Dear Sir or Madam,

Please find below a Request for Proposal ("RfP"). The deadline for the submission of Proposals is **31 July 2026**, in accordance with the terms and conditions set out below.

## 1. Background

Federale Participatie- en Investeringsmaatschappij / Société Fédérale de Participations et d'Investissement ("SFPIM") is a public limited company of public interest, whose registered office is located at 1050 Brussels, Avenue Louise - Louizalaan 32, box 4, and registered with the Crossroads Bank for Enterprises under number 0253.445.063 (RLP Brussels) (VAT BE 0253.445.063).

SFPIM was established on 1 November 2006, following the merger of the Federale Participatiemaatschappij / Société fédérale de Participations and the Federale investeringsmaatschappij / Société fédérale d'Investissement. Since then, SFPIM has acquired a central role in federal investment policy and in anchoring the strategic assets of our country. It manages over 200 participations and investments.

SFPIM is governed by the Law of 2 April 1962 relating to SFPIM and the regional investment companies. The Belgian State is the sole shareholder of SFPIM.

SFPIM aims to shape public ownership and federal investment policy by serving the financial interests of the State, while also promoting the prosperity of the Belgian economy and employment. This is pursued in line with the principles of sound management, sustainability, socially responsible entrepreneurship, and good corporate governance.

SFPIM pursues this objective by operating both as a public holding company and as an investment company. SFPIM is also mandated to carry out delegated missions, contributing to the implementation of the State's industrial policy and to the resolution of financial institutions. Additionally, it may be entrusted with specific advisory roles for the Government.

Further information about SFPIM and its subsidiaries is available on the website www.sfpim.be

## 2. Purpose of the RfP

SFPIM currently holds **CyFun Basic** certifications. To take the next step towards **CyFun Important** and **CyFun Essential**, a more formal and comprehensive architectural design is required, complemented by enhanced detection and response capabilities.

On one hand, SFPIM currently employs approximately 50 staff members and operates a proportionate IT environment.
On the other hand, SFPIM, though a subsidiary working in the same IT environment, is busy with investments in the defense sector.
Candidates are expected to take this context into account when proposing architectural, SIEM and SOC solutions.



**Société Fédérale de Participations et d'Investissement**
Société Anonyme d'Intérêt Public

**Federale Participatie-en Investerings Maatschappij**
Naamloze Vennootschap van Openbaar Nut

Avenue Louise - Louizalaan, 32/4
1050 Bruxelles - Brussel

RPM (Brussel – Franstalige afdeling) 0253.445.063
TVA BE 0253.445.063

The purpose of the assignment is to establish and implement an integrated cybersecurity framework for SFPIM, encompassing the design of the network and identity architecture, the deployment of a SIEM platform, and the provision of Security Operations Centre (SOC) services for continuous security monitoring and incident management.

## 3. Scope of services

Candidates are invited to submit their best proposal for :

- Inventory and assessment (As-Is) of network and identity components;
- Design of a target architecture (To-Be) for network, segmentation, and identity;
- Transferable and audit-ready documentation;
- SIEM implementation (design and configuration);
- SOC service delivery (operational);
- Trainings for IT people and table top exercises for all relevant workers

### 3.1 Current-state assessment (As-Is)

- Inventory of all relevant network components, including firewalls, switches, wireless infrastructure, WAN/ISP connectivity, VLANs, subnets and network traffic flows.
- Production of comprehensive As-Is network diagrams.
- Assessment of asset types, business criticality, data sensitivity and relationships between IT assets and critical business processes.
- Assessment of the current Active Directory and Microsoft Entra ID environments, including:
    - Organisational Unit (OU) structure;
    - Security groups;
    - Administrative accounts;
    - Service accounts;
    - Identity dependencies across systems and applications.

### 3.2 Target Architecture Design (To-Be)

- Architecture principles based on Zero Trust, Least Privilege, Defence-in-Depth, segregation of duties and auditability.
- Logical and physical network segmentation architecture.
- Definition of security zones and controlled communication paths.
- Identity governance model, including:
    - Target OU structure;
    - Role-based access control model;
    - Privileged access model;
    - Identity-based access architecture.
- Security monitoring and logging architecture.
- SIEM integration principles.
- High-level resilience, redundancy and fail-over architecture guidelines.

