are very far from PZT. This means that mastering the production of advanced and high performance lead-free piezoelectric materials at an industrial level remains challenging. For the time being, no lead-free solutions exist that facilitate the high level of performance required by military underwater applications.

Specific objective

The specific challenge is thus to advance the state-of-the-art in the research of, and innovation in, new high performance lead-free piezoelectric materials for military underwater sensors applications to replace PZT, with a view to future phases of

[34] Barium Titanate
[35] Potassium Sodium Niobate
[36] Potassium Niobate
[37] $Ba_{0.85}Ca_{0.15}Ti_{0.9}Zr_{0.1}O_3$

development and industrialization, leading to the prospective establishment of at least one European supply chain in this domain.

New materials can also provide the opportunity to generate additional benefits, for example, enlarging the operational frequency bandwidth of sensors or source generators, improving duty cycle limitations or reducing the sensor size. These opportunities can upgrade the performance of the sensors and should hence be considered in the evaluation of materials and processes to be studied.

Scope and types of activities

Scope

The proposals should carry out research actions for the development of advanced lead-free piezoelectric materials with physical and piezoelectric properties, enabling the substitution of PZT in military underwater applications. These research actions may be extended to disruptive ceramic technology processes, such as 3D printing, and material engineering to enhance current piezoelectric properties. Moreover, increasing the technological maturity of lead-free piezoelectric materials for PZT substitutions in military underwater applications, and assessing these new materials for military underwater applications on representative test transducers could also be considered. Furthermore, increasing the manufacturing readiness level of promising lead-free piezoelectric materials and enabling one or more European industrial suppliers of lead-free piezoelectric materials for sonar transducers is a benefit of research activities in this area. In addition, the proposal must pay particular attention to potential synergies and complementarity to other ongoing R&D projects at national, multinational and on-going dual-use initiatives at European Union level, to avoid unnecessary duplication.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (mandatory)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (optional)

(e)	**System prototyping**[38] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[39] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[40] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must cover the following activities:

- Generating knowledge, with in particular:
  - The review of the scientific and industrial state-of-the-art lead-free piezoelectric materials and innovative synthesis processes
  - The identification of the relevant materials and processes
  - The identification of manufacturing technologies for lead-free piezoelectric materials
  - The review of the available operational specifications
  - The definition of a roadmap for materials and processes development
- Integrating knowledge, with in particular:
  - The identification and assessment of EU industrial suppliers for the production of lead-free piezoelectric materials, including technology transfer.

In addition, proposals may address:

- Studies, with in particular:
  - The formulation, synthesis, physical and structural characterization, piezoelectric characterization of new composition of lead-free piezoelectric material.
  - The study of innovative process alternatives to current ceramic machining and advanced sintering processes.
- Design, with in particular:

[38] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[39] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[40] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- The material specifications and advanced material characterization (piezoelectric tensor measurement) at sample and transducer levels.

- The integration of parameters in transducer modelling, fabrication of representative transducer, which should be partially tested in real environmental conditions (e.g., assessment of linearity response with respect to stress and temperature, pressure and temperature cycling, endurance tests).

Functional requirements

The research to be conducted should meet the following functional requirements:

- Replace PZT by lead-free suitable piezoelectric materials and assess their performance level, aspiring to have no loss in performance or even a potential gain, against the following (not exhaustive):

  - For Active transducers: maximal Source Level, matched electrical bandwidth, power density, efficiency, and more generally for high drive, temperature, stress and electric field handling, duty cycle, power linearity

  - For Passive transducers: signal to noise ratio, stress handling (depth rating/for deep-sea applications), frequency bandwidth, and sensitivity.

- The choice of lead-free piezoelectric materials may differ depending on military underwater applications (passive or active transducers), and different use cases should be addressed. For both use cases (active, passive), the loss, or gain, versus actual PZT transducers will be addressed through a redesign phase of equivalent lead-free transducers. These lead-free transducers shall undergo a series of pre-qualification tests (not exhaustive):

  - Functional evaluation: source level, signal to noise ratio, sensitivity, frequency bandwidth, directivity, efficiency, linearity with power, endurance test

  - Environmental evaluation: pressure and temperature cycling, vibrations, shocks.

Expected impact

The research should contribute to:

- reduction in pollution, which is a part of the European Green Deal,

- Strong technological differentiators compared to non-European sonar suppliers,

- Emergence of one or more European supply chains,

- Patenting of new formulations and processes,

- Compliance with REACH regulations on hazardous substances and obsolescence anticipation,

- Sustainability components for underwater applications

EDF-2022-RA-MATCOMP-PACOMP: Packaging technologies for critical defence components

Objectives

General objective

Future defence systems that target information superiority, new communication capabilities, new battlefield operations, combat capabilities and inter-theatre air operations require electronic components with high performance and multiple functionalities. Systems such as radiofrequency (RF) sensors for radars or electronic warfare systems, intelligent processing platforms or hardware-secured/cyber-secured modules need to be highly integrated and to fulfil specific military requirements. A particular challenge for defence forces is the digital control of the RF spectrum. For example, digital radar equipment will be driven mainly by components like analog-to-digital converters (ADC), digital-to-analog converters (DAC), the RF frontend, which will be mainly characterised by a transmit (high power amplifier - HPA) signal chain and a receiver (low noise amplifier - LNA) signal chain, and a robust switch, setting the mode of operation.

Specific objective

The performance of such a system will not only depend on the performance of the single chips used for each component but also on the quality and efficiency of their integration into packages and the optimization of their interplay with respect to the targeted application. Advanced packaging technologies are key to obtain compact, robust and reliable electronic components by integrating and encapsulating multiple electronic chips. The resulting Multi-Chip Modules and/or System in Packages (SiP) can provide high performance and multiple functions. Packaging with short interconnections between components minimizes parasitic elements that degrade signal integrity. This is particularly relevant for next generation radio-frequency application (e.g., radars or electronic warfare systems). Furthermore, an advanced density of integration allows hiding sensitive signals and integrating protection features, which is relevant for anti-tamper and secure module solutions.

Packaging technologies can also increase the resilience of supply in key technology areas, reducing dependence and improve security of information by allowing the use of components of different technologies and from different sources within a quality and security assured process. This is particularly relevant for defence applications for which securing the EU supply chains of critical electronic components is challenging due to small manufacturing volumes and potential constraints such as export restrictions.

Scope and types of activities

Scope

The topic addresses advanced System-in-Package technologies and architectures that take into account needs of defence systems with a particular focus on radio-frequency applications. It addresses improvement of packaging technologies, the preparation of design tools and the preparation of pilot lines.

The System-in-package should contain various types of elements (e.g., passives, high-speed digital components, ADC, DAC, memory components, microelectromechanical systems (MEMS), optical component) made of different materials (e.g., Si, SiGe, III/V semiconductors such as GaN and GaAs, RF complementary metal-oxide-semiconductor (CMOS)) and produced by different processes (semiconductors technology nodes both manufactured in the EU or Norway and outside.). A package should combine digital and analogue functions and

integrate, if adapted to the considered application, further security functions and thermal management functionalities.

Proposals should strive to identify a supply chain from actors from the EU and Norway offering independent OSAT (Outsourced Semiconductor Assembly and Test) services, in order to reinforce an EU and Norway industrial sovereignty independent from any usage constraints. As appropriate, proposals should take into account different technologies (such as Fan-Out Wafer Level-Packaging – FOWLP etc.) for creating the System-in-Package.

Relevant use cases for defence applications include RF sensors (Radar, electronic warfare including high power source for jamming, millimetre wave communications), data security and smart sensors for ammunitions.

Size, weight and power dissipation are of high concern for embedded applications. Moreover, the use in harsh environment should be taken into account. This can include aspects of G-hardening, shocks and thermal conditions, e.g., necessary for gun-launched applications or brutal landing on aircraft carriers.

This topic is linked to the sectoral analysis performed by DG DEFIS and studies performed by EDA in the framework of the CapTech TCM. Synergies between defence, space and civil technologies have to be taken account in order to avoid duplication costs.

