STRIKE IT

Call for proposals 2026
Information document including submission and evaluation guidelines and budget rules

Important dates:

Information day CFD6000: 11 February 2026 (10h30 - 14h30)
Information day CFD8000: 12 February 2026 (10h30 - 14h30)
Deadline proposals: 8 March 2026 (23h59)
Selection jury: 4 May 2026

For more information on the programme, please visit Call STRIKE IT

DEFENSIE
LA DÉFENSE

TABLE OF CONTENTS

1. RESEARCH, DEVELOPMENT, INNOVATION AND INDUSTRIALIZATION OF THE MINISTRY OF DEFENCE

1.1. CONTEXT

Scientific and technological research in the domain of security and defence is key to maintaining the Belgian Defence military and technological edge, to face current and future security challenges.

For this purpose, the Ministry of Defence (2025)[1] seeks to further develop and strengthen the links between Defence, the national research institutions and the industry by gradually increasing its R&T contribution as from 2022, with a view to reaching 2% of the total defence effort in 2030.

The setup of the Cyber Defence Factory programme fits perfectly in and contributes to the implementation of this strategic vision and general policy for Defence.

1.2. ROLE OF THE ROYAL HIGHER INSTITUTE FOR DEFENCE - RHID

As a "smart hub" and "honest broker" for scientific and technological research, the Royal Higher Institute for Defence (RHID) is responsible for the development and implementation of the Ministry of Defence's policy on scientific and technological research. Within this policy, twelve focus areas have been identified, in which research is actively supported and stimulated.

As a "smart hub", RHID aims to promote the growth of Belgian scientific and technological research in the field of defence and security, as well as to restore and strengthen the links between administrations, universities and companies at this prospect. It wishes to achieve this, among others, by promoting and facilitating the participation of Belgium and the Belgian Ministry of Defence in international, national and regional research programmes. In addition, the results of research are published annually for a wide audience and colloquia are held regularly.

As an "honest broker", RHID manages and facilitates, through the department Research, Development, Innovation and Industrialization (RDII), the research programme of the Ministry of Defence. Although in the past this programme was primarily reserved for Defence research institutions, collaboration with other partners, including Belgian research institutes and industry, is increasingly becoming the norm.

The Ministry of Defence wants to further develop its capabilities through collaborative research with external partners by launching annual open calls for proposals within the frame of its research programme. The current call is the first STRIKE IT call, based on one (1) well-defined research theme in which applicants can propose Defence-relevant research in the relevant technology domain.

More information on the institute and its activities can be found on the website: https://www.defence-institute.be/en/accueil-english/

[1] Strategic Vision of Defence

2. STRIKE IT CALL

2.1. OBJECTIVES OF THE STRIKE IT PROGRAMME

Through the funding of projects based on scientific and technological excellence, the STRIKE IT programme allows meeting the technological, operational and readiness needs of the Belgian Defence.

The **STRIKE IT call for proposals**, as part of the **Cyber Defence Factory (CDF) Programme** has **clearly defined strategic objectives** focused on cybersecurity innovation:

- Enhance IoT cybersecurity for defence and dual-use applications
- Deliver mature, testable solutions
- Address military and civilian cyber risks
- Strengthen industry-driven defence innovation base, in accordance with the Defence, Industry and Research Strategy (DIRS), to the development of a competitive and credible national industrial and technological base in the field of security and defence
- Accelerate innovation from lab to operational use
- Encourage the participation of highly qualified Belgian research institutes and industry in Defence and security related research activities.
- Promote systemic, multidisciplinary/interdisciplinary and integrative approaches.

This is the **first call** in the frame of the Cyber Defence Factories.

2.2. ELIGIBILITY CRITERIA FOR PROJECT PARTNERS

This call is open to **Belgian** public and private non-profit research institutes and private companies.

From the **public research sector**, all Belgian universities, colleges of higher education, federal scientific institutions, defence research institutes and other public research institutes are eligible partners.

Private non-profit research centres must have operational and/or research activities in Belgium. They must have legal personality and their registered office in Belgium.

