



REQUEST FOR PROPOSAL

BID NUMBER: ECIC05P-2026/27

CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

CLOSING DATE: 6 OCTOBER 2026

CLOSING TIME: 11H00 (SAST, OBTAINABLE BY DIALLING TELKOM ON 1026)

Address Byls Bridge Office Park, Building 9, Fourth Floor, 11 Byls Bridge Boulevard, Highveld Extension 73, Centurion, 0157, South Africa

Tel +27 (0)12 471 3800 | **Email** info@ecic.co.za | **Website** www.ecic.co.za

Directors: Ms. DP Ndlovu (Chair), Ms. LR Seroka (CEO), Mr. S Mayekiso, Ms. SK O' Mahony, Mr. BI Mkhize, Ms. PM Mthethwa, Ms. XE Daku; Mr. W van Der Spuy, *Mr. L. Govender, Mr. S Bhanisi | **Company Secretary:** Ms. N Moffatt

Company registration no: 2001/013128/30 | ECIC is a licensed non-life insurer and authorised Financial Services Provider (FSP 30656). Currently exempted in terms of FAIS Notice 78 of 2019.

*alternate to Mr. W van Der Spuy

YOUR EXPORT RISK PARTNER

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

CONTENTS

A.	INTRODUCTION TO THE REQUEST FOR PROPOSAL (RFP)	3
1.	Introduction	3
2.	Purpose	3
3.	Background	3
4.	Procurement Regulations	4
B.	TERMS OF REFERENCE	5
5.	Scope of services	5
6.	Service level agreement	7
7.	Billing structure	8
8.	Delivery address	8
9.	Bid/contract conditions	9
10.	Due diligence/site inspection	10
11.	Bid evaluation	10
12.	Evaluation Phase Two: Functional	12
13.	Phase Three: Preference point system	17
14.	Document(s) required to substantiate claims for Specific Goals	18
15.	Phase Four: Objective criteria	18
16.	Standard bidding documents	19
17.	Instructions to respondents	19
18.	Timeline of the bid process	21
19.	Bid rules	22
	ANNEXES	26
	Annexure A: Protection of personal information	26
	Annexure B: Format for fee proposal (Pricing Example)	28
	APPLICABLE STANDARD BIDDING DOCUMENTS	29
	SBD 1	29
	SBD 4	31
	SBD 6.1	35
	Checklist	41

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

A. INTRODUCTION TO THE REQUEST FOR PROPOSAL (RFP)

1. Introduction

- 1.1. The Export Credit Insurance Corporation of South Africa (SOC) Limited¹ (ECIC or Corporation) is a self-sustained state-owned entity listed under Schedule 3B of the Public Finance Management Act 1 of 1999 (as amended) and established in terms of the Export Credit and Foreign Investments Insurance Act 78 of 1957 (as amended).
- 1.2. The mandate of ECIC is to facilitate and encourage South African export trade, by underwriting export credit loans and investments outside the country, to enable South African contractors to win capital goods and services contracts in countries outside South Africa. ECIC is a registered Financial Service Provider and is regulated by the Financial Sector Conduct Authority and Prudential Authority (FSP No: 30656). Currently exempted in terms of FAIS Notice 78 of 2019.
- 1.3. ECIC operates at the following address:

Byls Bridge Office Park
Building 9, Fourth Floor
11 Byls Bridge Boulevard
Highveld Extension 73
Centurion
0157

2. Purpose

- 2.1. The purpose of this Request for Proposal (RFP) is to appoint a service provider to provide Managed Security Services, including conducting ISO27001:2022 and COBIT2019 follow-up assessments, for a period of three (3) years.

3. Background

- 3.1. The ECIC operates on a hybrid sourcing model for ICT comprising internal resources and leveraging skills and competencies through outsourced services. The outsourced services in the area of ICT Governance and Information Security are a critical strategic position to ensure the ECIC have access to specialised skills as and when a need arises for proactive and reactive support.
- 3.2. ECIC subscribes to the Corporate Governance of ICT Policy Framework, COBIT 2019 and ISO 27001 as guidelines for the implementation of ICT Governance and Information Security Management within the Corporation, which is supported by the ISO27001:2022 and COBIT2019 assessments conducted every two years to determine the capability maturity level of the Corporation.
- 3.3. The high-level summary of the current ECIC technology environment in line with the required services:
 - 3.3.1. KnowBe4.