Where applicable, proposals should build on skills, technologies and associated industrial capacities that are partially available in EU and Norway for defence or for civil applications. The proposals must substantiate synergies and complementarity with civil initiatives, notably supported by EU programmes in the space sector. It must avoid unnecessary duplications with other EU, intergovernmental or NATO initiatives.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)

(e)	**System prototyping**[41] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[42] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[43] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

Among other tasks that the applicants deem necessary, the following tasks must be performed as part of the mandatory activities of the project:

- Integrating knowledge:
  - Research activities on materials (e.g., innovative substrate), interconnect technologies and components for high-performance packaging, including tests of candidate technologies
  - Research activities on the integration of heterogeneous components and necessary interfaces, including experimental testing.
- Studies
  - Evaluation of different modular architectures and targeted platform technologies (such as FOWLP)
  - Identification of chiplets categories needed for relevant defence applications such as RF sensors, digital security, IMU (Inertial Measurement Units), etc.,
  - Definition of relevant chiplet interfaces that enable integration of the chiplets in advanced packaging, taking into account open initiatives focussing on civil applications for standard functionalities.
  - Assessment of requirements and common candidate technologies for a wide range of different defence applications, and specifically the interface between die and package to ease integration of chiplets
  - Definition of a test strategy to ensure safety and security standards for low-volume heterogeneous integration
  - Taking into account the outcome of the design activities, identification of the best supply chain per technology and use case application

41 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

42 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

43 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

(sensitive or not) compatible with real production (Manufacturing Readiness Level aspect)

Proposals may additionally include the following tasks under this activity:

- Study on the set-up and management of a shared library for chiplets

- Design

  - Definition of System-in-Package modular architectures, including those based on chiplets, supporting RF sensors, digital security, inertial measurement units (IMU), etc., and technologies for functions with military specificities

  - Define design methodologies and set up physical design kits (toolbox, modular physical design kits, multi-physics design) for the targeted technology platforms, taking into account the specificities of military systems.

  - Design of physical interfaces for components (or chiplets) that optimize integration in the package.

  - Design of selected common interface protocols for components (or chiplets) that enable reuse and optimize integration in next generation SiP platforms

  - Develop demonstrators of common interface test chips (such integrated passives including switches, protocol bridges and links, test structures…), integrate and test them on a SiP technology demonstrator platform

  - Design of test structures that can ensure safety and security standards for low-volume heterogeneous integration

  - Design of technological demonstrators taking into account the defined use cases

  - Testing in at least two iterations of the technological demonstrators, including reliability tests, for the evaluation on relevant platforms and including a failure analysis, if applicable.

  - Design of a pilot line, including the strategy of test and feasibility tests.

Functional requirements

Proposals should address technologies and solutions that fulfil the following requirements:

- Compatibility with several defence applications, including active electronically scanned array (AESA) radar preferably targeting X-Band and above, electronic warfare including high power source for jamming, millimetre wave communications, data security and smart sensors for ammunitions

- Optimization for radio-frequency applications with high-power, low signal

- Modularity and configurability to meet various requirements of different military applications.

- Optimization of size, weight, cost and power dissipation capability
- Integration of solutions against reverse engineering and enemy observation (like anti tampering and tempest)
- Compliance with the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) and Restriction of Hazardous Substances (ROHS) regulations
- Compliance with the military standards (e.g., MIL-STD 810…) for the target applications (e.g., taking into account requirements for aviation certification), in particular with respect to harsh environments, G-hardening, shocks and extreme thermal conditions

Expected impact

- Increase level of skill and knowledge in the European Defence Technological and Industrial Base concerning advanced packaging
- Create System-in-Package reference architectures and technological solutions for next generation military systems
- Strengthen the independence and competitiveness of the European supply chain for low-volume technologies and solutions that fulfil military requirements by enabling a heterogeneous integration approach (combining European based semiconductor components and non-European advanced nodes components)
- Enhance security of information by defining adapted test strategies and methods for risk mitigation
- Guarantee the access to packaging services to the EU Member States and Norway
- Promote a collaboration network between EU Member States and Norway including academy, research centres and industry looking for synergies with civil initiatives.

EDF-2022-RA-PROTMOB-FMTC: Future mid-size tactical cargo aircraft

Objectives

Tactical transport aircrafts are the workhorses of battlefields, fulfilling missions like airdrop delivery, parachutist drop, logistics, medical evacuation (MEDEVAC), air to air refuelling, special missions under harsh and adverse conditions, which are critical for the success of military operations. Operations in hostile environments demand e.g., built in electronic warfare self-protection systems and set requirements on the platform performance/build up in order to be suitable for the task, and furthermore to operate with limited ground infrastructure (e.g., unprepared runways).

Beyond their pure military role, tactical transport aircrafts are also key assets for a better civil defence/protection and EU-internal needs, with critical contribution to disaster relief, search-and-rescue and sanitary crises response.

Beside the A400M, which is on the high-performance side of the capacity, the initial conception of the majority of currently operating tactical aircraft (C130, C-295, C-27J…) is now 40 years old, and there is a need for a new medium tactical European aircraft, lighter than the A400M that could provide a complementary capacity for tactical transport.

Currently, some EU Member States are operating medium payload tactical military transport aircrafts within their fleet, which can be replaced with growing capabilities,

able to cope with the envisaged operational challenges.

The Future Mid-size Tactical Cargo aircraft (FMTC) feasibility study proposal for EDF 2022 addresses this coming strategic gap within the European transport portfolio. FMTC proposes a cooperative analysis of the transport aircraft replacement needs on the 2030-2050 horizon and the identification of European development opportunities, among the EDF participating Member States and associated countries.

This topic is an opportunity for Europe to federate efforts by providing the EU defence community (nations and industry) with robust elements to decide what the 2035+ future of EU military tactical transport could be.

Scope and types of activities

Scope

The scope must cover the feasibility study phase of the possible development of a future tactical transport aircraft.

Proposals must include at least the following activities:

- Feasibility Study for one or two aircraft, depending on the convergence on the requirements by the participating Member States and associated countries;
- Preliminary requirements review (PRR) accepted by the cooperating Member States and associated countries, which will confirm the technical, programmatic, industrial and market feasibility of the analysed solutions, giving participating States all necessary elements to select the aircraft configuration that could be carried forward through a development and industrialization phase.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (optional)

(e)	**System prototyping**[44] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[45] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[46] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

In particular, proposals must address:

a) Technical activities:

- Definition and assessment of the candidate aircraft solutions (one or two aircraft alternatives);
- Assessment of the preliminary technical specifications, concept studies and sizing for major sub-systems (propulsion, avionics and general systems);
- Identification of critical technologies for technical and economic feasibility, and proposal of pre-development plans. Specific areas of interest are:
  - design and manufacturing technologies to reduce acquisition and maintenance costs;
  - technologies towards lower or zero emission production and operation;
  - technologies to improve operational availability.
- Identification of critical technologies to improve the operational capability in the domain of:
  - take-off and landing in challenged environment;
  - wide range and low consumption;
  - self-protection capabilities;
  - more autonomy;
  - improved connectivity in the operational theatre.

[44] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[45] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[46] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

b) Programme activities:

- Establish the preliminary programme management and the system engineering plans;
- Establish the overall programme schedule / roadmap;
- Perform a costing evaluation exercise;
- Perform a market assessment review;
- Identify risks and constraints related to implementation, costs, schedule, organisation, operations, maintenance, production and disposal;
- Identify key technological aspects and plan for their maturation within the programme plan.

c) Operations activities:

- Define the concept of operation;
- Define the sustainment model (i.e., number of planned flight hours, layout of bases, deployments);
- Define a baseline for aircraft logistic support.

d) Iterative definition of aircraft detailed requirements:

- Perform a mission definition review (MDR) and Preliminary Requirements Review (PRR).

e) For a subsequent design phase:

- Provide a proposal for a best candidate solution based on a complete value analysis covering performances, costs, risks, modularity, manufacturability, safety, consistency with Member States and Norway' operational needs, with jointly defined detailed criteria and hypothesis.

Functional requirements

The proposition of a new aircraft development would be based on:

(1) Intangible:

- European Geo return: Development and involvement of European industries, acting as tractor for many European aerospace companies and small and medium-sized enterprises (SMEs);
- Export opportunities: Custom made to fit EU partner's requirements, with open architecture to address worldwide opportunities;
- Based on operational scenarios & threat environment 2030+ (i.e., Multi Domain connectivity).