From the **private sector**, companies (including SMEs) complying with the following criteria are eligible partners:

- The company must have operational and/or research activities on the Belgian territory.
- The company must have a legal personality and its registered office in Belgium. The legal personality is required at the latest when signing the research contract.
- At the moment of signing the contract, the company must have fulfilled its obligations to pay its taxes and social security contributions.

Foreign partners cannot participate in the call.

The project partnership is preferably a **triple helix composition** where academia and industry work together to foster R&T(D) for Defence. Specific partnership requirements are set out in section 3.5.

NOTES FOR COMPANIES, A(I)SBL AND FOUNDATIONS:

The delivery of the following documents is a formal requirement for a valid application for the call:

- As foreseen in the law of 18 September 2017, **companies, a(i)sbl and foundations** must have submitted accurate and current information on their beneficial owners to the UBO (Ultimate Beneficial Owner) register of the FPS Finances. **The extract of the UBO register must be provided by e-mail to** strike-it@mil.be **before 8 March 2026.**
- The consent form relating to the law of 20 December 2024 on classification and security clearances, security advice and the publicly regulated service (available in Dutch and French on the STRIKE IT website) must be completed by the natural persons listed on the UBO form and sent to bureau.industrie@mil.be for verification . **Proof of dispatch of this form to the "bureau industrie" must be provided by e-mail to** strike-it@mil.be **before 8 March 2026**. A negative opinion from the administrative authority for at least one of the persons listed on the UBO may result in the legal entity being refused participation in the project.
- A company Honourability & Vulnerability self-assessment declaration must be delivered to guarantee the company honourability, ethics & professional conduct. This declaration must be sent by e-mail to strike-it@mil.b **before 8 March 2026.**

For funded partners and subcontractors: You are a **company, a(i)sbl or a foundation**?		
Document	**Name and format of the file**	**How to deliver?**
Extract(s) from the UBO register	ACRONYM_UBO_COMPANY.pdf	E-mail to strike-it@mil.be
Consent form(s) for security verification	ACRONYM_CONSENT_COMPANY_PERSON.pdf	E-mail to bureau.industrie@mil.be
Proof(s) of dispatch of the consent form(s) for security verification	ACRONYM_PROOF_COMPANY_PERSON.pdf	E-mail to strike-it@mil.be
Company Honourability & Vulnerability self-assessment declaration	ACRONYM_DECLARATION.pdf	E-mail to strike-it@mil.be
Failing to deliver these documents will result in exclusion of the proposal		

2.3. INFORMATION DAY

To inform potential applicants about the context, scope and modalities of this call and to offer them network opportunities, an information day will be held on **Wednesday 11 February 2026 at CDF6000 (Charleroi) and Thursday 12 February 2026 at CDF8000 (Brugge).**

Registration prior to the event is required.

More details are announced through the and the **STRIKE IT** website as well as through social media.

3. CALL INFORMATION

3.1. DOCUMENTATION RELATED TO THIS CALL

The following documents are available on the STRIKE IT website (Call Strike IT - IRSD-KHID-RHID)

- Information document, including submission and evaluation guidelines and budget rules: general information on the programme and the call, overview proposal content and corresponding evaluation criteria for the applicants and the evaluators (the present document)
- Evaluators eligibility: eligibility criteria for potential remote evaluators
- Evaluation matrix for proposals: overview of the evaluation ratings for the proposals
- FAQ
- Proposal structure (word-file available on the website platform)
- Veiligheidsverificatie toestemming – Vérification de sécurité consentement
- Company Honourability & Vulnerability self-assessment declaration
- Ethics self-assessment
- Gantt chart
- Budget file

3.2. INDICATIVE CALENDAR OF THE CALL

	Date	**At / via**
Information sessions	11 February 2026 12 February 2026	CDF6000 (Charleroi) CDF8000 (Brugge)
Deadline proposals	8 March 2026 (23h59)	Mail
Remote scientific peer review evaluation	9 March – 3 April 2026	Online
Ethical Evaluation	9 March – 25 March 2026	RHID
Internal selection of proposals	4 May 2026	RHID
Communication of results to applicants	6 May 2026	Mail

3.3. RESEARCH THEMES AND INDICATIVE BUDGET OF THIS CALL

The present call covers the theme of cybersecurity of the Internet of Things (IoT). Up to 12 projects will be funded, for a total amount of 1.8 M EUR. 6 projects will be selected regarding Theme 1: Cybersecurity of connected objects, including flying systems, vehicular platforms, and smart appliances. CDF6000 – Charleroi (A6K) and 6 projects will be selected regarding Theme 2: Cybersecurity of connected systems onboard vessels and within port environments. CDF8000 – Brugge (Howest).