¹ Further information on the ECIC can be found at www.ecic.co.za

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

- 3.3.2. Windows server environment (5 servers, which may grow to 7 servers).
- 3.3.3. Microsoft 365 E3.
- 3.3.4. Kaspersky EDR.
- 3.3.5. N-Able Cove backup.
- 3.3.6. 100 end users expected to grow to 120 users.
- 3.3.7. Internal Security personnel responsible for coordinating and managing the MSS provider.
- 3.4. ECIC has its own licenses for the technologies mentioned above. Only the license subscriptions specified under the scope of work must be quoted for

4. Procurement Regulations

- 4.1. This bid is subject to the Preferential Procurement Policy Framework Act No. 5 of 2000 and the Preferential Procurement Regulations, 2022, the General Conditions of Contract (GCC) and, if applicable, any other special conditions of contract. Where, however, the special conditions of contract conflict with the general conditions of contract, the special conditions of contract prevail.

B. TERMS OF REFERENCE

5. Scope of services

5.1. The successful bidder will be required to provide the following Cybersecurity Services:

5.1.1. Microsoft 365 security services

- 5.1.1.1. Monitor and conduct regular security health checks of the Microsoft 365 environment, make recommendations, and assist with the implementation of remediations.
- 5.1.1.2. Assist with the implementation of CIS Baselines on both the Microsoft environment and the hosted Windows Server environment.
- 5.1.1.3. Provide monthly reports on the security posture of the environment.

5.1.2. Endpoint security services

- 5.1.2.1. Monitor and conduct regular health checks of the endpoints based on the current Kaspersky endpoint protection solution.
- 5.1.2.2. Assist with optimising the configuration and testing of the environment, including security dashboards and reports.
- 5.1.2.3. Provide monthly reports on the security posture of the environment.

5.1.3. Cloud backup services (N-Able Cove)

- 5.1.3.1. Monitor and conduct regular health checks of cloud backups based on the N-Able Cove solution.
- 5.1.3.2. Assist with optimising the configuration and testing of the environment, including dashboards and reports.
- 5.1.3.3. Provide monthly reports on the health and performance of the backup environment.

5.1.4. Vulnerability Management

- 5.1.4.1. Provide an online tool for prompt remediation of vulnerabilities such as Tenable Nessus or equivalent. The tool must not require the ECIC to provide infrastructure such as servers. The tool must be an online tool with the capability to monitor ECIC devices on premises, at a private cloud hosting location and in various locations when users work remotely.
- 5.1.4.2. Provide monthly reports with age analysis for remediation of vulnerabilities with different classifications (Critical, High, Medium, Low, etc).

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

5.1.4.3. Provide a tool that automates vulnerability management and the Executive Age Summary reporting capabilities to reduce dependency on manual effort and human-driven reporting processes to calculate vulnerability age analysis.

5.1.5. **DMARC (Domain-based Message Authentication, Reporting and Conformance) Analyser**

5.1.5.1. Provide, configure, and support DMARC analyser for the ECIC domain (@ecic.co.za). The ECIC does not have DMARC implemented and intends to implement it to mitigate the risk of domain impersonation/spoofing and provide monthly reports.

5.1.5.2. The DMARC analyser subscription must be for three years and registered under the ECIC's account.

5.1.6. **Cybersecurity Awareness**

5.1.6.1. Provide two annual interactive cybersecurity awareness sessions, one for staff (October/November) and the other for Management (Date to be confirmed), and the sessions must be in person. The staff session is to be arranged as a Cyber Day in person.

5.1.6.2. Provide quarterly phishing simulations leading up to each of the interactive cybersecurity awareness sessions.

5.1.6.3. Assist with strategic advisory based on insights from the KnowBe4 platform and monthly reporting to ensure effective and measurable cyber-awareness training.

5.1.7. **ISO27001:2022 Assessment (Years 1 and 3 – Once Off)**

5.1.7.1. Assess the Corporation's information security controls based on the ISO27001:2022 framework.

5.1.7.2. Provide a report of the detailed findings and recommendations for improving the compliance level of the Corporation.

5.1.7.3. Assist with remediation of ISO27001 findings, which may include expert advice and/or updating and developing certain documentation such as plans, framework and policies.