(2) Tangible:

- Affordability, in terms of acquisition and lifecycle costs. Operating costs below similar available solutions in the market;

- Operations in demanding unprepared runways, hostile environments and tactical intra theatre operations;

- Flexibility for operating different kind of military missions and possibly reconfigurable for supporting civilian needs;

- Logistics capability: ability to carry tactical vehicles that do not fit in existing solutions;

- Multi-mission capability: ability to act as a multi-mission transport platform and be customized for specific roles;

- State of the art development, ensuring availability and reliability of the platform and avoiding obsolescence concerns;

- Sustainability along the entire product lifecycle: from the conception / production by means of digitalisation up to the product use with reduced environmental footprint due to e.g., advanced propulsion system, low weight and more efficient flight capabilities.

Expected impact

- Reinforce the European strategic autonomy in the military transport segment;

- Develop vital military capabilities in highly contested environments (e.g., tactical transport, airdrop, air assault) against technologically advanced adversaries;

- Develop EU MEDEVAC capabilities and EU disaster relief, and sanitary crisis response capabilities;

- Promote and protect the European technological and industrial ecosystem, based on a potential new aircraft development;

- Enhance cross-border collaboration (from large industrial groups to SMEs) through the opportunities offered by the several elements of the platform and its architecture.

EDF-2022-RA-UWW-UTS: Underwater manned-unmanned teaming and swarms

Objectives

General objective

This topic addresses research for future capabilities addressing moving subsurface threats using manned-unmanned teaming and swarm technologies, possibly including surface and air platforms and components, particularly in confined and shallow waters (CSW). This System-of-Systems (SoS) should enable enhanced operational efficiency and performance. The actions in this topic should address state-of-the-art, and beyond, swarm control solutions. This includes analysis of centralised, distributed, and hybrid control models. Swarm control may employ control scheme with a global or local approach and their optimised combination. The control-scheme should adopt to mission type changes as the operation evolves from one phase to another. Guidance and control strategies for the swarm are also to be considered, where inductive and swarm internal cognitive-like self-control needs to be analysed.

Specific objective

The aim is to develop swarming technologies up to at least TRL 4 and validated in seawater. The expected result of the research activities performed with the support of this call is a better mission performance result than the one obtained by an individual UxV or platform alone. This should take into account data sources of opportunity. The main challenges or factors to be solved to enable this are the following:

- The SoS shares a common objective for all the individual components
- The SoS can be composed of systems, vehicles, and platforms of different nature and capacities
- The architecture and functions need to be derived and controlled by the task or mission aim that has been defined.
- The SoS architecture and protocols enables it to utilise resources outside the cooperative system.

Scope and types of activities

Scope

The proposal for research on swarm aspects of unmanned systems and the collaboration policies that govern it, performing underwater missions, in CSW, shall address, among others, the following aspects:

(1) Mission or task-based performance by the swarm and all its components. The definition, and management of the collaborative system, dependent on the architecture defined, will aim to optimize the use of every individual to better obtain the common objective. This will require planning and control with a focus on at least the following:

a. Coordination and cooperation inside the system to share a defined space/environment and also the information obtained. Interoperability of the system within a defined architecture (centralized/decentralized).

b. Adjust to changes in the environment and optimise accordingly, while maintaining mission objective.

c. The cooperation of heterogeneous vehicles will involve the integration of a large amount information provided by different sensors.

d. The information obtained about the environment or operation must be combined, analysed and disseminated in real time in order to provide feedback to the system through interoperability standards, which should be consistent with relevant NATO standards.

e. Communication: A Shared link between vehicle and control station must be robust and reliable. Relevant protocols, such as JANUS underwater communications protocol must be taken into consideration.

f. Providing the HMI-infrastructure to control the system, taking into account different levels of autonomy.

g. The definition of the behaviour model of every individual inside the system and of different swarm collaborative models, e.g.: One mission shared by the platforms of the swarm; or swarm split in two or more squads with their own missions

(2) Participation of vehicles with different characteristics: The use of different platforms will allow the use of different capacities taking into account several aspects such as:

a. Level of autonomy and combinations of different levels

b. Movement (kinetic) characteristics

d. Types of platforms (UUV, USV, sonobuoys, gliders etc.)

e. Enabling systems installed such as detect and avoid (DAA) systems (below and on the surface)

f. Command, Control, and Communication Systems

g. In-swarm localisation, communication and coordination

h. Payloads, such as sensors and effectors

The proposed solution must give due consideration to the need to cooperate with other platforms to achieve a common goal (interoperability, information processing, security in operation, communication, detect and avoid, etc.). The resulting cooperation policies need to integrate all the existing with the new challenges arising from this kind of operation.

The proposal must give due consideration to techniques of cooperation between unmanned autonomous systems when acting as a swarm, namely task allocation/mission/route optimisation algorithms. Other, novel methods are also encouraged and invited to this topic.

Proposals that envisage unmanned and autonomous systems to work together as a squad -rather than as a swarm- (i. e each system/platform is performing a different task) are also welcome. Then the task allocation problem must be solved as well as the automatic re-tasking of the whole squad or group and each single unmanned asset. It should then also propose a solution for the automatic reconfiguration of the squad. The method of hierarchical task networks, or the method of intelligent software agents for implementing cooperation between systems/platforms can be used, but any other, alternative method can also be proposed.

An analysis and the elaboration of policies of cooperation between unmanned systems (swarming) should be described in detail in the proposal.

Appropriate level of human control must be respected also in proposals containing solutions with autonomous features.

The proposal should address SoS architecture, control, and guidance solutions of unmanned systems (swarming) and/or unmanned and manned systems in the underwater domain. This includes:

- Combinations of autonomous sub-swarms or squads of heterogeneous unmanned vehicles that cooperate and collaborate to complete different types of missions (for example anti-surface warfare ASuW, anti-submarine warfare ASW, intelligence surveillance and reconnaissance ISR, MCM, Mine-laying and transport).

- An analysis of the general aspects of the operation of a cooperative system of unmanned vehicles and platforms, where the SoS may draw upon resources available to it from systems outside the cooperative system.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (mandatory)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (optional)
(e)	**System prototyping**[47] of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[48] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[49] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must include generating knowledge, integrating knowledge, and studies activities. The proposal may include design activities.

The proposals must substantiate synergies and complementarity, while avoiding duplication, with concepts and architectures developed in complementary ongoing European work streams and projects where relevant.

The following tasks must be performed as part of the required activities:

- Articulation, and if necessary, development, of relevant military scenarios, that will form the basis for development of solutions.

47 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

48 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

49 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Improvement and creation of knowledge by in-depth research in the form of studies that address the most critical technology gaps to enable capabilities for swarms to function in dynamic underwater environments while performing military tasks. Also research topics that address other specific shortfalls of manned-unmanned teaming in the context of swarms with autonomous features must be addressed.

- The feasibility of developed solutions based on the in-depth research must be explored through technological demonstrations, trials and/or simulations in relevant military scenarios. The demonstration must include seawater (underwater) tasks for relevant parts. A final demonstration will serve as an instrument to show the industrial state-of-art performance to the military community, visualize the results of the targeted research activities, present potential military value and identify technology shortfalls that need to be addressed in subsequent activities in nations and EU

Functional requirements

The solution should enable swarm configuration optimisation taking into account mission and task, resources, environment, military scenario and threat.

The swarm, sub-swarm, individual and node control solutions should enable obstacle detection and avoidance, reconfiguration in case of failure of individuals or nodes, behaviour in case of loss of communication.

The solution should facilitate swarm control and guidance for swarm sizes up to several hundreds of individuals in multiple sub-swarm configurations.

The solutions should enable mission performance with loss of individuals, communication and control.

The solution should enable functionality in GNSS degraded and cyber contested environment.

The solution should enable in-swarm localisation and coordination. The solution should be interoperable with existing standards when relevant, including NATO standards.

Collaborative systems composed by multi domain platforms (UUV, USV, sonobuoys, gliders, etc.) operating together may face several challenges. The solution should enable:

- Ensuring bidirectional communications link between the subsea units and the mother ship or ground control station.

