



# European Defence Fund (EDF)

## Call for proposals

EDF-2022-LS-RA-CHALLENGE

Version 1.2  
08 August 2022



<b>HISTORY OF CHANGES</b>			
<b>Version</b>	<b>Publication Date</b>	<b>Change</b>	<b>Page</b>
1.0	09.06.2022	– Initial version.	
1.1	04.07.2022	– Removal of fixed subcontracting limit	26
1.2	08.08.2022	– Removal of limit to participation of research organisations	26
		–	



**EUROPEAN COMMISSION**  
 Directorate-General for Defence Industry and Space  
 DEFIS.A – Defence Industry

## CALL FOR PROPOSALS

### TABLE OF CONTENTS

0. Introduction .....	5
1. Background.....	6
2. Type of action and funding rate — Objectives — Scope and types of activities — Functional requirements — Expected impact — Specific topic conditions .....	7
Type of action and funding rate .....	7
Specific topic conditions.....	7
EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP: Unmanned ground and aerial systems for hidden threats detection – Participation to a technological challenge .....	7
Objectives.....	7
Scope and types of activities .....	8
Functional requirements .....	9
Expected impact.....	10
EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO: Unmanned ground and aerial systems for hidden threats detection – Organisation of a technological challenge .....	10
Objectives.....	10
Scope and types of activities .....	10
Functional requirements .....	12
Expected impact .....	12
3. Available budget.....	13
4. Timetable and deadlines .....	13
5. Admissibility and documents .....	13
6. Eligibility .....	15
Eligible participants (eligible countries).....	15
Consortium composition .....	16
Eligible actions and activities.....	16
Geographic location (target countries).....	17
Duration .....	17
Project budget.....	17
Ethics .....	17
Security.....	18
7. Financial and operational capacity and exclusion.....	19

Financial capacity .....	19
Operational capacity.....	20
Exclusion .....	20
8. Evaluation and award procedure .....	21
9. Award criteria.....	22
10. Legal and financial set-up of the Grant Agreements.....	24
Starting date and project duration .....	24
Milestones and deliverables.....	25
Form of grant, funding rate and maximum grant amount.....	25
Budget categories and cost eligibility rules .....	25
Reporting and payment arrangements.....	27
Prefinancing guarantees .....	27
Certificates .....	28
Liability regime for recoveries.....	28
Provisions concerning the project implementation .....	28
Other specificities .....	29
Non-compliance and breach of contract .....	29
11. How to submit an application.....	29
12. Help .....	30
13. Important .....	31
Annex 1 .....	34
Annex 2 .....	36
Annex 3 .....	38
Annex 4 .....	42

## 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](#)<sup>1</sup>).

The call is launched in accordance with the Work Programmes 2022 Part II<sup>2</sup> and will be managed by the **European Commission, Directorate-General for Defence Industry and Space (DG DEFIS)**.

The call covers the following **2 topics**:

- **EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP: Unmanned ground and aerial systems for hidden threats detection – Participation to a technological challenge**
- **EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO: Unmanned ground and aerial systems for hidden threats detection – Organisation of a technological challenge**

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.

The 2 topics are linked. Grants under the topic EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP will be managed as linked actions with the grant under the topic EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO.

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)

---

<sup>1</sup> 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).

<sup>2</sup> 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.

- 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 EDF Work Programmes 2022 Part II, this call covers thematic topics addressing research actions for a technological challenge to be implemented through lump sum 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 concerns EDF Lump Sum Grants for Research Actions (LS-RA).

Lump Sum Grants for Research Actions are managed as contributions on the basis of an estimated project budget where each activity will be reimbursed at the funding rate that applies to Research Actions (100%).