### 3.3 Transferable Implementation Documentation

- Delivery of technology-agnostic implementation documentation suitable for execution by SFPIM's operational IT partner.

- Documentation shall include:
    - Architecture diagrams;
    - Design principles;
    - Security assumptions;
    - Compliance mapping;
    - Implementation prerequisites;
    - Risks and dependencies.

### 3.4 SIEM Platform Design and Implementation

- Configuration of the SIEM platform.
- Integration of logs from:
    - Network infrastructure;
    - Active Directory / Microsoft Entra ID;
    - Endpoints;
    - Cloud environments.
- Development of detection rules and monitoring use cases.
- Dashboards and reporting.
- Documentation and knowledge transfer.

***Minimum Detection Capabilities***

The proposed SIEM solution shall provide, at a minimum, detection capabilities for:

- Suspicious authentication events and login anomalies;
- Privilege escalation attempts;
- Suspicious administrative activities;
- Suspicious network behaviour;
- Non-compliant or unauthorised devices.

Candidates shall provide examples of proposed detection use cases and alerting logic.

***Detection Use Case Catalogue***

The Candidate shall provide a Detection Use Case Catalogue identifying the proposed monitoring and detection use cases. The catalogue shall include, at a minimum, coverage across identity, endpoint, network, cloud and data-related threats.
The Candidate shall describe how detection use cases are maintained, reviewed and improved over time.
Preference will be given to proposals that demonstrate detection coverage mapping against recognised cybersecurity frameworks such as MITRE ATT&CK.

***Log Collection and Coverage Matrix***

The Candidate shall provide a Log Collection Matrix identifying:

proposed log sources;
scope of collection;
retention periods;
ownership of log onboarding activities;

dependencies and assumptions.

The Candidate shall clearly identify any limitations in monitoring coverage and any log sources that are recommended but excluded from the proposed scope.

***SIEM Sizing Principles***

The proposed SIEM solution must be proportionate to SFPIM's size, complexity and risk profile.

Particular attention will be paid to:

- Operational simplicity;
- Limited internal operational overhead;
- Cost predictability;
- Scalability towards higher maturity levels;
- Avoidance of over-engineered solutions.

Overly complex or oversized solutions may result in a lower evaluation score

### 3.5 SOC services

Candidates shall clearly describe:

- Monitoring model (8x5, 24x7 or other);
- Detection capabilities;
- Incident triage process;
- Escalation process;
- Response capabilities;
- Use of automation;
- Reporting methodology;
- Service Level Agreements (SLAs);
- Response times.

***Minimum Scope***

The proposed SOC service shall include:

- Monitoring of SIEM alerts;
- Incident detection and triage;
- Escalation to SFPIM;
- Periodic reporting;
- Threat hunting capabilities;
- Continuous tuning and improvement of detection use cases.

Where applicable, candidates shall clearly specify whether active response actions (containment or isolation) are included.

All SOC activities, escalations, investigations and response actions shall be fully traceable and auditable.

***KPI Framework***

The Candidate shall provide a comprehensive operational KPI framework covering, where applicable:

- Mean Time To Detect (MTTD);

- Mean Time To Investigate (MTTI);
- Mean Time To Respond (MTTR);
- Mean Time To Contain (MTTC);
- false positive rate;
- detection use case coverage;
- SIEM platform availability;
- SLA compliance rate.

Additional KPIs may be proposed by the Candidate if considered relevant to the quality and maturity of the proposed service.

**KPI *Definitions***

For each KPI and SLA, the Candidate shall provide:

- the calculation method;
- the measurement frequency;
- the reporting frequency;
- the proposed target value;
- any thresholds triggering escalation or corrective actions.

SFPIM reserves the right to request clarification regarding KPI definitions and measurement methodologies during the evaluation process.

***Detection Validation and Security Exercises***

Candidates shall describe their approach to validating the effectiveness of monitoring and detection capabilities.

The Proposal shall indicate whether the service includes or supports:

- attack simulations;
- purple team exercises;
- ransomware detection validation;
- compromised account detection validation;
- MITRE ATT&CK-based coverage assessments.

Any associated deliverables and reporting shall be clearly described.

### 3.6 Regulatory and cybersecurity requirements

The proposed solution and services shall be aligned with applicable cybersecurity standards and regulatory requirements, including, without limitation, the GDPR and the NIS2 Directive.