- Ability to use own sensors (such as towed SSS/deployable sonars, etc.) to carry out the mission of subsea monitoring, while being able to cooperate with other platforms and systems

- Ability for USV to carry on board a set of UUVs to be rapidly deployed in a certain surveillance area at relevant distance from the ship.

Expected impact

It is expected that the outcome should:

- Strengthen the European defence technological and industrial base (EDTIB) on technologies related to unmanned and autonomous swarming technologies that operate both above and below the water.

- Generate knowledge to fill capability gaps in use of underwater manned – unmanned teaming and swarms in support of naval operations

- Contribute to the interoperability and future capabilities of European forces in the area of swarm solutions for mission execution in the naval domain, including in particular the underwater domain.

EDF-2022-RA-UWW-ODAC: Underwater observation, detection, acquisition and communications

Objectives

General objective

Timely and robust detection and monitoring of moving underwater threats (such as submarines, swimmer delivery vehicles (SDV), combat divers, underwater unmanned vehicles (UUV)) in open sea and coastal waters is critical for maintaining sea control, for ensuring freedom to operate own forces, for A2AD operations, for harbour protection, for force protection, and for protection of critical national infrastructure.

Future capabilities need to be effective, mobile, adaptive, scalable, and flexible to counter threats from the underwater domain, leading to new technical and conceptual solutions to be developed. As traditional naval ships will become an increasingly scarce and expensive resource and will not be sufficient to provide the necessary geographical coverage and flexibility needed for the future, research is required on modular unmanned systems for underwater warfare with prerequisite principles of unmanned air, surface and underwater (UxV) standards.

Specific objective

Underwater communication, detection, and monitoring of moving targets are common denominators for traditional warfare areas such as Anti-Submarine Warfare (ASW), underwater surveillance, harbour protection, and seabed warfare. Mission specific sensor solutions and tactical approaches differ in these, despite having common denominators. Timely detection of moving underwater threats at sufficient range is identified as one of the biggest challenges. Providing technical solutions for underwater target detection, allowing to prepare appropriate reaction to a subsurface threat, will therefore impact the whole range of warfare areas mentioned above. The aim is to develop technological novelties at least up to TRL 5.

Scope and types of activities

Scope

The proposal for research on underwater observation, detection, acquisition and communications is expected to make an evaluation of critical technologies for detection of underwater threats for protection of maritime infrastructures and coastal strategic areas and assets, and identify novel technologies for improved situational awareness. This assessment of individual technologies will in a first stage be integrated to demonstrate an improved capability in underwater surveillance in littoral waters. This does not exclude open sea as an environment of operational use for the capability.

The proposal must cover at least the following parts:

- The first part is a scientifically focused part of research topics that today represent critical shortfalls in the process chain from sensor to underwater situational awareness and challenges in coordinated operation of unmanned system-of-systems. A strong emphasis is on the scientific quality and

relevance of these identified research topics. Technology areas and solutions for specific underwater missions, excluding MCM, that must at least be considered are: sensor systems for the detection of underwater threats at long ranges; processing methods for noise attenuation and automated target detection; technologies for target classification, positioning, tracking, and target identification; autonomy and autonomous adaptive operation of UxV; System-of-system architecture and interoperability standards; Command, control, communication and information systems in support of operations

- The second part is a comprehensive demonstration of the project results in a realistic scenario at sea, adapting them to existing UxVs, sensor and communication systems, infrastructure components, and data management systems .

An overall system-of-systems (SoS) approach must be used that puts together experimental configurations of unmanned mobile sensor platforms, rapidly deployed distributed autonomous nodes, ad-hoc underwater and radio communication networks together with an overall combat management system (CMS) for establishing situational awareness of the underwater threat.

Different components of the system of systems are expected to bring increased flexibility through a modular toolbox, comprising a range of systems focused to be deployed as autonomous sensors or to be adaptable to existing or newly developed maritime platforms.

Appropriate level of human control must be respected also in proposals containing solutions with autonomous features.

Types of activities

The following table lists the types of activities which are eligible, and whether they are mandatory or optional *(see Article 10(3) EDF Regulation)*:

Types of activities (art 10(3) EDF Regulation)		**Eligible?**
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optional)
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	**System prototyping**[50] of a defence product, tangible or intangible component or technology	No

[50] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification**[51] of a defence product, tangible or intangible component or technology	No
(h)	**Certification**[52] of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must include study and design activities. The proposal may include generating knowledge and integrating knowledge activities.

The proposals must substantiate synergies and complementarity, while avoiding duplication, with concepts and architectures developed in complementary ongoing European work streams and projects where relevant.

The following tasks must be performed as part of the required activities:

- For studies, supported by experimentation: In-depth research that address the most critical technology gaps to enable capabilities for underwater detection, classification, tracking and surveillance of underwater moving targets, as well as to enable capable and reliable communication links within the SoS.

- For design, including demonstration: a final comprehensive SoS demonstration involving state-of-art unmanned and autonomous systems that may be configured to represent a complete process chain from detection-to-awareness, playing a realistic military scenario and using realistic moving targets in real environmental conditions. The demonstration must implement results from the scientific studies in such a way that the impact of each of the studies has a potential operational capability, will be clearly visible in the demonstration. In addition, sub-systems to the SoS should be demonstrated.

The tasks must address at least:

- Methods, technologies, systems and devices for the detection of underwater moving threats at long ranges, their classification, positioning and subsequent tracking. These have to consider covert detection solutions, such as multi-static and distributed systems. Also automated target detection has to be addressed. In addition, methods related to mitigation of environmental influence on detection have to be addressed. Autonomy and autonomous adaptive solutions to ameliorate the probability of detection, classification, positioning and tracking of underwater moving targets have also to be addressed.

- Methods and technologies for robust and resilient communication for an underwater system of systems with the aim to establish situational awareness of the underwater threats

[51] 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

[52] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

A final demonstration will serve as an instrument to show to the military community the results of the targeted research activities, present potential military value and identify technology shortfalls that need to be addressed in subsequent activities in nations and in EU.

The SoS design must respect an open architecture approach and interoperability standards.

Additional tasks may address other specific shortfalls in unmanned and autonomous technologies and coordinated operation of SoS may be addressed. The following tasks may be performed as part of the eligible activities:

- Research on novel technologies for accurate target positioning and tracking. These may include solutions for active and passive arrays and towed arrays mounted on unmanned vehicles (UxV).

- Research on Command, control, communication and information systems in support of operations. For underwater communication: signal processing using novel processing techniques for robust, long range and adaptive communication, including adaptive networks. These can include novel techniques and standards for the implementation of next-generation underwater communication networks.

- Research on enablers for autonomous operations of UxVs in order to develop a consistent preliminary operational system of systems - such as; robust precision navigation, adaptive behaviour, long endurance (high efficiency energy sources), launch & recovery (e.g., UxV deployment platforms - such as military vessel specially designed to launch and recover naval UxV), underwater infrastructure networks

- Research on Human machine interface (HMI).

- Research on Internet of Underwater Things (IoUT, or UIoT) applications including all characteristic layers of IoUT (perception, network and application) and approach to solve the challenge of detection of underwater threats at long distance.

Functional requirements

The proposal should meet requirements for demonstrating a military scenario where detection, acquisition, and timely communication of underwater threats represent the core innovation part of the project.

The proposed solution should:

- Improve and speed up detection, tracking and classification of underwater moving threats especially in most demanding conditions and complex environments (coastal areas, reverberations, maritime traffic, sea state, environmental noise)

- Involve improved or new generation of sensors (active / passive sonar, magnetic anomaly detectors (MAD), hydrophones, active and passive sonobuoys, etc.).

- Have improved capabilities for underwater data connectivity to other equipment (tactical systems, multiple sensor-data fusion configurations) including in cyber-contested environments.

- Be interoperable with existing standards, where relevant, including NATO standards.

- Offer a modular and flexible design to ease the integration of new sensors and effectors (to ensure high scalability in terms of integration with existing or new sensors, effectors and subsystems)

Expected impact

It is expected that the outcome should:

- Strengthen the European defence technological and industrial base (EDTIB) on technologies related to unmanned systems, autonomy and the system-of-systems infrastructure needed to demonstrate situational awareness related to moving underwater threats.

- Identify specific research topics and generate knowledge to fill capability gaps in underwater threat assessment.