### Specific topic conditions

- For all topics under this call, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (*see section 6*)
- For all topics under this call, following reimbursement option for equipment costs applies: depreciation only (*see section 10*)

## **EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP: Unmanned ground and aerial systems for hidden threats detection – Participation to a technological challenge**

### Objectives

Improvised explosive devices (IEDs) and landmines are a significant threat to military personnel, civilians and equipment, and a major cause of casualties for European forces during operations. Countering these hidden threats is essential to protect soldiers, reduce loss of equipment, secure critical logistic activities, improve mobility and freedom to act by increasing the security of operation areas, and more generally enhance operational efficiency. Furthermore, in a hybrid warfare context, these threats are increasingly used against civilian populations. In particular, they have the potential to severely disrupt both military and civilian supply chains, damage critical infrastructures and affect strategic lines of communication.

Detecting these hidden threats is a first essential step to counter them. Since they are by design difficult to detect for humans, automatic detection technologies can play an important role. However, the task is intrinsically difficult, and the performance of existing technologies is still far from answering the needs. Scenarios classically encountered by armed forces in past missions such as route clearance already represent a challenge. In addition, IEDs are increasingly used in urban scenarios where the detection is even more difficult, especially if multiple IEDs emplacements are used. There is a need to enhance detection technologies, especially for scenarios where single detection devices are not sufficient and the use of distributed sensors is deemed useful. There is also a need to determine their type (e.g., how they are triggered), in particular to ease their neutralisation (rendering safe, disabling or destroying).

While the above issues have been the subject of much research over many years, progress is hindered by the lack of standardised benchmarks, and there is a need to evaluate the performances of integrated functional demonstrators in an objective and comparable manner, using representative testing environments and well-defined metrics.

Overall progress in IED and landmine detection and characterisation can be driven by progress along several lines:

- Physics-based sensors enhancement;
- Collection of representative data, combined with various artificial intelligence (AI) techniques, e.g., computer vision for object detection and localisation;
- Use of various sensors borne by a fleet of unmanned ground and aerial systems, combined with information fusion techniques;
- Better exploitation of limited amounts of data and use of models that are easier to adapt to new environments (through innovative AI techniques such as learning methods requiring less supervision from expert developers, transfer learning...);
- Multidisciplinary cooperation between the hardware sensors and AI communities.

### Scope and types of activities

#### *Scope*

Proposals should address technological solutions to detect and characterise IEDs and landmines in complex environments, using a combination of advanced sensors, information fusion from these sensors, and unmanned ground and aerial systems to extend the detection capabilities. These solutions should be evaluable through the testing environment set up in the framework of the technological challenge.

Proposals should include clear descriptions of criteria to assess work package completion. Criteria should include the participation to the test campaigns organised in the framework of the technological challenge, the delivery of sensor data collected during the field tests, and the delivery of descriptions of the systems submitted to the tests.

#### *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*):

<b>Types of activities</b> (art 10(3) EDF Regulation)		<b>Eligible?</b>
(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 ( <b>generating knowledge</b> )	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 ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	<b>Design</b> 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)	<b>System prototyping</b> <sup>3</sup> of a defence product, tangible or intangible component or technology	No
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	No
(g)	<b>Qualification</b> <sup>4</sup> of a defence product, tangible or intangible component or technology	No
(h)	<b>Certification</b> <sup>5</sup> of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	No

The proposals must address in particular the following as part of the mandatory activities:

- Research on new approaches and technologies for hidden threat detection and characterisation
- Participation to the evaluation campaigns organised in the framework of the technological challenge, including
  - Contribution to the exchanges with other stakeholders on the evaluation plans
  - Submission of the systems to experimental performance measurements during the field and online test campaigns managed by the challenge organisers
  - Collection and sharing of data
  - Participation to debriefing workshops

### Functional requirements

The proposed solutions should fulfil the following requirements:

- Ability to go through a zone with IEDs or landmines while minimizing the risk of damage
- Ability to detect and map IEDs and landmines in a given area, with maximum accuracy
- Ability to characterise IEDs and landmines, with maximum accuracy

The performances for these abilities should be measurable through the test campaign conducted in the framework of the technological challenge, using protocols and metrics based on those described in the preliminary evaluation plan provided as part of the call documents (see Annex 4). Details about how the proposed approaches and

<sup>3</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>4</sup> '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.