The maximum budget per project is up to 150,000 EUR. Applicants should take into consideration the most efficient use of public resources.

The number of projects that will be funded depends on the evaluation of the proposals. Passing the threshold of excellence and quality, the best ranked proposals will be funded. The proposals will be put together in a ranking list based on their final evaluation.

Budget transfers between the projects are possible.

3.3.1. THEME– Cybersecurity of connected objects (flying, driving, smart appliances)

1. Context

Modern defence and security systems increasingly rely on connected technologies, particularly IoT. Nowadays civilian IoT and military IoT are interconnected. As civilian IoT directly feeds into and enables military IoT, their vulnerabilities converge, meaning that weaknesses in civilian systems translate immediately into operational risks for defence and security missions.
STRIKE IT 2026 addresses this structural challenge through a whole-of-society approach, recognising that cyber threats do not respect civilian–military boundaries. Its relevance and impact lie in strengthening end-to-end capabilities to protect, detect, and defend across both civilian and military IoT environments. The higher the level of cyber protection and resilience across society, the stronger, more aware, and more resilient military IoT and defence operations become.
STRIKE IT 2026 is fully aligned with the **EU Cyber Resilience Act**, reinforcing security-by-design, lifecycle security, and vulnerability management for connected technologies. By strengthening preventive protection, early detection, and coordinated cyber defence across the civilian digital foundations underpinning military IoT, the initiative acts as a force multiplier for defence resilience and operational continuity.

2. Scope

STRIKE IT 2026 invites proposals focused on deployable, mature cybersecurity capabilities that are already close to operational deployment in civilian markets. The scope explicitly excludes fundamental research and instead prioritises system integration, operational deployment, and lifecycle resilience of existing technologies.
STRIKE IT 2026 is grounded in a **whole-of-society approach**. Accordingly, the scope is not limited to defence-specific use cases, but targets solutions that strengthen cybersecurity across civilian environments, recognising their direct relevance and impact on defence and security ecosystems. These solutions can be delivered as **technological goods, operational services, or applied education and training.**
The programme STRIKE IT 2026 is structured around two complementary thematic streams:

- **Theme 1**: Cybersecurity of connected objects, including flying systems, vehicular platforms, and smart appliances. CDF6000 – Charleroi (A6K). Focus: Land and air domains. This includes, and is not limited to: connected wearables, connected tools, connected cars (manned or unmanned), secure by design and/or by default, Ability to operate in degraded or contested connectivity environments, …

- **Theme 2**: Cybersecurity of connected systems onboard vessels and within port environments. CDF8000 – Brugge (Howest). Focus: Maritime and naval domains. This includes, and is not limited to connected wearables, connected tools, onboard vessel systems (manned or unmanned), ports, and logistics chains, ports, and logistics chains, cyber resilience of navigation, propulsion, cargo, and situational awareness systems

Together, these two streams address the cybersecurity challenges of connected objects and systems across key operational domains, reinforcing protection, detection, and defence capabilities across civilian and defence-relevant environments.

3. Impact for Defence

Proposals are expected to demonstrate clear impact and excellence for defence and security by delivering operationally relevant cybersecurity outcomes. Solutions should contribute to the following objectives:

- Reduce systemic cyber risk by securing dual-use IoT ecosystems, strengthening baseline security across civilian IoT and military IoT, and thereby enhancing mission assurance, safety, and continuity of operations.
- Increase trust in civilian-origin technologies used to support defence and security missions, ensuring their reliability, integrity, and resilience in operational contexts.
- Strengthen defence readiness and resilience by improving preparedness, response, and recovery capabilities, moving beyond threat detection alone toward full lifecycle cyber resilience.
- Secure civilian IoT as a precondition for effective defence, recognising that robust protection of civilian digital infrastructures directly underpins military effectiveness, operational continuity, and strategic credibility.