- Contribute to the interoperability and future capabilities of European forces in the area of underwater communication, detection, and monitoring of moving targets.

3. Available budget

The available call budget is **EUR 270 000 000**.

Specific budget information per topic can be found in the table below.

Topic	Topic budget	Multi-topic with common budget envelope (common ranked list)	Fixed maximum number of projects
EDF-2022-RA-MCBRN-HICP: Diagnostics, treatment, transport and monitoring of highly contagious, injured and/or contaminated personnel	EUR 25 000 000	No	1
EDF-2022-RA-C4ISR-AIRC2: Single European Sky interoperability	EUR 20 000 000	No	1
EDF-2022-RA-SENS-CSENS: Covert sensing	EUR 25 000 000	No	No
EDF-2022-RA-SENS-ART: Advanced radar technologies	EUR 15 000 000	No	No
EDF-2022-RA-CYBER-CSACE: Adapting cyber situational awareness for evolving computing environments	EUR 10 000 000	No	No
EDF-2022-RA-SPACE-RSS: Responsive space system	EUR 20 000 000	No	1

EDF-2022-RA-DIGIT-DBIR: Shared databases and integrated systems for image recognition	EUR 25 000 000	No	No
EDF-2022-RA-ENERENV-CUW: Sustainable components for underwater applications	EUR 20 000 000	No	1
EDF-2022-RA-MATCOMP-PACOMP: Packaging technologies for critical defence components	EUR 25 000 000	No	No
EDF-2022-RA-PROTMOB-FMTC: Future mid-size tactical cargo aircraft	EUR 30 000 000	No	No
EDF-2022-RA-UWW-UTS: Underwater manned-unmanned teaming and swarms	EUR 25 000 000	No	No
EDF-2022-RA-UWW-ODAC: Underwater observation, detection, acquisition and communications	EUR 30 000 000	No	1

The availability of the call budget still depends on the adoption of the EU budget for the year 2023 by the EU budgetary authority.

We reserve the right not to award all available funds or to redistribute them between the call priorities, depending on the proposals received and the results of the evaluation.

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	21 June 2022
Deadline for submission:	24 November 2022 – 17:00:00 CET (Brussels)
Evaluation:	November 2022 - June 2023
Information on evaluation results:	June/July 2023
GA signature[53]:	July-December 2023

5. Admissibility and documents

Proposals must be submitted before the **call deadline** *(see timetable section 4)*.

[53] In case of change in the management mode for a given action (see Section 3 of the EDF Work Programme), this timeframe may be different.

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the Search Funding & Tenders section). **Paper submissions are NOT possible**.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System (⚠ NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:

- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project *(to be filled in directly online)*
- Application Form Part B — contains the technical description of the project *(to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded)*
- mandatory annexes and supporting documents *(templates available to be downloaded from the Portal Submission System, completed, assembled and re-uploaded together with Application Form Part B)*:
  - detailed budget table/calculator
  - participant information (including previous projects, if any)
  - list of infrastructure, facilities, assets and resources
  - actual indirect cost methodology declarations (if actual indirect costs used)
  - ethics issues table
  - ownership control declarations

Please note that the amounts entered into the summarised budget table (filled in directly online) must correspond to the amounts calculated in the detailed budget table. In case of discrepancies, the amounts in the online summarised budget table will prevail.

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that the participants comply with the conditions for receiving EU funding (especially eligibility, financial and operational capacity, exclusion, etc). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable**, **accessible and printable**.

Proposals (Part B) are limited to maximum **100 pages** (counting the work package descriptions). Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents *(for legal entity validation, financial capacity check, bank account validation, etc)*.

ℹ For more information about the submission process (including IT aspects), consult the Online Manual.

6. Eligibility

Eligible participants (eligible countries)

In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
  - EU Member States (including overseas countries and territories (OCTs))
  - non-EU countries :
    - listed EEA countries ('EDF associated countries', *see list of participating countries*)
- have their executive management structure established in eligible countries
- must not be subject to control by a non-associated third country or non-associated third-country entity (unless they can provide guarantees – see Annex 2 - approved by the Member State or EDF associated country where they are established)

Beneficiaries and affiliated entities must register in the Participant Register — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Other entities may participate in other roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc *(see section 13)*.

⚠ Please note that, in EDF, subcontractors involved in the action[54] and associated partners–must also comply with the above-listed conditions concerning establishment and control.

Associated partners which are not established in one of the eligible countries (or which are subject to control by a non-associated third country or non-associated third-country entity) may however participate exceptionally if certain conditions are fulfilled *(not contravene EU and MS security and defence interests; consistent with EDF objectives; results not subject to control or restriction by non-associated third countries or non-associated third-country entities; no unauthorised access to classified information; no potential negative effects over security of supply of inputs which are critical for the project)*, subject to agreement by the granting authority and without any funding under the grant.

Specific cases

Natural persons — Natural persons are NOT eligible (with the exception of self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

International organisations —International organisations are not eligible, unless they are international organisations whose members are only Member States or EDF associated countries and whose executive management structure is in a Member State or EDF associated country.

[54] 'Subcontractors involved in the action' means subcontractors with a direct contractual relationship to a beneficiary or affiliated entity, other subcontractors to which at least 10 % of the total eligible costs of the action are allocated, and subcontractors which may need access to classified information in order to carry out the project.

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons[55].

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'[56]. ⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Subcontractors involved in the action — Subcontractors with a direct contractual relationship to a recipient *(i.e. beneficiary or affiliated entity)*, other subcontractors to which at least 10 % of the total eligible costs of the action is allocated, and subcontractors which may need access to classified information in order to carry out the action.

EU restrictive measures — Special rules apply for certain entities *(e.g. entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)[57] and entities covered by Commission Guidelines No 2013/C 205/05[58])*. Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

ℹ For more information, *see Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Consortium composition

Proposals must be submitted by minimum 3 independent applicants (beneficiaries; not affiliated entities) from 3 different eligible countries.

Eligible actions and activities

Eligible actions and activities are the ones set out in section 2 above.

The following actions and activities are not considered as eligible for funding under this call:

- projects that do not implement the objectives set out in Article 3 of the EDF Regulation
- projects that do not concern new defence products or technologies or the upgrade of existing defence products or technologies
- projects that do not relate to at least one of the types of activities set out in Article 10(3) of the EDF Regulation
- projects that do not cover the mandatory types of activities set out in section 2
- projects that concern products and technologies whose use, development or

[55] See Article 197(2)(c) EU Financial Regulation 2018/1046.
[56] For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.
[57] Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the EU Sanctions Map.
[58] Commission guidelines No 2013/C 205/05 on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

production is prohibited by international law

- projects that concern the development of lethal autonomous weapons without the possibility for meaningful human control over selection and engagement decisions when carrying out strikes against humans (with the exception of the development of early warning systems and countermeasures for defensive purposes).

- projects where background or results:

  - would be subject to control or restriction by a non-associated third country or non-associated third-country entity, directly, or indirectly through one or more intermediate legal entities, including in terms of technology transfer

  - and, for pre-existing information (background), this would impact the results

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).

Projects must comply with EU policy interests and priorities *(such as environment, social, security, industrial and trade policy, etc)*.

Financial support to third parties is not allowed.

Geographic location (target countries)

Proposals must relate to activities taking place in the eligible countries *(see above).*

⚠ Please note that moreover, in EDF, only infrastructure, facilities, assets and resources which are located or held in an eligible country may be used. Other assets, infrastructure, facilities or resources may be used only exceptionally if certain conditions are fulfilled (*no competitive substitutes are readily available; not contravene EU and MS security and defence interests; consistent with EDF objectives; results not subject to control or restriction by non-associated third countries or non-associated third-country entities)*, subject to agreement by the granting authority and without any funding under the grant.

Duration

Project duration:

- for all topics: between 12 and 48 months

Projects of longer duration may be accepted in duly justified cases. Extensions are possible, if duly justified and through an amendment.

Project budget

Project budgets (maximum grant amount):

- for all topics under this call: should not exceed the budget available for the topic (see table in section 3).

This does not however preclude the submission/selection of proposals requesting other amounts. The grant awarded may be lower than the amount requested.

Ethics

Projects must comply with:

- highest ethical standards (including highest standards of research integrity) and
- applicable EU, international and national law.