<sup>5</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

systems will address the tasks outlined in the preliminary evaluation plan should be described in the proposals.

Systems should be able to record the data acquired through their sensors, in order to enable reproduction of experiments in a software environment. The types of data that could be shared with other teams should be described in the proposals.

While much flexibility is left concerning the system configuration for the challenge, systems should be designed to experiment operationally relevant solutions.

#### Expected impact

- Enhanced clarity on performances of equipment for IED and landmine detection and characterisation
- Availability of databases to further develop and test equipment
- Enhanced soldier protection and increased survivability, through reduced risk for lethal or damaging incidents
- Enhanced freedom of action
- Reduced risks of disruption of strategic infrastructures

### **EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO: Unmanned ground and aerial systems for hidden threats detection – Organisation of a technological challenge**

#### Objectives

IED and landmine detection has been a research topic for many years. However, progress is hindered by the lack of standardised benchmarks. There is a need to rely on representative testing environments enabling an objective and comparable evaluation of developed systems.

Furthermore, field tests cannot be repeated at will and are not perfectly reproducible, especially for detection systems that involve artificial intelligence. Online tests of software components, for which measurements are easily reproducible and which enable short development cycles, should therefore also be organised. Since little data is readily available, data for online tests need to be collected during field tests organised previously during the challenge. This combination of field tests and online tests is needed to steer fast progress toward operational goals.

#### Scope and types of activities

##### *Scope*

Proposals should address the organisation of a technological challenge on IED and landmine detection based on the preliminary evaluation plan provided as part of the call documents (see Annex 4). This includes the collection of data recorded by the participating teams during field tests, the annotation of this data and the sharing of the resulting databases.

Proposals should include clear descriptions of criteria to assess work package completion. Criteria should include the production of detailed evaluation plans agreed upon by all stakeholders, the production of the annotated databases needed for the evaluations, the production of measurements for all systems submitted to the tests by the participating teams following these plans, and the organisation of the needed events.

*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):

<b>Types of activities</b> (art 10(3) EDF Regulation)		<b>Eligible?</b>
(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 ( <b>generating knowledge</b> )	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 ( <b>integrating knowledge</b> )	Yes (mandatory)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	<b>Design</b> 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)	<b>System prototyping</b> <sup>6</sup> of a defence product, tangible or intangible component or technology	No
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	No
(g)	<b>Qualification</b> <sup>7</sup> of a defence product, tangible or intangible component or technology	No
(h)	<b>Certification</b> <sup>8</sup> of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	No

The proposals must address in particular the following as part of the mandatory activities:

- Setting up of the hardware and software infrastructures for testing hidden threat detection and characterisation technologies in the framework of the technological challenge
- Collection of sensor data from the participating teams, annotation of the data with ground truth information, and quality assessment, distribution and curation of databases
- Organisation of the evaluation campaigns, and in particular

<sup>6</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>7</sup> '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.

<sup>8</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Coordination of the exchanges with other stakeholders on the evaluation plans and elaboration of these plans
- Management of the experimental hardware and software test campaigns and of the objective measurements of the performances of the systems submitted to the tests by the participating teams according to the protocols and metrics described in the evaluation plans
- Organisation of the debriefing workshops

### Functional requirements

The proposed solutions should enable to measure the performances of the tested systems according to detailed evaluation plans based on the preliminary evaluation plan provided as part of the call documents. Key aspects of the foreseen detailed evaluation plans and associated data management should be described in the proposals. Proposals should in particular describe:

- scenarios, nature and size of test ranges, and environmental conditions,
- types of devices, concealment, attack geography,
- nature and volume of data annotation,
- the framework for trusted sharing of data,
- the detailed planning of the test campaigns, including how runs can be organised in parallel on several test ranges,
- evaluation procedures (rules and tools to implement the metrics) and significance tests performed on measurements.

The testing environment should be able to accommodate for up to six participating teams.