### 3.7 Deliverables

The Proposal shall clearly identify all deliverables, implementation milestones, assumptions, dependencies, service levels, timeline and required involvement from SFPIM.
The services are expected to be provided in English, French and/or Dutch.

The final architecture documentation shall be sufficiently detailed to allow implementation by a third-party IT provider without requiring substantial redesign or reinterpretation.

## 4. Content of the Proposal

The proposal must contain a presentation explaining, point by point and in the order shown below, the aspects described below.

### *4.1 Quality of services and methodology*

The Proposal shall describe in detail:

- the understanding of SFPIM's needs and cybersecurity context;
- the proposed methodology for architecture assessment, SIEM implementation and SOC setup;
- implementation timeline and milestones;
- service model for SOC activities, including escalation process, alert triage, incident handling and response processes;
- proposed service levels (including availability, monitoring, escalation and reporting);
- assumptions, dependencies and key risks;
- knowledge transfer, training and documentation approach;
- confidentiality, business continuity and cybersecurity measures.

Candidates shall clearly explain:

- why the proposed SIEM solution is appropriate for SFPIM;
- which alternative solutions were considered;
- how unnecessary complexity and over-dimensioning are avoided.

### *4.2 Pricing*

The Proposal shall include a complete and transparent pricing structure in EUR (excluding VAT), clearly distinguishing between:

- one-off implementation costs (CAPEX);
- recurring operational costs (OPEX);
- licensing costs, where applicable;
- implementation, maintenance, support and managed service costs;
- assumptions relating to pricing;
- any optional services or additional costs.

Candidates shall clearly specify any pricing assumptions and indicate whether alternative pricing models are proposed.
The Proposal shall include a clear explanation of the proposed commercial model and invoicing assumptions.

### *4.3 Relevant experience and references*

The Proposal shall include to the extent possible and without breaching confidentiality:

- description of comparable assignments performed during the last five (5) years, including experience relating to organisations operating in sensitive, regulated and/or security-driven environments;
- CVs of the key individuals proposed for the mission, including their role, seniority, certifications, expertise and relevant experience (e.g. cybersecurity, SOC, SIEM, cloud, infrastructure, compliance);
- description of the proposed governance and project team.

### *4.4 Diversity and gender balance*

- Meaningful steps toward achieving, maintaining, and promoting diversity & gender balance in the staffing of project teams.

### *4.5 CSR profile*

- The way social, environmental and governance criteria are integrated into the candidate's operations, in particular measures taken in relation to the following topics: (a) employee well-being, (b) the environment, and (c) ethics. Providing a carbon footprint disclosure will be considered an advantage.
- Broader sustainability, ethical or social responsibility initiatives implemented by the candidate.

### *4.6 Information to be included in and/or documents to be attached to the Proposal*

- A representation confirming that to its best knowledge, the candidate has no conflict of interests preventing it from submitting the Proposal;
- A representation confirming that appropriate technical and organizational cybersecurity measures, in accordance with applicable standards and legislation (including, without limitation, the GDPR and the NIS II Directive) are implemented and maintained, to ensure the confidentiality and security of all data and information exchanged with SFPIM, if possible certified by an accredited assessment body or independent auditor;
- If possible, security data compliance certification from an accredited assessment body or independent auditor;
- Any information in the Proposal that is confidential and/or relates to technical or commercial secrets and may therefore not be disclosed by SFPIM;
- If possible, carbon footprint disclosure;
- Evidence of compliance with fiscal and social obligations (Tax and social security obligations clearance certificates);
- Evidence of absence of conviction (Criminal record extract);
- Identification of any subcontractors or third-party providers involved in the services;
- Any other information deemed useful for the purposes of entering into an Agreement.

## 5. Binding period

Each candidate submitting a Proposal shall remain bound by the terms of its Proposal for a minimum period of ninety (90) days starting from the first business day following the submission deadline.

## 6. Language of the Proposal

The Proposal and the documents that are required to be attached to it must be drafted in French, Dutch or English. They may be drafted in part of one of these languages, and in part in another of these languages.

## 7. Terms of the Agreement

a. Subject of the Agreement

The selected candidate shall enter into an agreement with SFPIM relating to the provision of services described in this RfP.
The agreement shall cover the assessment and design of SFPIM's IT and cybersecurity architecture, the implementation of a SIEM solution and the provision of SOC services.

b. Term

The architecture assessment, architecture design and SIEM implementation shall constitute a one-off project.