3.4. PROJECT DURATION

The projects will have a duration of **maximum 6 months**.

3.5. PROJECT PARTNERSHIP

3.5.1. PARTNERSHIP

Triple-helix partnerships are encouraged but proposals submitted by one private company will be eligible as well. If a proposal is submitted, it must contain at least one private company.
All types of organisations can act as project leader.

Partnership:
- At least one private company
- Triple-helix partnerships are encouraged

Belgian Defence research institutes (Royal Military Academy (RMA), Military Hospital Queen Astrid (MHQA) and the Defence Laboratories (DLD)) are eligible partners. However, it will not have a beneficial effect on the evaluation result (no bonus).

3.5.2. ROLES AND RESPONSIBILITIES WITHIN THE PROJECT

Project partners jointly share obligations and responsibilities during the implementation of the project. The project should be fairly balanced, even if different partners may have different tasks and subsequently different budgets.

A **coordinator** must be appointed in each network proposal.

For each project, a **Steering Committee** shall be established at the start of the project to act as the governing body (see section 6.3).

ROLE OF THE COORDINATOR

The coordinator is responsible for the overall project management and coordination. He/she is the contact person for the RHID to communicate with the partnership and must transfer all relevant information to the other project partners. He/she shall:

- Coordinate all activities to be carried out in the framework of the project,
- Coordinate the internal meetings between the network members,
- Coordinate the production of the required project reports intended for Belgian Defence as described in section 6.4.,
- Coordinate the synthesis and translation of the research results, with a view to applications and support for decision-making,
- Coordinate the publication and dissemination of the research results,
- Convene meetings of the Steering Committee and write the reports of these meetings. The coordinator shall give notice in writing of a meeting with the agenda to each member no later than fourteen (14) calendar days in advance,
- Inform the Steering Committee and the RHID of any problems that might hinder the implementation of the project.

SUBCONTRACTORS

The project may require specific or punctual expertise, which can be delivered in the form of **subcontracting**. It is the responsibility of the project team to ensure that the rules and practices of the subcontractor, and in particular the ownership and valorisation of research results, publications and communications, are compatible with the rules governing the call. The project team takes full responsibility for the final result of the subcontracted work.
Subcontractors must be registered in Belgium. Subcontractors that are companies, a(i)sbl and foundations must submit accurate and current information on their beneficial owners to the UBO (Ultimate Beneficial Owner) register of the FPS Finances and deliver an extract of the UBO register to the DEFRA secretariat.

In case the subcontractor needs access to classified information, the subcontractor must also obtain a security clearance (see section 7.2).

Subcontractors must be registered in Belgium. If they are a company, a(i)sbl or foundation, they must provide:
- an extract from the UBO register
- proof of delivery of security verification consent
- company honourability & vulnerability awareness self-assessment

3.6. RESEARCH ETHICS

The "Code of Ethics for Scientific Research in Belgium" is a joint initiative of the Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique, the Académie Royale de Médecine de Belgique, the Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten and the Koninklijke Academie voor Geneeskunde van België.

All projects must take this code of ethics into account in their research. If applicable, it is the responsibility of the applicants to consult the relevant Ethical Board for their organisation before submitting a proposal.

The code of ethics for scientific research in Belgium is available here: http://www.belspo.be/belspo/organisation/publ/pub_ostc/Eth_code/ethcode_en.pdf.

It is the responsibility of the applicants to consult the relevant Ethical Board for their organisation before submitting a proposal.

Applicants will be required to complete an "ethics self-assessment" when preparing the proposal. The Ethical Advisory Board of the RHID will assess this information and can advise the partnership how to deal with the ethical aspects of its proposal.

3.7. BUDGET RULES

Financing by Defence: This call is subject to the European legislation on State Funding (Art 107 (1) TFEU and the General Block Exemption Regulation in particular. Therefore, financing a public research institute or a private non-profit research centre is set to a maximum of 100% of the eligible costs. Financing a private company is limited to a maximum of 65% of the eligible costs, with a potential maximum of 80%, according to the size of the company.