During the challenge, drafts of the detailed evaluation plans should be submitted for discussion to the participating teams and to any stakeholder designated by the funding authority, early enough to take into account the feedback for the actual evaluation campaigns. Any evolution of the evaluation plans should take into account several factors: technical possibilities and cost, scientific relevance of the measurement, and representativeness of the metrics and protocols with respect to military needs. The justification of any change that is not subject to a consensus should be documented.

### Expected impact

- Enhanced metrics and protocols to measure progress of R&D on IED and landmine detection and characterisation
- Standardisation of combined online and field testing for IED and landmine detection and characterisation
- Availability of databases to further develop and test equipment
- Enhanced clarity of system performances for all stakeholders, including system developers, funders and users
- Enhanced community building for the topic.

### 3. Available budget

The available call budget is **EUR 25 000 000**.

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-LS-RA-CHALLENGE-DIGIT-HTDP: Unmanned ground and aerial systems for hidden threats detection – Participation to a technological challenge	EUR 20 000 000	No	No
EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO: Unmanned ground and aerial systems for hidden threats detection – Organisation of a technological challenge	EUR 5 000 000	No	1

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:	<u>24 November 2022 – 17:00:00 CET (Brussels)</u>
Evaluation:	November 2022 - June 2023
Information on evaluation results:	June/July 2023
GA signature <sup>9</sup> :	July-December 2023

### 5. Admissibility and documents

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

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).

<sup>9</sup> 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 **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
  - 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 be aware that since the detailed budget table serves as the basis for fixing the lump sums for the grants (and since lump sums must be reliable proxies for the actual costs of a project), the costs you include **MUST** comply with the basic eligibility conditions for EU actual cost grants (see [AGA – Annotated Grant Agreement, art 6](#)). This is particularly important for purchases and subcontracting, which must comply with best value for money (or if appropriate the lowest price) and be free of any conflict of interests. If the budget table contains ineligible costs, the grant may be reduced (even later on during the project implementation or after their end).

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*).

 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<sup>10</sup> 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.

---

<sup>10</sup> '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<sup>11</sup>.

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'<sup>12</sup>. ⚠ 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)*<sup>13</sup> and entities covered by Commission Guidelines No [2013/C 205/05](#)<sup>14</sup>). 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).

 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

<sup>11</sup> See Article 197(2)(c) EU Financial Regulation [2018/1046](#).

<sup>12</sup> For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation [2018/1046](#).

<sup>13</sup> 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](#).

<sup>14</sup> 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: **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: **should not exceed EUR 5 000 000.**

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](#)<sup>15</sup> and its implementing rules<sup>16</sup>.

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 information agreement with the EU (or an administrative arrangement with the Commission)
- disclosure of classified information to third parties is subject to prior written

---

<sup>15</sup> 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).

<sup>16</sup> See Article 27(4) EDF Regulation.

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<sup>17</sup>:

- 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<sup>18</sup> (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)
- 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-

<sup>17</sup> See Articles 136 and 141 of EU Financial Regulation [2018/1046](#).

<sup>18</sup> 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.

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<sup>19</sup>:

- 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

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.

---

<sup>19</sup> See Article 141 EU Financial Regulation [2018/1046](#).

**⚠️ 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 targeted 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 European 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
<b>Overall weighted (pass) scores</b>	<b>30</b>	<b>45</b>	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, 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<sup>20</sup>.

### 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 lump sum grant. This means that it will reimburse a fixed amount, based on a lump sum or financing not linked to costs. The amount will be fixed by the granting authority on the basis of the estimated project budget and funding rates that depend on the type of activities and participants (*see section 2*).

### 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*).

*Budget categories for this call:*

- Lump sum contributions<sup>21</sup>

*Specific cost eligibility rules for this call:*

- the lump sum amount must be calculated in accordance with the methodology set out in the lump sum decision and using the detailed budget table/calculator provided (if any)
- the lump sum calculation should respect the following conditions:
  - for lump sums based on estimated project budgets: the estimated budget must comply with the basic eligibility conditions for EU actual cost grants (*see [AGA – Annotated Grant Agreement, art 6](#)*), in particular:
    - personnel costs:
      - average personnel costs (unit cost according to usual cost accounting practices): Yes
      - SME owner/natural person unit cost<sup>22</sup>: Yes

<sup>20</sup> '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*).