Proposals under this call will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

Security

Projects involving classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

Projects where the Member States of the participating beneficiaries and affiliated entities decide to establish a specific security framework under Article 27(4) of the EDF Regulation, will be subject to this specific security framework and classified foreground information (results) generated by the project will be under the originatorship of these Member States.

If no such specific security framework is set up by the signature of the grant agreement, the security rules will be governed by Commission Decision 2015/444[59] and its implementing rules[60].

These rules provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
  - created or accessed only on premises with facility security clearing (FSC) from the competent national security authority (NSA), in accordance with the national rules
  - handled only in a secured area accredited by the competent NSA
  - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know
- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving classified information may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of

[59] See Commission Decision 2015/544/EU,Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

[60] See Article 27(4) EDF Regulation.

information agreement with the EU (or an administrative arrangement with the Commission)

- disclosure of classified information to third parties is subject to prior written approval from the granting authority.

Please note that facility security clearing may have to be provided before grant signature. The granting authority will assess the need for clearing in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearing.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables *(e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc)*.

Beneficiaries must ensure that their projects are not subject to third-country/international organisation security requirements that could affect implementation or put into question the award of the grant *(e.g. technology restrictions, national security classification, etc)*. The granting authority must be notified immediately of any potential security issues.

More information on security aspects can be found in Annex 3.

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all these projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the Participant Register during grant preparation *(e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc)*. The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information
- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities *(see below, section 10)*
- prefinancing paid in instalments
- (one or more) prefinancing guarantees *(see below, section 10)*

or

- propose no prefinancing
- request that you are replaced or, if needed, reject the entire proposal.

For more information, *see* *Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project.
- description of the consortium participants (including previous projects, if any)

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Public bodies, Member State organisations and international organisations are exempted from the operational capacity check.

Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate[61]:

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct[62] (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

[61] See Articles 136 and 141 of EU Financial Regulation 2018/1046.

[62] Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain advantage.

- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- guilty of irregularities within the meaning of Article 1(2) of EU Regulation 2988/95 (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant).

Applicants will also be refused if it turns out that[63]:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, *see sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each budget envelope; *see section 3*) against the operational capacity and award criteria *(see sections 7 and 9)* and then ranked according to their scores.

For proposals with the same score (within a budget envelope) a **priority order** will be determined according to the following approach:

Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:

1) Proposals will be prioritised according to the scores they have been awarded for the criterion 'Excellence and potential of disruption'. When these scores are equal, priority will be based on scores for the criterion 'Innovation and technological development'. When these scores are equal, priority will be based on scores for the criterion 'Competitiveness. When these scores are equal, priority will be based on scores for the criterion 'Creation of new cross-border cooperation'

2) If necessary, any further prioritisation will be based on the number of Member States or EDF associated countries, in which applicants involved in the proposal are established

[63] See Article 141 EU Financial Regulation 2018/1046.

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

⚠ No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc*.

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending will be considered to have been accessed and that deadlines will be counted from opening/access *(see also Funding & Tenders Portal Terms and Conditions)*. Please also be aware that for complaints submitted electronically, there may be character limitations.

9. Award criteria

The **award criteria** for this call are as follows:

- **Excellence and potential of disruption (5 points)**
  - Excellence of the overall concept and soundness of the proposed approach for the solution, including main ideas, technologies and methodology
  - Compliance of the proposal with the objectives, scope and types of activities, functional requirements and expected impact of the topic as set out in section 2
  - Extent to which the objective and expected outcome of the proposed project differs from (and represents an advantage at strategic, technological or defence operational level over) existing defence products or technologies, or has a potential of disruption in the defence domain
- **Innovation and technological development (5 points)**
  - Extent to which the proposal demonstrates innovation potential and contains ground-breaking or novel concepts and approaches *(e.g. new products, services or business and organizational models)*, new promising technological improvements, or the application of technologies or concepts previously not applied in the defence sector
  - Integration of existing knowledge and previous or ongoing R&D activities in the defence and/or civil sectors, while avoiding unnecessary duplication
  - Extent to which the innovations or technologies developed under the proposal could spin-off to other defence applications and products

- **Competitiveness (5 points)**

  - Foreseen competitive advantage of the product/technology/solution vis-a-vis existing or planned products/technologies/solutions across the EU and beyond, including consideration given to the balance between performance and cost-efficiency of the solution

  - Potential to accelerate the growth of companies throughout the EU, based on an analysis of the EU internal market and the global market place, indicating, to the extent possible, the size and the growth potential of the market it addresses, as well as expected volumes of sales both within and outside of the EU.

  - Strength of the IP strategy *(e.g. patents)* associated with the solution to support the competitiveness and growth of the applicant companies

- **EDTIB autonomy (5 points)**

  - Extent to which the proposed project will contribute to the autonomy of the EU's Defence Technological and Industrial Base (EDTIB) by increasing the EU's industrial and technological non-dependency from third countries

  - Beneficial impact that the proposed activities will have on the strength of the European security of supply, including the creation of a new supply chain

  - Extent to which the project outcome will contribute to the defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy (CFSP), and in particular in the context of the Capability Development Plan (EDA version releasable to the industry); where appropriate, extent to which the proposal addresses regional or an international priorities which serve the security and defence interests of the EU as determined under the CFSP and do not exclude the possibility of participation of Member States or EDF associated countries

- **Creation of new cross-border cooperation (5 points)**

  - Extent to which the proposed project will create new cross-border cooperation between legal entities established in Member States or EDF associated countries, in particular SMEs and mid-caps, especially compared to former activities in the technological area of the call and taking into account the specificity of the market

  - Planned future cross-border cooperation between legal entities established in Member States or EDF associated countries and cooperation opportunities created by the proposed activities

  - Extent to which SMEs and mid-caps which cooperate cross-border participate substantially, and industrial or technological added value brought by them

- **Implementation (5 points)**

  - Effectiveness and practicality of the structure of the work plan (work breakdown structure), including timing and inter-relation of the

different work packages and their components (illustrated by a Gantt chart, Pert chart or similar)

- Usefulness and comprehensiveness of the milestones and deliverables of the project;. coherence and clarity of the criteria for reaching the milestones, which should be measurable, realistic and achievable within the proposed duration

- Appropriateness of the management structures and procedures, including decision-making mechanisms, to the complexity and scale of the project;. quality of the risk management, including identification and assessment of the project specific critical risks, which could compromise the achievement of the stated project's objectives and detail of proposed risk treatments *(e.g. mitigation measures)*

- Appropriateness of the allocation of tasks and resources between consortium members, ensuring that all participants have a valid and complementary role; allocation of the work share that ensures a high level of effectiveness and efficiency for carrying out the project

Award criteria	Minimum pass score	Maximum score	Weighting
Excellence and potential of disruption	n/a	5	2
Innovation and technological development	n/a	5	2
Competitiveness	n/a	5	1
EDTIB autonomy	n/a	5	1
Creation of new cross-border cooperation	n/a	5	2
Implementation	n/a	5	1
Overall weighted (pass) scores	**30**	**45**	N/A

Maximum points: 45 points.

There is no minimum pass score for individual criteria.

Overall threshold: 30 points.

Proposals that pass the overall threshold will be considered for funding — within the limits of the available budget (i.e. up to the budget ceiling). Other proposals will be rejected.

Only one solution will be funded (i.e. if there are two proposals covering the same solution, only the higher ranked proposal will be selected).

10. Legal and financial set-up of the Grant Agreements

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on Portal Reference Documents.

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement *(Data Sheet, point 1)*. Normally the starting date will be after grant signature. Retroactive application can be granted exceptionally for duly justified reasons — but never earlier than the proposal submission date.

Project duration: *see section 6 above*

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

The following deliverables will be mandatory for all projects:

- progress reports (every 6 to 12 months, to be agreed during grant agreement preparation)
- special report[64].

Form of grant, funding rate and maximum grant amount

The grant parameters *(maximum grant amount, funding rate, total eligible costs, etc)* will be fixed in the Grant Agreement *(Data Sheet, point 3 and art 5)*.

Project budget (maximum grant amount): *see section 6 above*.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted* costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement *(see art 6 and Annex 2 and 2a)*.

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of activities and participants *(see section 2)*.