The total project budget must be detailed in the tables of the budget file (100% cost) of the full proposal. Additional columns are foreseen to indicate the partner contribution to the total project cost (depending on the partner type) and the subsequent RHID funding contribution. (section 6.5 of the full proposal template: Budget assessment)

The project budget is reserved exclusively for the project activities. The different categories of expenditure financed by Defence are:

Staff: Pre-tax wages associated with increases in the cost of living, employers' social security and statutory insurance contributions, as well as any other compensation or allowance due by law and secondary to the salary itself. Defence does not allow cumulative wages for staff. Staff members bound contractually to a public institution - full time or part time - cannot apply for him/herself for Defence staff budget for that part.

The RHID prefers staff to be hired under a labour contract.

Costs related to non-employee staff, i.e. staff working in a management company, as freelancer or interim staff on behalf of the partner are also accepted.

Tax-free doctoral or post-doctoral scholarships are not accepted.

For persons to be hired for the project (so not identified by name in the proposal), the staff costs are limited to a maximum amount of:

- 5 700 €/month FTE for a technician/bachelor (regardless of years of experience)
- 8 000 €/month FTE for a Master (regardless of years of experience)
- 8 700 €/month FTE for a Master in engineering (regardless of years of experience)
- 10 500 €/month FTE for a PhD (regardless of years of experience)

The funding is limited to the time and period in which the (employee and non-employee) staff participates in the project.

General operating costs: this includes daily/usual supplies and products for the laboratory, workshop and office, documentation, consignments, use of daily software and IT facilities, organisation of internal meetings, etc. The general operating budget may not exceed 15% of the overall project staff budget for the project coordinator and 10% for the other project partners. The amounts claimed must correspond to actual expenditures strictly related to the project, even if supporting documents are not requested. Although no detailed justification is required for these costs, the administration of the concerned partner must keep these invoices in its accounts in the event of an audit.

Specific operating costs: this includes a list of operating costs specific to the execution of the project tasks, such as costs for project analyses, testing, maintenance and repair of equipment purchased by the project, use of specific IT facilities and software, costs for surveys, open data publications, organisation of workshops and events, etc. These costs need to be clearly described in the proposal and each of them shall be justified by invoices during the project.

Overheads: Institutions' general overheads that cover, in one lump sum, administration, telephone, postal, maintenance, heating, lighting, electricity, rent, machine depreciation, and insurance costs. The total amount of this item is set as a fix amount of 10% of the total staff and operating costs.

Equipment: List of investment goods specific to the implementation of the project and to be purchased on the project budget. It concerns the purchase and installation of scientific and technical equipment and instruments, including computer equipment, to be entered in the inventory or assets of the institute/company. Equipment needs to be clearly described in the proposal and shall be justified by invoices.

Subcontracting: Expenses incurred by a third party to carry out project tasks or provide services that require special scientific or technical competences outside the partner's normal area of activity. The amount may not exceed 25% of the total budget allocated to the partner concerned. If the subcontractor is not yet known then only the nature, the planned duration and the estimated amount needs to be indicated in the proposal.

	STAFF COSTS (monthly costs)	GENERAL OPERATION COSTS	SPECIFIC OPERATION COSTS	OVERHEADS	EQUIPMENT	SUBCONTRACTING
PROJECT COORDINATOR	**Technician**: 5 700€/month	15% of Staff costs *(Automatically generated)*	-	10% of [Staff costs + Operation costs] *(Automatically generated)*	-	Max. 25% of the total budget of this partner
	Master: 8 000€/month					
	Master (engineering): 8 700€/month					
	PhD: 10 500€/month					
OTHER PROJECT PARTNERS	**Technician**: 5 700€/month	10% of Staff costs *(Automatically generated)*	-	10% of [Staff costs + Operation costs] *(Automatically generated)*	-	Max. 25% of the total budget of this partner
	Master: 8 000€/month					
	Master (engineering): 8 700€/month					
	PhD: 10 500€/month					

3.8. GENDER

The RHID strongly encourages the applicants to take into account the equality between women and men and to ensure gender mainstreaming in the implementation of the project. The project should include this both in the choice of the researchers and, where relevant, by integrating the gender dimension into their research.