<sup>21</sup> [Decision](#) of 30.11.2021 authorising the use of lump sums for specific actions under the European Defence Fund.

- subcontracting costs:
  - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
- travel and subsistence unit cost<sup>23</sup>: 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 (costs 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

  - actual costs
    - ⚠ The indirect cost method selected will be fixed for the project and cannot be changed later on.
- 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
  - 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*)
- the lump sum breakdown must comply with the following:

---

<sup>22</sup> 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).

<sup>23</sup> 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).

- the types of activity (*see section 2*) may be broken down into several work packages
- a work package must cover one type of activity only
- the funding rate to be used for WP 1 — Project management and coordination must be the one for the type of activity (c) Studies.
- other:
  - eligible cost country restrictions: Yes, only costs/contributions for activities carried out in eligible countries are eligible

### 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**.

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.

### 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 EU Login 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](mailto: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](mailto: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 through 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](mailto: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 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

	<b>Secret</b>	<b>Confidential</b>	<b>Restricted</b>
<b>EU</b>	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
<b>Austria</b>	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
<b>Belgium</b>	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)
<b>Bulgaria</b>	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
<b>Croatia</b>	ТАЈНО	POVJERLJIVO	OGRANIČENO
<b>Cyprus</b>	ΑΠΟΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΟ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ ABR:(ΠΧ)
<b>Czech Republic</b>	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
<b>Denmark</b>	HEMMELOGT	FORTROLIGT	TIL TJENESTEBRUG
<b>Estonia</b>	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
<b>Finland</b>	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG

<b>France</b>	SECRET SECRET DÉFENSE <i>(Note 2, see below)</i>	CONFIDENTIEL DÉFENSE <i>(Notes 2 and 3, see below)</i>	<i>(Note 4, see below)</i>
<b>Germany</b> <i>(Note 5, see below)</i>	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
<b>Greece</b>	ΑΠΟΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΟ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ ABR:(ΠΧ)
<b>Hungary</b>	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
<b>Ireland</b>	SECRET	CONFIDENTIAL	RESTRICTED
<b>Italy</b>	SEGRETO	RISERVATISSIMO	RISERVATO
<b>Latvia</b>	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
<b>Lithuania</b>	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
<b>Luxembourg</b>	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
<b>Malta</b>	SIGRIET	KUNFIDENZJALI	RISTRETT
<b>Netherlands</b>	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
<b>Poland</b>	TAJNE	POUFNE	ZASTRZEŻONE
<b>Portugal</b>	SEGRETO	CONFIDENCIAL	RESERVADO <i>(Note 6, see below)</i>
<b>Romania</b>	STRICT SECRET	SECRET	SECRET DE SERVICIU
<b>Slovakia</b>	TAJNÉ	DÔVERNÉ	VYHRADENÉ
<b>Slovenia</b>	TAJNO	ZAUPNO	INTERNO
<b>Spain</b>	RESERVADO <i>(Note 6, see below)</i>	CONFIDENCIAL	DIFUSIÓN LIMITADA
<b>Sweden</b>	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.

**Annex 4****Preliminary evaluation plan  
for the EDF Challenge on Hidden Threats Detection**

(Topics EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDP and EDF-2022-LS-RA-CHALLENGE-DIGIT-HTDO)

**Introduction**

This annex is the preliminary evaluation plan for the EDF Challenge on Hidden Threats Detection. It provides a general description of the testing environment, metrics and protocols under which the research teams participating to the challenge will evaluate their systems. It is provided as part of the call documents for the topics of the EDF call EDF-2022-LS-RA-CHALLENGE in order to enable applicants to prepare projects that can cooperate smoothly with one another. For each actual test campaign, a more detailed evaluation plan will be produced by the challenge organisers.