5.1.8. **COBIT 2019 Assessment (Year 2 – Once Off)**

5.1.8.1. Conduct the ICT governance maturity for the Corporation based on the COBIT 2019 framework.

5.1.8.2. Provide a report of the detailed findings and recommendations for improving the maturity level of the Corporation.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

- 5.1.8.3. Assist with remediation of COBIT2019 findings, which may include expert advice and/or updating and developing certain documentation such as plans, framework and policies.

5.1.9. Skills transfer and knowledge sharing:

- 5.1.9.1. Provide skills transfer and knowledge sharing plan outlining how the ECIC ICT personnel (up to 3 personnel) will be equipped with practical skills and knowledge to perform basic support of the technology solutions provided and/or supported by the bidder as part of this tender. The skills transfer will include at least configuration and technical support-related aspects.

6. Service level agreement

- 6.1. The bidder must have adequate team capacity to provide continuous support to the ECIC. The support structure must ensure business continuity by avoiding dependency on a single resource and maintaining sufficient backup capabilities. The bidder shall provide security-related proactive and reactive support services throughout the contract period.
- 6.2. The ECIC-authorized ICT personnel (up to 3 personnel) must have access to the tools provided and supported by the bidder. The access is for pulling ad hoc reports and performing basic support functions.
- 6.3. The bidder must be able to log support calls directly with the OEM on behalf of the ECIC for all technology solutions supported and provided for under the scope of work.
- 6.4. The bidder must provide an established technical support process with an electronic helpdesk system and a defined Service Level Agreement (SLA) matrix for attending to and resolving queries. The bidder will need to align their SLA matrix with the commitment and measurement of the below matrix. to provide consistent service, support and delivery:
 - 6.4.1. Target Time to Action (TTA): The maximum allowable to acknowledge ticket and must begin active work or intervention on the query logged.
 - 6.4.2. Mean Time to Resolution/Repair (MTTR): Measures the average time it takes to resolve an incident once it's been identified.
 - 6.4.3. Severity and Priority:
 - 6.4.3.1. Severity 1: Outage or unavailability of service or functionality affecting business continuity.
 - 6.4.3.2. Severity 2: Major disruptions to a significant business service or system but isn't as devastating as a severity 1.
 - 6.4.3.3. Severity 3: Moderate effect on ECIC operations; usually affecting non-critical functionalities within core systems, however, significantly hinders business productivity.
 - 6.4.3.4. Severity 4: Represents a low-priority issue that causes minimal or no disruption to normal service.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

NOTE: A detailed SLA will be discussed and agreed on during the contractual stage.

Table 1

Severity	Target Time to action (TTA)		Mean Time to Resolution/Repair (MTTR)	
Severity	Target Time to action (TTA)	Mean Time to Resolution/Repair (MTTR)		
Severity 1 – Critical			15 min	2 hours
Severity 2 - High			30 min	4 hours
Severity 3 – Medium			1 hour	8 hours
Severity 4 – low			4 hours	24 hours

7. Billing structure

7.1. The managed services contract will be billable across two components as follows:

7.1.1. Monthly retainer:

7.1.1.1. **16 hours monthly** allocated towards weekly health checks and security posture reporting for in-scope services such as Microsoft services, endpoint security services, vulnerability management, cloud backup services, DMARC and cybersecurity awareness.

7.1.1.2. Unused hours will not be utilised beyond the contract end date.

7.1.2. Bucket of support hours:

7.1.2.1. Usable towards any of the in-scope service areas. The work may include advisory-related services, technical support and implementation.

7.1.2.2. Billable on a time and materials basis – estimated hours for each assignment must be formally communicated and/or approved by the ECIC before the work is conducted.

7.1.2.3. A total of **260 hours** per year must be quoted for.

7.1.2.4. Unused hours will not be utilised beyond the contract end date (except for the hours already committed).

8. Delivery address

8.1. The implementation and support can be provided remotely; however, where necessary, a representative of the service provider may be required to be at the ECIC office at the following address:

Byls Bridge Office Park
Building 9, Fourth Floor
11 Byls Bridge Boulevard

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

Highveld Extension 73
Centurion
0157

9. Bid/contract conditions

9.1. The following condition of contract applies to this bid:

9.1.1. **Governance compliance:**

- 9.1.1.1. The appointed bidder will be subjected to completing a Third-Party Risk Assessment to demonstrate the level of security, governance, compliance and industry standards the bidder conforms to.
- 9.1.1.2. The bidder must provide evidence and documentation when responding to the Third-Party Risk assessment.
- 9.1.1.3. The bidder must indicate which industry standards are currently being used in their organisation to manage and implement the tools and services mentioned in the scope of work.