4. SUBMISSION PROCEDURE

The submission of projects will be done in one phase using the following e-mail:

strike-it@mil.be

4.1. PROPOSAL

Your **proposal** and the required documents must be submitted at the latest on **8 March 2026 (23h59)** by e-mail to strike-it@mil.be

The proposal form can be downloaded from the website and must contain all following information:

- The choice of the factory site (CDF6000 or CDF8000)
  - CDF6000 (Charleroi-A6K): Focus on land and air domains
  - CDF 8000 (Brugge-Howest): Focus on maritime/naval domains
- The title and acronym of the project
- The coordinates of the foreseen partners, if applicable
- Executive Summary of the project
- Keywords (min 2; max 6).
- Scope and objectives,
- State of the art and innovative character,
- Relevance and potential impact for Defence, including the data management plan and quality of the partners/partnership of the project,
- The work plan: work packages, the project risk assessment, the budget assessment.
- The name and contact details of 2 to 4 scientific experts (**Belgian** and/or **foreign** experts) capable of assessing the proposal. Optionally, the name and contact details of 2 non-grata scientific experts to be excluded from the evaluation of the proposal under the condition of sufficient motivation.

As a separate document which can be downloaded from the website:

- The GANTT chart
- Budget file
- Ethics Self-Assessment

The total length of each section of the **proposal** should not exceed **the word count limit indicated**.

Companies, a(i)sbl and foundations must deliver the extract of the Ultimate Beneficial Owner (UBO) register as an annex to the proposal (in pdf format) and sent it by e-mail to strike-it@mil.be

The proof of dispatch of the form “veiligheidsverificatie_toestemming / vérification de sécurité_consentement” and the “Company Honourability & Vulnerability self-assessment declaration” must be sent by e-mail to **strike-it@mil.be**. Please provide these documents grouped by pre-proposal.

RHID and Cyber Command will perform an eligibility check on the basis of the proposal documents. The proposals that have passed the eligibility check will be evaluated through a remote peer evaluation.

5. EVALUATION PROCEDURE AND CRITERIA

5.1. EVALUATION PROCEDURE OF PROPOSALS

Only proposals that are complete and submitted on time will be taken into account.

RHID and Cyber Command will perform an eligibility check on the basis of the proposal documents. Following criteria are applied:

- Completeness of the proposal (all fields fully completed, UBO extracts available, proof of dispatch of the form "veiligheidsverificatie_toestemming / vérification de sécurité_consentement" and the "Company Honourability & Vulnerability self-assessment declaration" available, additional documents available)(see section 4.1)
- Eligibility of each project partner (see section 2.2),
- Partnership composition (see section 3.5.1).

Proposals will, in the next step, be evaluated based on a peer-review evaluation executed by a panel composed of experts having an adequate combined expertise to evaluate the research proposal.

For each proposal, an individual written evaluation is performed. The written evaluation takes place remotely, based on an evaluation form. During this assessment, the experts will only have access to the proposals they will evaluate. They will not know the other reviewers are for that proposal, nor will they have access to each other's evaluations.

Each reviewer will assess the proposal and provide comments taking into account a variety of (sub)criteria, namely in the following categories:

- Overall quality
- Quality proposed solution
- Impact for Defence and for society

More information about the criteria used can be found in the evaluation matrix for proposals.

The individual evaluations are not communicated to the applicants.

This remote peer evaluation will take place between 9 March and 3 April 26 after the submission of the proposals.

After the remote peer review evaluation, the proposals will be evaluated by an internal evaluation committee chaired by Belgian Defence on the basis of a consensus report and taking into account the following criteria:

- The match between the proposal and the scope of call,
- The quality of the proposal, based on the description of the project objectives and the innovation with respect to the state of the art,
- The quality of the partners and the adequacy of the partnership,
- The relevance and potential impact for Defence.

6. ROYAL DECREE AND CONTRACTUAL OBLIGATIONS FOR SELECTED PROJECTS

6.1. PROJECT STARTING AND END DATE

The projects selected within the context of the current call will start 01 June 2026.

The project contracts will have a duration of 6 months plus 1 month to allow meeting all administrative requirements before the effective start-up of the project).

6.2. ROYAL DECREE AND CONTRACTS

For the selected proposals, a Royal Decree is decided, and a contract is conducted between Belgian Defence and the funded partners.

