EDF-2026-LS-DIS-RA-SMERO – Project for the defence supply logistics resilience

Summary

Profile type
Research & Development Request

Company's country
Spain

POD reference
RDRES20260521021

Profile status
PUBLISHED

Type of partnership
Research and development cooperation agreement

Targeted countries
- **Finland**
- **Greece**
- **Spain**
- **France**

Contact Person
Enrico FRANZIN

Term of validity
21 May 2026
21 May 2027

Last update
21 May 2026

General Information

Short summary

A Spanish industrial SME specialized in the manufacturing of precision metal components prepares a proposal aimed to develop a secure and federated digital manufacturing-as-a-service platform geared towards defence, to improve the resilience of the European supply chain, and to be submitted to the EDF Program. They seek technology centres or companies with experience in cybersecurity, resilience modelling, and industrial digital platforms for an R&D collaboration agreement.

Full description

A Spanish industrial SME specialized in the manufacturing of precision metal components (promoter of the project) together with European industrial and technological partners in the defence sector, prepares a proposal aimed to develop a secure and federated digital manufacturing-as-a-service platform geared towards defence, to improve the resilience of the European supply chain, enabling the sharing of certified production capabilities, production reallocation, and rapid response to disruptions or demand spikes.

This project addresses a key problem in the defence sector: the difficulty in reacting quickly to supply chain disruptions (e.g., supplier failures or sudden increases in demand).

It proposes to develop a secure digital platform that will allow European companies to share information about their production capacity (in a controlled manner) and coordinate to redistribute manufacturing when necessary.

The goal is to improve Europe's industrial resilience by reducing delays and external dependencies.

The project will be developed in a European consortium with industrial companies, technology centres, and cybersecurity and logistics experts.

This project falls under the European Defence Fund, which finances collaborative research and innovation projects aimed at improving European industrial and technological capabilities in defence. This type of call for proposals requires: Participation of European entities (especially SMEs and research centres).

Strict compliance with security, confidentiality, and data sovereignty requirements is needed along the project and a focus on the European impact (cooperation between countries, reduction of strategic dependencies).

The proposal is going to be submitted to the European Defence Fund program, within the call for proposals aimed at SMEs and technology centres (EDF 2026 LSRA SMERO).

Timelines (based on available information):

- Call deadline: expected by the end of September 2026.
- EOI (Expression of Interest): 15th of June 2026.

Project duration: 3-4 years.

The partners sought are technology centers or companies with experience in cybersecurity, resilience modelling, and industrial digital platforms, and their role will be focused on technological development, validation, interoperability, and compliance with defence requirements.

Advantages and innovations

Impact on industry and the market:
• Improvement of the European defence industry's responsiveness to crises by enabling the rapid redistribution of production among certified suppliers.
• Increase of the use of existing production capacity, avoiding bottlenecks and improving the overall efficiency of the supply chain.
• Strengthening of the position of European SMEs by facilitating their integration into high-value supply chains (e.g., critical components).

Impact on society and security:
• Contribution to greater European strategic autonomy by reducing dependence on external suppliers in sensitive sectors.
• Improvement of the capacity to respond to emergencies or crises (conflicts, logistical disruptions), which has an impact on overall security and stability.
• Strengthening of the trust in supply chains through control, traceability, and information security mechanisms.

Technological impact:
• Promotion of the development of advanced digital platforms with high cybersecurity requirements and management of sensitive industrial data. It introduces new models of industrial collaboration based on federated data exchange and coordination among multiple European actors.

Environmental impact (indirect):
• Optimization of the use of existing industrial resources, avoiding production duplication and reducing waste.
• Potential reduction in unnecessary transport by more efficiently reallocating production within Europe (estimated impact).

The project improves key indicators such as:
• Response time to disruptions (expected reduction)
• Production capacity utilization (expected increase)
• Number of active networked suppliers (increase by integrating SMEs)

Technical specification or expertise sought

Partners with relevant technical expertise are sought, especially in:
• Industrial cybersecurity and data protection
• Industrial digital platforms and integration systems (e.g., connection to factory systems)
• Resilience modelling and supply chain management

Stage of development

Under development

Sustainable Development goals

- **Goal 8: Decent Work and Economic Growth**
- **Goal 9: Industry, Innovation and Infrastructure**
- **Goal 16: Peace and Justice Strong Institutions**
- **Goal 12: Responsible Consumption and Production**
- **Goal 10: Reduced Inequality**
- **Goal 17: Partnerships to achieve the Goal**

IPR Status

No IPR applied

IPR Notes

Partner Sought

Expected role of the partner

The following profiles are primarily sought:
• Technology centres or universities with experience in applied research in industrial digitalization, cybersecurity, or logistics.
• Technology companies, especially SMEs specializing in industrial software development, digital platforms, or data analytics.
• Companies with experience in critical or regulated environments (defence, aerospace, or advanced industrial sectors) that are familiar with security and certification requirements.

Previous experience in European projects or international collaborations will be highly valued.

Expected roles for the partners sought:
• Development of technological components of the platform
• Integration with real industrial systems
• Technical validation in defense environments
• Support in regulatory compliance and security requirements

Type of partnership

Research and development cooperation agreement

Type and size of the partner

- **University**
- **SME 11-49**
- **SME <=10**
- **Big company**
- **R&D Institution**
- **Other**
- **SME 50 - 249**

Call Details

Framework program

Secure societies – Protecting freedom and security of Europe and its citizens

Call title and identifier

EDF-2026-LS-DIS-RA-SMERO
Non-thematic research actions by SMEs and research organisations

Submission and evaluation scheme

The topics under this call for proposals concern EDF Lump Sum Grants for Nonthematic Disruptive Actions (LS-DIS).
Lump Sum Grants for non-thematic Disruptive Actions are managed as contributions on the basis of an estimated project budget where each activi

Anticipated project budget

EUR 5 000 000

Coordinator required

Yes

Deadline for EoI

15 Jun 2026

Deadline of the call

29 Sep 2026

Project duration in weeks

208

Web link to the call

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/EDF-2026-LS-DIS-RA-SMERO-NT?order=DESC&pageNumber=1&pageSize=50&sortBy=startDate&keywords=EDF-2026-LS-DIS-RA-SMERO&isExactMatch=true&status=31094501,31094502,

Project title and acronym

ROBUST-MaaS (MaaSAI): Robust Manufacturing-as-a-Service for Defence Supply-Chain Resilience

Dissemination

Technology keywords

- **02010001 - Planning and security**
- **02010002 - Engineering**
- **02003004 - Supply chain**
- **02003005 - Information processing & Systems, Workflow**
- **02003002 - Manufacturing plants networks**

Market keywords

- **02007011 - Manufacturing/industrial software**
- **08003007 - Other industrial equipment and machinery**
- **02007005 - Communications/networking**
- **02007003 - Operating systems and utilities**

Targeted countries

- **Finland**
- **Greece**
- **Spain**
- **France**

Sector groups involved

- **Aerospace and Defence**