Grants may in principle NOT produce a profit (i.e. surplus of revenues + EU grant over costs). Where the no-profit rule is activated in the Grant Agreement, for-profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount *(see art 22.3)*.

Moreover, please be aware that the final grant amount may be reduced in case of non-compliance with the Grant Agreement *(e.g. improper implementation, breach of obligations, etc)*.

Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement *(Data Sheet, point 3, art 6 and Annex 2)*.

[64] 'special report' means a specific deliverable of a research action summarising its results, providing extensive information on the basic principles, the aims, the outcomes, the basic properties, the tests performed, the potential benefits, the potential defence applications and the expected exploitation path of the research towards development, including information on the ownership of IPRs but not requiring the inclusion of IPR information *(see art 2(23) EDF Regulation)*.

Budget categories for this call:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties
  - D.2 Internally invoiced goods and services
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:
  - average personnel costs (unit cost according to usual cost accounting practices):Yes
  - SME owner/natural person unit cost[65]: Yes
- subcontracting costs:
  - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
- travel and subsistence unit cost[66]: No (only actual costs)
- equipment costs:
  - depreciation only
- other cost categories:
  - costs for financial support to third parties: not allowed
  - internally invoiced goods and services (unit cost according to usual cost accounting practices): Yes
- indirect cost:
  - flat-rate: 25% of the eligible direct costs (categories A-D, except subcontracting costs, financial support to third parties and exempted specific cost categories, i.e. internally invoiced goods and services and PCP procurement costs)

  or

[65] Commission Decision of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7715).

[66] Commission Decision of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

- actual costs

  ⚠ The indirect cost method selected will be fixed for the project and cannot be changed lateron.

- VAT: non-deductible VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
  - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
  - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
  - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible
  - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible
  - other ineligible costs: Yes, costs related to the use of assets, infrastructure, facilities or resources located or held outside the eligible countries are not eligible (even if their use was authorised, *see section 6*)

Reporting and payment arrangements

The reporting and payment arrangements are fixed in the Grant Agreement *(Data Sheet, point 4 and art 21 and 22)*.

After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **55%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/starting date/financial guarantee (if required) — whichever is the latest.

For projects of more than 18 months, there may be one or more **additional prefinancing payments** linked to a prefinancing report and one or more **interim payments** (with detailed cost reporting).

In addition, you will be requested to submit one or more progress reports not linked to payments.

Payment of the balance: At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All payments will be made to the coordinator.

⚠ Please be aware that payments will be automatically lowered if one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement *(see art 22)*.

Please also note that you are responsible for keeping records on all the work done and the costs declared.

Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement *(Data Sheet, point 4)*. The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are formally NOT linked to individual consortium members, which means that you are free to organise how to provide the guarantee amount *(by one or several beneficiaries, for the overall amount or several guarantees for partial amounts, by the beneficiary concerned or by another beneficiary, etc)*. It is however important that the requested amount is covered and that the guarantee(s) are sent to us in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement.

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement *(Data Sheet, point 4 and art 24)*.

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement *(Data Sheet point 4.4 and art 22).*

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up* to their maximum grant amount
- unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*

or

- individual financial responsibility — *each beneficiary only for their own debts*.

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary).

Provisions concerning the project implementation

Security rules: *see Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- background and list of background: Yes

- protection of results: Yes
- limitations to transfers and licensing: Yes
- rights of use on results: Yes
- for Research Actions: access to results for policy purposes: Yes
- for Research Actions: access to special report: Yes
- for Research Actions: access rights to further develop results: Yes

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5):*

- additional communication and dissemination activities: Yes

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5):*

- specific rules for EDF actions: Yes
- specific rules for PCP Grants for Procurement: No
- place of performance obligation for PCP Grants for Procurement: No
- specific rules for Grants for Financial Support: No
- specific rules for blending operations: No

Other specificities

n/a

Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).

For more information, *see AGA — Annotated Grant Agreement*.

11. How to submit an application

All proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

a) **create a user account and register your organisation**

To use the Submission System (the only way to apply), all participants need to create an EU Login user account.

Once you have an EULogin account, you can register your organisation in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).

b) **submit the proposal**

Access the Electronic Submission System via the Topic page in the Search Funding & Tenders section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 2 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B and Annexes through a password-protected single zip archive:
  - Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and add to the zip archive as a PDF
  - Annexes (*see section 5*). Download templates, and add to zip archive as PDFs (unless other format specified).

The zip archive must be submitted password-protected (using AES-256 encryption method), with a size of less than 100 MB. The password (and any other passwords used in the documents) must be communicated before the deadline for submission to the following email address: DEFIS-EDF-PROPOSALS-PWD@ec.europa.eu (together with the proposal ID and the name of the zip archive).

⚠ If your proposal includes **classified information**, please contact us at DEFIS-EDF-PROPOSALS@ec.europa.eu — well in time before the deadline, in order to arrange the delivery of the classified documents. Please be aware that such documents MUST NOT under any circumstances be submitted online though the Funding & Tenders Portal.

The proposal must keep to the **page limits** *(see section 5)*; excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System otherwise the proposal might be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (*see section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the IT Helpdesk webform, explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the Online Manual. The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- Online Manual
- FAQs on the Topic page (for call-specific questions in open calls; not applicable

for actions by invitation)

- Portal FAQ (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

Contact

For individual questions on the Portal Submission System, please contact the IT Helpdesk.

Non-IT related questions should be sent to the following email address: DEFIS-EDF-PROPOSALS@ec.europa.eu.

Please indicate clearly the reference of the call and topic to which your question relates *(see cover page)*.

13. Important

IMPORTANT

- **Don't wait until the end —** Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions *(e.g. congestion, etc)* will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System —** By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the Portal Terms & Conditions.
- **Registration —** Before submitting the application, all beneficiaries, affiliated entities, associated partners must be registered in the Participant Register. The draft participant identification code (PIC) (one per participant) is mandatory for the Application Form.

  If your project applies for the SME/Mid-cap bonuses, registration (draft PIC and SME self-assessment wizard) is also mandatory for all participants claiming SME/Mid-cap status (beneficiaries, affiliated entities and subcontractors involved in the action; *see section 2*).

  Moreover, registration (draft PIC) is required for entities that must submit an ownership control assessment declaration (beneficiaries, affiliated entities, subcontractors involved in the action and associated partners).
- **Consortium roles —** When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.

  The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs per beneficiary/affiliated entity must be justified in the application and may be accepted by the granting authority if the topic is not subject to a fixed subcontracting limit *(see section 10)*.
- **Coordinator —** In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities —** Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any).
- **Associated partners —** Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.

- **Consortium agreement —** For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget —** Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully *(e.g. own contributions, income generated by the action, financial contributions from third parties, etc)*. You may be requested to lower your estimated costs, if they are ineligible (including excessive).

- **No-profit rule —** Grants may in principle NOT give a profit (i.e. surplus of revenues + EU grant over costs). Where the no-profit rule is activated in the Grant Agreement, this will be checked by us at the end of the project.

- **No double funding —** There is a strict prohibition of double funding from the EU budget (except under EU Synergies actions). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances declared to two different EU actions.

- **Completed/ongoing projects —** Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).

- **Combination with EU operating grants —** Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice *(see AGA — Annotated Model Grant Agreement, art 6.2.E)*.

- **Multiple proposals —** Applicants may submit more than one proposal for *different* projects under the same call (and be awarded a funding for them).

  Organisations may participate in several proposals.

  BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw one of them (or it will be rejected).

- **Resubmission —** Proposals may be changed and re-submitted until the deadline for submission.

- **Rejection —** By submitting the application, all applicants accept the call conditions set out in this this Call Document (and the documents it refers to). Proposals that do not comply with all the call conditions will be **rejected**. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, it must be replaced or the entire proposal will be rejected.

- **Cancellation —** There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.

- **Language —** You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, see section 12).

- **Transparency —** In accordance with Article 38 of the EU Financial Regulation, information about EU grants awarded is published each year on the Europa website.

  This includes:
  - beneficiary names
  - beneficiary addresses
  - the purpose for which the grant was awarded
  - the maximum amount awarded.

  The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection —** The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the Funding & Tenders Portal Privacy Statement.