**Overall concept and timeline**

The challenge aims at measuring, in an objective and comparable way, the performances of different approaches to hidden threat detection and characterisation. The hidden threats considered are Improvised Explosive Devices (IEDs) and landmines. Since this is the first challenge in this domain, defining the metric and protocols is also an objective in itself. Another specific objective of the challenge is to measure the potential added value of using sensors embedded in unmanned ground and aerial systems in addition to sensors embedded in a manned ground vehicle.

In the framework of the challenge, field tests are organised during which systems developed by the participating teams go through a zone with simulated IEDs and landmines. The simulated devices are as much as possible representative of real ones (real-scale fully functional devices) while being harmless under basic security conditions (e.g. containing only small explosive charges or smoke bombs). The focus is on static devices (subsurface, surface and side attack). However, moving (e.g. UAV-borne) devices can be considered for the last years of the challenge. Both command-operated and victim-operated devices are considered.

During field tests, the goal of the teams piloting the systems is to lead them from a designated starting area to a predefined target location in a "safe" manner, i.e. by avoiding being "hit" by IEDs or landmines. During such a test, the systems process the sensor data in real-time to automatically detect IEDs and landmines and characterise them. The information is presented to the pilots in order to help them achieving the goal of safely reaching the target location.

Sensor data acquired and used by the systems during the field tests shall be recorded in order to develop further the automatic detection and characterisation functions in a well-controlled way and with short development cycles in between field tests.

Data sharing across teams is encouraged in order to experiment various approaches on various data. A framework for trusted and secure information exchange is set up for that purpose.

Furthermore, in order to measure performances of AI-based software modules in an objective and comparable way, online tests are organised whereby test data is released simultaneously to all participating teams who send back the system outputs to the organisers by a given deadline a few days later.

Online tests take place in between two field test campaigns, in order to use data collected during a given campaign to enhance software modules and use them for the next one. Both online and field tests are followed by a debriefing workshop, where the organisers present the consolidated performance measurements and all teams

present an analysis of their results. The draft evaluation plan for each campaign is presented and discussed well in advance of the tests.

The challenge lasts four years and covers four evaluation campaigns, each lasting about a year. The first one involves only field tests. It is a dry-run phase, where some adaptation of the evaluation protocols might be needed before delivering meaningful measurements. The next three evaluation campaigns are fully-fledged ones involving both field and online tests.

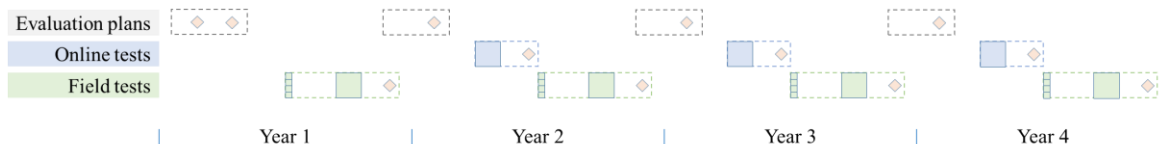
For each of the three fully-fledged campaigns, a proposed general timeline is as follows:

- January: Evaluation plan discussion workshop
- April: Online tests
- June: Debriefing workshop; Individual on-site trials
- September: Field tests
- November: Debriefing workshop

For the first campaign, a proposed general timeline is as follows:

- Spring: Evaluation plan discussion workshops
- June: Individual on-site trials
- September: Field tests
- November: Debriefing workshop

This proposed general timeline is illustrated below.



Each field test campaign lasts a week. The first day is devoted to the installation of the teams and trials using a small-scale testing area available to the participating teams with minimal constraints. The next three days are devoted to actual tests. Several testing zones are available, enabling several teams to perform runs in parallel. The last day is devoted to a debriefing meeting before departure of the teams.

The precise timeline of online tests is determined in the specific evaluations plan of each campaign.

A few weeks before each field test campaign, on-site trials are organised individually for each team, for a duration of up to two days per team.