9.1.2. **Bidder accreditations:**

- 9.1.2.1. The bidder must provide proof that they are an authorised partner of Microsoft; valid proof of partnership such as a letter or certificate or any other valid proof such as confirmation from the Microsoft partner portal must be provided. ECIC will verify the information provided on the Microsoft Partner Portal. If a bidder did not provide the information, but such information can be obtained from Microsoft Partner Portal, ECIC will use such information as if it was submitted by the identified bidder.
- 9.1.2.2. The bidder must provide proof that they are an authorised partner of the DMARC and Vulnerability tools proposed.

9.1.3. **Bidders' team capacity to conduct assessments: Security and Governance Assessments:**

- 9.1.3.1. The bidder must provide copies of Curriculum Vitae(s) and certifications of at least one resource who will conduct the assessments for ISO27001:2022 or latest and COBIT 2019 or latest. The resource(s) must be certified as an ISO27001 lead auditor/implementer and COBIT 2019 Design and Implementation with at least 3 years' experience.

9.1.4. **Contactable references**

- 9.1.4.1. The bidder must provide contactable reference letters for previous Managed Cybersecurity Services and Independent Assessments (ISO27001 and COBIT2019) projects. If only a list of references was provided for functional evaluation criteria 1.1 and 1.2. The reference letters and/or project delivery date must not be older than five years

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

from the closing date of this bid. Reference letters must be on a company letterhead.

ECIC will not appoint a bidder who fails to provide all the information required under paragraph 9.1.

- 9.2. The successful bidder must sign a confidentiality undertaking as part of the service level agreement.
- 9.3. The agreement may be terminated by the ECIC if it has reasonable grounds to do so, with not less than 90 days' prior written notice. A termination clause will form part of the agreement and may include events such as unsatisfactory performance, defining events, departure of key personnel, governance and ownership issues and reputational risks.

10. Due diligence/site inspection

- 10.1. At the ECIC's discretion, a due diligence and/or site inspection may be conducted on the identified bidder. ECIC will visit the identified bidders' premises or bidder's client (with permission from the bidder) with the objective of verifying information as contained in their respective bid documents.
- 10.2. Where applicable, the ECIC will issue criteria for the due diligence review or site inspection beforehand to the applicable bidder(s). Should it be discovered during a due diligence visit or site inspection that the information submitted by the identified bidder is inconsistent with what is on their current premises of business, ECIC reserves the right to disqualify such bidder.
- 10.3. ECIC may identify another bidder using the next highest points obtained in the evaluation phase as stipulated in paragraph 11.1.3, taking into consideration the process followed under paragraphs 10.1 and 10.2.

11. Bid evaluation

- 11.1. The proposals will be evaluated in phases as highlighted below and detailed in paragraphs 11.1.1 and 11.1.4 of this document:

11.1.1. Phase One: Compliance

Compliance with the requirements of this bid in this evaluation phase, all bidders that fail to provide the required information and documentation will be disqualified from further evaluation.

11.1.2. Phase Two: Functional evaluation

In this evaluation phase, bidders are expected to obtain a minimum of 75 out of 100 points to proceed to the next evaluation stage of the evaluation. Regardless of whether the overall minimum score of 75 is achieved, bidders must also achieve the minimum threshold as indicated in paragraph 12.4. Failure to obtain the prescribed minimum points will automatically disqualify the bid offer from proceeding to the next evaluation phase.

11.1.3. Phase Three: Preference point system

The 80/20 preference point system shall be applicable to this phase, where 80 points represent maximum obtainable points for the lowest acceptable bid and 20 points represents maximum obtainable points for Specific Goals. Points will be awarded to a bidder for attaining the Specific Goals in accordance with the table as listed in the bid documentation (refer to paragraph 13, read together with the table in **page 38 (paragraph 4.1)**).