The contract is composed of three parts that make up the research contract:

- Basic contract
- Annex I: Technical specifications
- Annex II: General conditions applicable to the 2025 contracts.

The basic contract designates the contracting parties (partners and Defence) and contains the general obligations applicable to the project, including the project and contract duration and budget. **The basic contract is signed by the heads of the partners involved (directors, rectors, CEOs).**

The content of Annex I "Technical specifications" is specifically related to the operational implementation of the project. It includes the detailed work description and schedule, details on funding by expenditure category etc. **Annex I "Technical specifications" is signed by the STRIKE-IT programme manager and the promotors concerned.**

Annex II "General conditions applicable to the contract" contains all general provisions applicable to all STRIKE-IT contracts. It is available on the STRIKE-IT website and **will not be signed**.

Belgian Defence/RHID grants the selected projects the funds required for their implementation. The RHID shall reimburse at most, and up to the amount specified in the granted budget, the actual costs proven by the partners providing these costs are directly related to the implementation of the project.

The partnership is encouraged to conclude a Consortium Agreement to define internal regulations regarding intellectual property (access to foreground and background, valorisation rights and modalities, and any other theme deemed necessary). A copy of the signed Consortium Agreement must be handed over to the Royal Higher Institute for Defence (RHID, strike-it@mil.be).

6.3. COMPOSITION AND ROLE OF THE STEERING COMMITTEE

Each project will be accompanied by a **Steering Committee**, to be set up at the start of the project. The Steering Committee is composed of the project managers of the partners, the programme manager, the research manager of Defence and the intended end user of Belgian Defence.

The Steering Committee acts as a governance body, to ensure that the project remains in line with the research objectives and adapt the project plan accordingly whenever necessary. It ensures that the project reporting is done in accordance with section 6.4.

The Steering Committee should meet at least once a month to discuss the project's progress. The organisation of such meeting must be included in the project work plan and the project budget.

The following actions and decisions will be taken by the Steering Committee:

- Examine information collected by the coordinator on the progress of the Project, to assess the compliance of the Project with the Proposal and, if necessary, propose modification of the Proposal.
- Determine the policy for press releases, joint publications and other public disclosures regarding the Project.
- Keep a register of Foreground generated within the Project and patents filed thereon, which is concluded at the end of the Project.
- Examine and approve proposed changes to the work programme. In case of actions with a budgetary impact, the Steering Committee will make proposals to the funding authority but cannot decide without the approval of this funding authority.
- If necessary, propose the termination of all or part of the Project.

6.4. REPORTS

The contract foresees the following reports to be submitted to the RHID:

- Initial report: to be submitted within three weeks of the start of the project.
- Progress report(s): to be submitted according to the specifications in the contract (annex 1, technical specifications).
- Final report: to be submitted one month after the end of the project.
- If deemed useful by the RHID, an additional report may be requested for an external evaluation of the project.
- The RHID can ask for a report or other input at any time during the course of the project in order to provide scientific support to valorisation and service actions related to the programme.

These reports are to be included in the project work plan and the cost of preparing them (including possible translations) must be covered by the project budget.

They should contain all necessary information to assess the progress of the project in relation to the work packages, deliverables and budget. Problems must be identified, including possible solutions.

To evaluate the impact of the STRIKE IT programme, the RHID can ask input from the partnership until 3 years after the end of the project.

7. DATA, RESULTS, INTELLECTUAL OWNERSHIP AND SECURITY REQUIREMENTS

7.1. GENERAL CONDITIONS

The Data Management Plan (DMP), to be submitted as part of the proposal, describes how the project partners deal with the collected data before, during and after the project. It is a key element of good data management.

For all aspects regarding the use of data, intellectual ownership and valorisation of the project results and the confidentiality or security requirements, the conditions of the General Conditions (Annex II of the contract and the articles 12, 13 and 14 in particular) apply.

Ownership of existing information and data (the individual background) remains with the original owner.

As a principle, the Foreground - the results (including information) produced by the project - shall be the property of the partner carrying out the work generating this foreground.