Discussion and debriefing workshops gather all stakeholders and are expected to last about two days, travel included. Additional meetings are likely to be needed, but can be organised online.

Over the challenge duration, field test campaigns are hosted in at least two different sites. Various types of environments including open air and urban ones are represented.

## Systems

Systems submitted to field tests should include one main ground vehicle and at least one accompanying ground robot or aerial drone. The accompanying robots and drones are remotely piloted, possibly relying on semi-autonomous navigation capabilities. Pilots can be in the main ground vehicle or outside the test zone.

Both the main ground vehicle and the accompanying robots and drones are equipped with sensors. All vehicles should be connected and the results of the information fusion should be available in the main ground vehicle.

Systems should be able to record the data acquired through their sensors. If some sensor data used for the automatic detection during field tests cannot be recorded for practical reasons, this should be justified.

## Tasks and metrics

### Overview

The table below provides an overview of the tasks that are evaluated in the framework of the challenge.

General objective	Task	Metric	Measurable during	
			Field tests	Online tests
Detect and avoid	Avoidance	Number of hits per km of track	X	
	Detection and mapping	Number of detection errors per km <sup>2</sup>	X	X
	Detection without mapping	Average number of detection errors per image		X
Characterise	Type identification	Classification error rate	X	X
	Feature estimation	Average percentage of error	X	X

These tasks are detailed in the following subsections.

### *IED and landmine avoidance (field tests only)*

The objective of the task is to go from a designated starting area to a predefined target location through a zone with simulated IEDs and landmines while minimising the number of hits (simulated device explosions).

The metric is the number of hits on the main vehicle per km of track. Hits on accompanying robots or drones are counted as a separate, secondary metric (these hits can however indirectly influence the main metric as the concerned parts should stop contributing to the mission). The track used for determining the distance travelled is the one provided by the organisers. Possible detours do not lead to use a longer track length for computing the metric.

A map of a recommended path leading from the starting area to the target location is provided in advance by the organisers, and runs of reconnaissance of the track leading to the target location are organised before the actual tests. During the tests, it is possible to deviate from the track, especially if deemed needed to avoid hits. However, the system should remain in a predefined zone, the perimeter of which is also provided in advance.

Runs with and without the help of the automatic hidden threat detection are organised in order to measure the added value of the real-time detection for the pilot of the main ground vehicle.

Several runs are conducted in the same range to give systems the possibility to rely on automatic change detection if deemed useful.

#### *IED and landmine detection and mapping*

The overall objective of the task is to detect IEDs and landmines over an area that the main ground vehicle has screened when going from the starting area to the target location. The detected devices should be positioned in the frame of reference (map) provided by the organisers.

The metric is the number of errors (false alarms and missed detections) per km<sup>2</sup> of area for which detection outputs are provided. This area should include the path followed by the vehicle.

A partial metric is first computed at any given time on a predefined area in front of the main ground vehicle corresponding to the area where the presence of a device is a threat. The extension of the area can for example be related to a maximum braking distance. The exact dimensions of the area should be defined in the detailed evaluation plans. Systems should provide at regular time intervals (e.g. every second) their positioning information (coordinates and orientation) and the estimated locations of detected devices in the frame of reference of the main vehicle. In order to compute the metric, this local map is first aligned with the map of the zone, using the vehicle positioning information. Estimated locations that do not match the ground truth within a certain tolerance threshold (to be defined in the detailed evaluation plans) are false alarms. Ground truth elements that are not matched within the tolerance threshold are missed detections.

In addition to instantaneous information provided at regular intervals for the area in front of the vehicle, systems provide at the end of the run an integrated map of the estimated positions of the detected devices within an area along a path that the vehicle has followed. The overall metric for the task is the number of errors over this area, divided by the surface of this area (in km<sup>2</sup>).

#### *IED and landmine detection without mapping (online tests only, optional task)*

The objective of the task is to detect IEDs and landmines in a predefined area in front of a vehicle, while positioning them in images captured from the vehicle.