11.1.4. Evaluation Phase Four: Objective criteria

ECIC will apply objective criteria as detailed in paragraph 15.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

12. Evaluation Phase Two: Functional

12.1. The proposal submitted by the bidder will be evaluated by the ECIC based on the following criteria and be rated as the factor score multiplied by the applicable points:

Table 2

EVALUATION CRITERIA	EVALUATION CRITERIA DESCRIPTION	DESCRIPTION OF POINTS ALLOCATION			
		DETAILS/INFORMATION	RATING		POINTS
			Factor	Sub-Points	
1. Contactable reference letters	1.1. Managed Cybersecurity Services experience: The bidder must provide contactable references (list/ letters) where the Managed Cybersecurity Services were provided. Reference letters and/or project delivery date must not be older than five years from the closing date of this bid. Reference letters must be on a company letterhead. Where a list is provided, contact details, name of the organisation where the project was delivered, project description and year the project was delivered must be included. Reference letters will be a condition of award.	1.1.1. No references provided.	0		35
		1.1.2. One contactable reference provided.	1		
		1.1.3. Two contactable references provided.	2		
		1.1.4. Three contactable references provided.	3		
		1.1.5. Four contactable references provided.	4	20	
		1.1.6. At least five contactable references provided.	5		
	1.2. ISO27001 and COBIT2019 Assessments: The bidder must provide contactable references (list/ letters) where they conducted similar assessments. Reference letters and/or project delivery date must not be older than 5 years from the closing date of this bid. Reference letters must be on a company letterhead.	1.2.1. No references provided.	0		15
		1.2.2. One contactable reference provided (Either COBIT2019 or ISO27001).	1		
		1.2.3. Two contactable references provided (1 x COBIT2019 and 1 x ISO27001).	2		
		1.2.4. Three contactable references provided (Either 2 x COBIT2019 and 1 x ISO27001 assessments or vice-versa).	3		

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

EVALUATION CRITERIA	EVALUATION CRITERIA DESCRIPTION	DESCRIPTION OF POINTS ALLOCATION			
		DETAILS/INFORMATION	RATING		POINTS
			Factor	Sub-Points	
2. Cybersecurity Managed Services proposal	Where a list is provided, contact details, name of the organisation where the project was delivered, project description and year the project was delivered must be included. Reference letters will be a condition of award	1.2.5. Four contactable references provided (A minimum of 2 x COBIT2019 and 2 x ISO27001 assessments or vice-versa).	4		
		1.2.6. At least five contactable references provided (A minimum of 3 x COBIT2019 and 2 x ISO27001 assessments or vice-versa).	5		
		2.1.1. The proposals lack some of the in-scope components, or it is not provided at all	0		15
3. Bidder's capacity team	2.1. The bidder must submit a detailed proposal outlining how they will meet each of the requirements under the scope of services and contract conditions. 3.1. Provide a CV of a project manager or equivalent role. The CV must be accompanied by at least one of the following certifications: • PMP (Project Management Professional). • Prince2. • Any other applicable project management qualification. • Project manager with at least 5 years project management experience. 3.2. Provide a CV of a technical lead/ senior engineer/consultant/architect or equivalent. The CV must provide employment history in Information Security/Cybersecurity with at least 7 years' relevant experience, including Microsoft 365 security suite. The CV must be	2.1.2. The proposal covered all in-scope components but is vague or lacks details.	1 to 3		
		2.1.3. The detailed proposal covers all in-scope components.	4 to 5		
		3.1.1. Either the CV with relevant experience or qualifications not provided.	0		35
		3.1.2. Provided copies of qualifications and the CV; however, the CV is vague with minimum requirements not clearly indicated.	1 to 3	10	
		3.1.3. CV clearly details the required experience and copies of qualifications provided.	4 to 5		
		3.2.1. CV not provided or CV provided does not meet minimum requirements or no copies of qualifications provided.	0	10	
		3.2.2. Provided copies of qualifications and the CV; however, the CV is vague, with	1 to 3		