Unless terminated early under clause c below, the Agreement for SOC services is concluded for an initial period of 3 years from its effective date (as specified in the Acceptance Letter), provided that the Agreement will be tacitly renewed for an additional 1-year period, unless terminated by either party to the Agreement by written notice to the other party at least 3 months prior to the expiry of the initial 3-year period.

Upon completion or termination of the mission, the provider shall ensure an orderly handover of all documentation, configurations, deliverables and information reasonably required by SFPIM.

c. Annual review of performance

For recurring SOC services, SFPIM reserves the right to periodically review the quality and performance of the services against the agreed service levels, reporting obligations and contractual requirements.
Where appropriate, SFPIM may request review meetings with the provider to assess performance, discuss incidents, remediation actions and service improvements.

In the event of material or repeated performance deficiencies that remain unresolved following reasonable remediation efforts, SFPIM reserves the right to terminate the Agreement in accordance with its terms.

d. Fees and annual indexation

Fees shall be those accepted by SFPIM as part of the Proposal and reflected in the Agreement.
Candidates shall clearly distinguish project-related fees and recurring service fees.
Any proposed fee revision mechanism, where applicable, shall be clearly disclosed and justified in the Proposal.

e. Invoicing and payment modalities

The candidate shall send its invoices electronically via Peppol to SFPIM and its subsidiaries, in accordance with the Belgian e-invoicing requirements.

Instructions for Peppol invoicing:

- PDF copies of invoices must not be sent separately by email, but included as an attachment in the XML Peppol file.
- After the start of Peppol invoicing, no invoices may be sent via other channels.
- Supporting annexes that cannot be included in the Peppol XML must be sent by email to accounting@sfpim.be.

All invoices must include at least a detailed description of the services provided.

The fees charged must be as set forth in accordance with the Agreement, unless otherwise agreed in writing between the parties.

Only services that have been duly performed and approved by SFPIM may be invoiced.

Payment shall be made by SFPIM within fifty (50) calendar days from the date of receipt of a duly issued invoice.

In the event of a dispute, SFPIM shall not be required to pay the disputed amounts until the dispute has been resolved. In the event of a dispute concerning a payment, the company shall continue to provide its services without interruption.

All invoices must be denominated in EUR.

f. Intellectual property

Any intellectual property rights generated in connection with the performance of the Agreement shall become and remain the exclusive property of SFPIM.

g. Confidentiality

Without prejudice to the legal obligation to observe professional secrecy, the candidate undertakes to ensure the strict confidentiality of any information communicated by SFPIM for the purposes of the (performance of) the Agreement, any such information being the property of SFPIM, and in particular:

- not to disclose it or otherwise make it accessible, in whole or in part, to any third party without the prior written consent of SFPIM;
- not to use it for its own purposes or for purposes other than those covered by the Agreement;
- to immediately notify SFPIM in the event of any misuse or unauthorised disclosure of such information.

SFPIM reserves the right to require the conclusion of a separate confidentiality agreement in connection with the opening of any specific file.

h. Cybersecurity

At any time, the candidate must be able, upon request, to demonstrate the existence of appropriate policies, procedures and safeguards in place to prevent, detect, and respond to cyber threats and data breaches, in accordance with applicable standards and legislation (including, without limitation, the GDPR and the NIS II Directive).

SFPIM reserves the right to audit or request evidence of such measures throughout the duration of a contract.

i. Insurance

The professional liability of the candidate must be covered throughout the term of the Agreement by an insurance policy taken out with a reputable insurance company.

j. Social responsibility

SFPIM believes that taking social, environmental, and governance issues into account contributes significantly to economic progress and long-term value creation. SFPIM expects its partners and suppliers to demonstrate impeccable ethics and to comply with the highest social, environmental, and governance standards. It encourages them to work in conditions that combine economic interest and corporate social responsibility.

k. Diversity and inclusion

SFPIM expects its partners and external advisors to be strongly committed to an inclusive and respectful work environment, free from any form of discrimination or harassment.
The candidate undertakes to promote workplace diversity at all levels of its organisation and a balanced representation of men and women.

l. General terms and conditions

The candidate's general terms and conditions (if applicable) shall only apply to the services provided under the Agreement on a subsidiary basis, provided that no contrary provision exists in the Agreement and that they have been explicitly submitted for approval and accepted by SFPIM.

m. Applicable law and competent courts

The Agreement shall be governed by Belgian law. In the event of a dispute between the parties concerning the validity, interpretation, performance, or termination of the Agreement, the parties undertake to negotiate in good faith in order to settle their dispute amicably. If no amicable settlement can be reached, the dispute shall be brought before Belgian courts.