Compared to the detection and mapping task described above, this task requires more annotation work to prepare the data but avoids the issue of the potential alignment uncertainty between the two frames of reference.

The metric is similar, except that the frame of reference for the estimated and ground truth locations is a set of images taken from the main ground vehicle. It is computed as the number of errors (false alarms and missed detections) averaged over the considered images.

If needed to further improve measurement accuracy, the locations of IEDs and landmines can be represented by their actual areas in the images rather than points.

#### *IED and landmine type identification*

The objective of the task is to identify the types of the detected IEDs and landmines. As a baseline, the classification of devices into command-operated and victim-operated is evaluated for IEDs, and into anti-personnel and anti-tank for landmines. Possibilities to evaluate classification among more fine-grained categories should be explored during the challenge.

The metric is the classification error rate.

For field tests, the metric is computed on the automatically detected IEDs and landmines. For online tests, the same metric is computed for the sake of comparability, but it is completed by another one based on all IEDs and landmines actually present in the same predefined area (i.e. knowing the ground truth of the detection task).

#### *IED and landmine feature estimation*

The objective of the task is to estimate some features of the detected IEDs or landmines such as the charge size. As a baseline, the estimation of the charge size is evaluated. Possibilities to evaluate the estimation of other features should be explored during the challenge.

The metric is the average percentage of estimation error.

For field tests, the metric is computed on the automatically detected IEDs and landmines. For online tests, the same metric is computed for the sake of comparability, but it is completed by another one based on all IEDs and landmines actually present in the same predefined area (i.e. knowing the ground truth of the detection task).

### **Data collection, annotation and sharing**

By default, all sensor data used for any challenge task should be provided to the challenge organisers and made available to the other teams in the framework of the challenge. In order to ensure trust and secure exchange of data, teams shall sign a data management agreement (template to be developed).

If some of the data used by a system cannot be shared for any reasons, and if the comparison between performances obtained during field tests (using all data) and online test (using only the provided subset) show a significant difference, the concerned team should report on an analysis of this difference.

While some test zones used for field tests are shown to the teams after the tests are completed and the corresponding information on the ground truth is provided as soon as possible, the ground truth for at least one of the test zones is not disclosed until it is used for online tests, together with the corresponding sensor data. Such data is expectedly used in the immediately following campaign. However, some of it can be set aside for a next campaign, in order to benefit then from data recorded in more varied conditions, and to enable more meaningful performance comparisons across years.

Additional data coming from other sources beyond the challenge can also be used if available and relevant.

Data annotation follow guidelines documented by the organisers. These guidelines are presented and discussed together with the evaluation plans.

In addition to the sensor data used as inputs by the systems, for the purpose of organisation and communication, the organisers can supervise field tests through various means such as filming them from a distance, while paying attention to avoid disturbing them.

### **Communication**

During the field tests, a live transmission of the system behaviour is foreseen. Systems should have a dedicated USB port available to plug in a radio transmitter provided by the organisers. The format of the information to provide will be defined in the detailed evaluation plans.

Representatives of potential users of the technologies can be invited to assist to field tests, and possibly to workshops.

Without prejudice to other provisions, participating teams can communicate on their own results and methods. Documents on challenge-level results are prepared by the organisers and are submitted for comments to the teams and for approval to the granting authority before actual publication.

### **Security aspects**

All participating systems should be fully compliant with the safety and security regulations (annex to be included in the detailed evaluation plans). In the event such compliance cannot be ensured, the concerned team must communicate this timely to the organising team in view of finding a suitable solution.

Further security aspects related to the field-testing sites can be defined in the detailed evaluation plans. Can in particular be covered:

- Limitations in term of usable electromagnetic frequencies and power
- Flight restrictions

### **Participation rules**

Participants must respect the rules ensuring that online tests are not biased. In particular, they should not look at the data content until completion of its processing.

### **Logistics**

During each field test week, the organisers make available a separate working area for each team. Accommodation and travel costs are covered by the teams.