The principles for the use of joint foreground will have to be determined by the project partners, with respect for these General Conditions. These principles can be included in a Consortium Agreement to be concluded between the partners.

7.2. CLASSIFIED INFORMATION/SECURITY RELATED ACTIVITIES

Projects aiming at developing or using sensitive or classified information's will not be funded by STRIKE IT.
However, certain activities undertaken in the frame of the projects may generate classified information. This paragraph solely concerns protective measures to be taken to preserve the confidentiality of security-sensitive information regarding these projects.

A classification is given to documents to prevent their improper use which could damage, among other things, the fulfilment of the tasks of Defence, the external security and international relations of the State and the scientific and economic potential of the country (for the complete list see "Wet van 20 Dec 2024 Art 3/Loi du 20 Déc 2024 Art 3").

According to the same law this identification should be based on the following classification levels:

- The "**TRES SECRET/ZEER GEHEIM**" level is assigned to a piece if its improper use could cause EXTREMELY SERIOUS damage to the main Belgian interests listed in the law. Topics that qualify under this category cannot be part of the project.
- The "**SECRET/GEHEIM**" level is assigned to a document if its improper use could cause SERIOUSLY damage to the interests listed in the law.
- The "**CONFIDENTIEL/VERTROUWELIJK**" level is assigned to a document if its improper use could harm any of the interests listed in the law.

Documents of which the originator wants to limit the distribution to persons who are authorized to use them on a need-to-know basis, without however attaching legal consequences to this limitation, are marked with the indication "**DIFFUSION RESTREINTE/BEPERKTE VERSPREIDING**".

These classification levels should be applied both to the need to protect information and the need to avoid unnecessary obstruction to the use of research information and results.

Applicants should identify in the Full-Proposal the classification needs for the work packages of the project that involve threat and /or vulnerability assessments and the information on specifications or capabilities of the tool(s) used.

- threat assessments (i.e. estimation of the likelihood of a malicious act against an asset, with particular reference to factors such as intention, capacity and potential impact)
- vulnerability assessments (i.e. description of gaps or weaknesses which can be exploited during malicious acts, and often contain suggestions to eliminate or diminish these weaknesses)
- specifications (i.e. exact guidelines on the design, composition, manufacture, maintenance or operation of threat substances or countermeasure substances, technologies and procedures)
- capability assessments (i.e. description of the ability of an asset, system, network, service or authority to fulfil its intended role — and in particular the capacity of units, installations, systems, technologies, substances and personnel that have security-related functions to carry these out successfully)

Based on the assessment of the provided input a security screening by Belgian Defence might be imposed in the contract on ALL partners and subcontractors of the selected project(s). In that case, these beneficiaries should obtain a security clearance before starting work on classified parts of the project.

The applicable security framework for the action must be in place at the latest before the signature of the contract and will be considered as an annex to the contract.
More information can be found on the website of the National Security Authority (Nationale Veiligheidsoverheid – Autorité Nationale de Sécurité) https://www.nvoans.be/

Persons that are involved in a project must be nationals of a country of the European Union or nationals of a country of the European Free Trade Association or nationals of a country that is a member of NATO.
Persons involved in a project may be subject to a verification. Only after a positive verification, a person can be recruited to the project.

8. COMPLAINTS

RHID places great importance on the quality of their service and on improving the way they operate. A, RHID will handle complaints about the administrative handling of this call for proposals and/or about content of the call and the contracts that are concluded as a result of the call.

A special form to handle complaints has been created.

The complaint form is available through the website of STRIKE-IT.

Complaints submitted anonymously or which are offensive or not related to our organisation will not be processed.

A complaint is handled as follows:

- Once your complaint has been filed, a notification of receipt will be sent.
- The complaint will be forwarded to the relevant departments and individuals and will be processed within one month.
- An answer will be sent by e-mail or letter.
- The complaint will be treated with strict confidentiality.

If you are dissatisfied by the initial response to a complaint, you can always contact the Médiateur Fédéral / Federal Ombudsman, rue de Louvain 48 bte 6 / Leuvenseweg 48 bus 6, 1000 Brussels (email: contact@mediateurfederal.be / contact@federaalombudsman.be).

9. CONTACTS

Further information can be obtained by contacting: strike-it@mil.be