## 8. Criteria

### 8.1 Selection criteria

Unless otherwise agreed by SFPIM, a Proposal will only be considered by SFPIM if it complies with the requirements of this RfP and the Agreement.

### 8.2 Evaluation criteria

Proposals will be evaluated based on the following evaluation criteria:

| | |
|---|---|
| • Pricing: competitive and transparent fee structures | 15 points |
| • Technical Architecture Quality | 15 points |
| • SIEM Solution Quality and Suitability | 15 points |
| • SOC Service Quality and Maturity | 15 points |
| • Methodology and Project Approach | 15 points |
| • Experience and references | 10 points |
| • Cybersecurity maturity and compliance approach | 10 points |
| • CSR profile (including carbon footprint disclosure) | 5 points |

SFPIM may, as the case may be, invite candidates to present and/or provide additional explanations regarding their Proposal.

The scores for all evaluation criteria will be added together. SFPIM will select the candidate that has obtained the highest total scores.

On the basis of such selection, SFPIM reserves the right to enter into negotiations with the candidates whose Proposals will be deemed the most interesting. Such negotiations may involve a meeting in the offices of SFPIM.

The entering into any such negotiations does not give rise to any obligation for SFPIM to enter into a Agreement with the candidate.

## 9. Questions and Answers

Any candidate who has questions regarding this RfP may submit them in writing to the following email address: k.onderbeke@sfpim.be. To ensure fairness and transparency in the process, all questions will be anonymized, collected and answered centrally. The answers will be sent to all candidates simultaneously and will be visible to all, ensuring that everyone has access to the same information in real-time.

Candidates must take this rule into account and ensure that all their questions are submitted within the specified deadlines.

Deadline for submitting questions: 15 July 2026

Date when the answers will be sent to all candidates: 20 July 2026.

## 10. Proposal submission deadline

Please submit your complete Proposal by **31 July 2026** to:
Katrien Onderbeke
Legal Operations Officer
k.onderbeke@sfpim.be

By submitting a proposal, each candidate is deemed to have represented and warranted that it has the full right, power and authority, and has taken all action required, to enter into and perform all obligations under its proposal. Each candidate also confirms that it has no conflict of interest to assist SFPIM with respect to the mission.

## 11. Confidentiality

By responding to this RfP, you agree to:

- treat all RfP documentation and related information provided by SFPIM (collectively, "Information") as strictly confidential,
- not share any Information with third parties, except on a need-to-know basis, and
- use the Information solely to evaluate this RfP and prepare your response.

## 12. No contract

You further understand and agree that SFPIM reserves the right at any time (i) to reject any, or all, of the candidates' Proposals and to possibly decide not to award the contract, (ii) to invite or not any candidate to negotiate, at any time, or to interrupt negotiations with any candidate at any time.

The issuance of this RfP does not imply any obligation for SFPIM to invite the candidate to negotiate nor to enter into any Agreement with the same. No legal relationship or other obligation shall arise between any candidate and SFPIM unless and until an Agreement for the services which are the subject of this RfP has been formally executed in writing by SFPIM and the awarded candidate.

## 13. Disclaimer

While SFPIM has used reasonable efforts to ensure an accurate representation of information in this RfP, the information contained herein is indicative and provided solely as a guideline for candidates. SFPIM does not guarantee nor warrant the accuracy or comprehensiveness of the information or statements herein.
Without prejudice to the generality of the foregoing, neither SFPIM nor its personnel, directors, advisers, consultants, contractors, servants and/or agents shall have any liability or responsibility in relation to the accuracy, adequacy or completeness of such information or any statements herein. For the avoidance of doubt, candidates should not assume that any such information or statements are correct, comprehensive and accurate nor that they will remain unchanged. They should make their own analysis and an independent estimation of the information given, if possible, check the accuracy, preciseness and exhaustiveness of the information.

By participating in the RfP-process, any candidate accepts the exclusion from liability.