Annex 1

EDF types of action

EDF uses the following actions to implement grants:

Research Actions

Description: Research Actions (RA) target activities consisting primarily of research activities, in particular applied research and where necessary fundamental research, with the aim of acquiring new knowledge and with an exclusive focus on defence applications.

Funding rate: 100%

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Development Actions

Description: Development Actions (DA) target activities consisting of defence-oriented activities primarily in the development phase, covering new defence products or technologies or the upgrading of existing ones, excluding the production or use of weapon.

Funding rate: variable per activity (rates depend on activity and bonuses for SME and mid-cap participation and PESCO)

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

PCP Grants for Procurement

Description: PCP Grants for Procurement (PCP) target activities that aim to help a transnational buyers' group to strengthen the public procurement of research, development, validation and, possibly, the first deployment of new solutions that can significantly improve quality and efficiency in areas of public interest, while opening market opportunities for industry and researchers active in Europe. Eligible activities include the preparation, management and follow-up, under the coordination of a lead procurer, of one joint PCP and additional activities to embed the PCP into a wider set of demand-side activities.

Funding rate: variable (to be defined in the work programme)

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — payment of the balance

Lump Sum Grants for Research Actions

Description: Lump Sum Grants (LS-RA) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature) on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented, only part of the lump sum will be paid.

Lump Sum Grants for Research Actions cover the same type of activities as Research Actions and follow — where relevant — similar rules *(e.g. for funding rates, etc.)*.

Funding rate: 100%

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Lump Sum Grants for Development Actions

Description: Lump Sum Grants (LS-DA) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature) on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented, only part of the lump sum will be paid.

Lump Sum Grants for Development Actions cover the same type of activities as Development Actions and follow — where relevant — similar rules *(e.g. for funding rates, etc)*.

Funding rate: variable per activity (rates depend on activity and bonuses for SME and mid-cap participation and PESCO)

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: FPAs establish a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

Funding rate: no funding for FPA

SGAs

Description: The SGAs are linked to an FPA and implement the action plan (or part of it). They are awarded via an invitation to submit a proposal (identified beneficiary action). The consortium composition should in principle match (meaning that only entities that are part of the FPA can participate in an SGA), but otherwise the implementation is rather flexible. FPAs and SGAs can have different coordinators; other partners of the FPA are free to participate in an SGA or not. There is no limit to the amount of SGAs signed under one FPA.

Funding rate: depending on the type: 100% or variable per activity

Payment model: Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

Annex 2

Guarantees pursuant to Article 9(4) of the EDF Regulation

All calls under the EDF Programme are subject to ownership control restrictions, meaning that they exclude the participation of legal entities which are established in the EU territory or in an EDF associated country, but are controlled by a non-associated third country or non-associated third country legal entity.

Thus, for the purposes of participating in EDF actions, beneficiaries, affiliated entities, associated partners and subcontractors involved in the action must not be subject to control by a non-associated third country or non-associated third-country entity and undergo an ownership control assessment procedure before grant signature.

Entities that do not comply with this requirement may however exceptionally nevertheless participate, if they can provide guarantees approved by the Member State/EDF associated country in which they are established. Such guarantees must be provided at the latest by grant signature.

The guarantees must provide assurance to the granting authority that the participation of the entity will not contravene the security and defence interests of the EU and its Member States as established in the framework of the Common Foreign and Security Policy (CFSP) pursuant to Title V of the TEU, or the objectives set out in Article 3 of the EDF Regulation. They must also comply with the provisions on ownership and intellectual property rights (Articles 20 and 23 of the EDF Regulation).

They must in particular substantiate that, for the purposes of the action, measures are in place to ensure that:

- **control** over the legal entity is not exercised in a manner that would restrain or restrict its ability to carry out the action and to deliver results, that would impose restrictions concerning its infrastructure, facilities, assets, resources, intellectual property or knowhow needed for the purposes of the action, or that would undermine its capabilities and standards necessary to carry out the action

- **access** by a non-associated third country or non-associated 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 clearance issued by a Member State or an EDF associated country, where appropriate

- **ownership** of the intellectual property arising from, and the results of, the action remain within the beneficiary or affiliated entity during and after completion of the action, are not subject to control or restriction by a non-associated third country or non-associated third-country entity, and are neither exported outside the EU/EDF associated countries nor accessible from outside the EU/EDF associated countries without the approval of the Member State/EDF associated country in which the legal entity is established and in accordance with the objectives set out in Article 3 of the EDF Regulation.

The guarantees may refer to the fact that the legal entity's executive management structure is established in the EU/EDF associated country or, if considered appropriate, to specific governmental rights in the control over the legal entity.

If considered appropriate by the Member State/EDF associated country, additional guarantees may be provided.

For more information, *see also* *Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls*.

Annex 3

Security aspects

Introduction

Pursuant to Article 27(4) of the EDF Regulation, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries and affiliated entities are established must decide on the originatorship of the classified foreground information (results) generated in the performance of the project. For that purpose, those Member States may decide on a specific security framework for the protection and handling of classified information relating to the project and must inform the granting authority. Such a security framework must be without prejudice to the possibility for the granting authority 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 Decision 2015/444.

In either case, the security framework will be put in place at the latest by the signature of the Grant Agreement.

The applicable security framework will be detailed in the security aspect letter (SAL) which will be annexed to the Grant Agreement.

When you implement a classified grant, please bear in mind the following key rules.

Access to classified information

The creation, handling or access to information classified CONFIDENTIAL or SECRET (or RESTRICTED where required by national rules) on the premises of a participant is only possible if 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 participant concerned.

The participant must hold a duly confirmed FSC at the appropriate level. Until a secured area is in place and accredited by the national NSA, the handling of classified information above RESTRICTED level on their premises is not allowed.

Access to and handling of classified information for the purposes of the project must be limited to individuals with a need-to-know and which are in possession of a valid personnel security clearance.

At the end of the Grant Agreement when EUCI is no longer required for the performance of the grant, the participant must return any EUCI they hold to the contracting authority immediately. If authorised to retain EUCI after the end of the grant, the EUCI must continue to be protected in accordance with Decision 2015/444.

Marking of classified information

Classified information generated for the performance of the action must be marked in accordance with the applicable security framework, as described in the SAL.

Grants must not involve information classified 'TRES SECRET UE/EU TOP SECRET' or any equivalent classification.

Other provisions

Where a participant has awarded a classified subcontract, the security provisions of the grant agreement must apply *mutatis mutandis* to the subcontractor(s) and their personnel. In such case, it is the responsibility of the participant to ensure that all subcontractors apply these principles to their own subcontracting arrangements.

All security breaches related to classified information will be investigated by the competent security authority and may lead to criminal prosecution under national law.

Table of equivalent security classification markings

	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)	*(Note 1, 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 SECRET DÉFENSE *(Note 2, see below)*	CONFIDENTIEL DÉFENSE *(Notes 2 and 3, see below)*	*(Note 4, see below)*
Germany ***(Note 5, 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
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 *(Note 6, see below)*
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO *(Note 6, see below)*	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG

Notes:

Note 1 Belgium: 'Diffusion Restreinte/Beperkte Verspreiding' is not a security classification in Belgium. Belgium handles and protects RESTREINT UE/EU RESTRICTED information and classified information bearing the national classification markings of RESTRICTED level in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

Note 2 France: Information generated by France before 1 July 2021 and classified SECRET DÉFENSE and CONFIDENTIEL DÉFENSE continues to be handled and protected at the equivalent level of SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL respectively.

Note 3 France: France handles and protects CONFIDENTIEL UE/EU CONFIDENTIAL information in accordance with the French security measures for protecting SECRET information.

Note 4 France: France does not use the classification 'RESTREINT' in its national system. France handles and protects RESTREINT UE/EU RESTRICTED information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union. France will handle classified information bearing the national classification markings of RESTRICTED level in accordance with its national rules and regulations in force for 'DIFFUSION RESTREINTE'. The other Participants will handle and protect information marked 'DIFFUSION RESTREINTE' according to their national laws and regulations in force for the level RESTRICTED or equivalent, and according to the standards defined in the present document.

Note 5 Germany: VS = Verschlusssache.

Note 6 Portugal and Spain: Attention is drawn to the fact that the markings RESERVADO used by Portugal and Spain refer to different classifications.