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

EVALUATION CRITERIA	EVALUATION CRITERIA DESCRIPTION	DESCRIPTION OF POINTS ALLOCATION			POINTS
		DETAILS/INFORMATION	RATING		
			Factor	Sub-Points	
	accompanied by copies of at least two of the following certifications or equivalent: • CISSP (Certified Information Systems Security Professional). • CEH (Certified Ethical Hacker). • ISO27001 (ISO/IEC 27001). • CISA (Certified Information Systems Auditor). • CISM (Certified Information Security Manager). • CompTIA Security+. • Microsoft Security Certification. • Any other applicable information security qualification/ international certification. Proof of certification may include the certificate or transcript from an authorised certification body.	minimum requirements not clearly indicated.			
		3.2.3. CV clearly details the required experience and copies of qualifications provided.	4 to 5		
		3.3.1. A minimum of two CVs provided; or CVs provided do not meet minimum requirements or no copies of qualifications provided.	0		
		3.3.2. Provided relevant copies of qualifications and a minimum of two CVs; however, the CV is vague, with minimum requirements not clearly indicated.	1 to 3	15	
3.3.3. A minimum of two CVs clearly indicating the minimum required experience and copies of relevant qualifications provided.	4 to 5				

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

EVALUATION CRITERIA	EVALUATION CRITERIA DESCRIPTION	DESCRIPTION OF POINTS ALLOCATION			POINTS
		DETAILS/INFORMATION	RATING		
			Factor	Sub-Points	
	• CompTIA Security+. • Microsoft Security Certification. • Any other applicable information security qualification/ international certification. Proof of certification may include the certificate or transcript from an authorised certification body.				
4. Bidders' experience	4.1. Provide a detailed company profile indicating at least: • Years of experience the company has in providing cybersecurity services including managed security services. • Areas of specialisation.	4.1.1. No company profile provided or the bidder has less than 5 years in providing managed security services, or it is not possible to determine the experience from the profile.	0		15
		4.1.2. Company profile provided and the bidder has 5 to 7 years of experience in providing managed security services.	1		
		4.1.3. Company profile provided and the bidder has more than 7 to less than 10 years of experience in providing managed security services.	2 to 4		
		4.1.4. Company profile provided and the bidder has 10 or more years of experience in providing managed security services.	5		
Total					100

12.2. Total points achieved under this evaluation criteria will be rounded to the nearest two decimal places.

12.3. Bidders are expected to obtain a minimum of 75 out of 100 points to proceed to the next evaluation stage of the evaluation. Failure to obtain the prescribed minimum points will automatically disqualify the bid offer from proceeding to the next evaluation phase.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

- 12.4. Regardless of whether the overall minimum score of 75 is achieved, bidders must score the minimum threshold per evaluation criteria listed below:
- 12.4.1. 60% (3/5) for contactable references (Criteria 1.1);
 - 12.4.2. 40% (2/5) on contactable references (Criteria 1.2);
 - 12.4.3. 60% (3/5) for Cybersecurity Managed Services proposal (Criteria 2.1);
 - 12.4.4. 60% (3/5) for Bidder's team capacity (Criterion 3.2 and 3.3); and
 - 12.4.5. 40% (2/5) on Bidder's experience (Criteria 4.1).
- 12.5. Failure to obtain the prescribed minimum points required under paragraph 12.4 will automatically disqualify the bid offer from proceeding to the next evaluation phase.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

13. Phase Three: Preference point system

13.1. The formula below will be used to calculate the lowest acceptable bid price:

$$Ps = 80 \left(1 - \frac{Pt - Pmin}{Pmin} \right)$$

Where

Ps = Points scored for price of tender under consideration;

Pt = Comparative price of bid or offer under consideration; and

Pmin = Price of the lowest acceptable tender.

13.2. Depending on the bidder's level of Specific Goals, a maximum of 20 Specific Goals points may be awarded to a bidder. The points scored by a bidder for Specific Goals will be added to the points allocated for price.

13.3. The table below reflects the number of points to be allocated to a bidder for Specific Goals:

Table 3

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system)
B-BBEE Procurement Recognition Level of 135% and at least 50.1% ownership by (or combination thereof): a. Black people, or b. Black female, or c. Black Designated Group, or d. Black Voting Rights.	20
B-BBEE Procurement Recognition Level of at least 110% and at least 30% ownership by (or combination thereof): a. Black people, or b. Black female, or c. Black Designated Group, or d. Black Voting Rights.	10
B-BBEE Procurement Recognition Level of at least 110% and up to 30% ownership by (or combination thereof): a. Black people, or b. Black female, or c. Black Designated Group, or d. Black Voting Rights.	5
Any other B-BBEE Procurement Recognition Level up to 110%.	0

[BIDDERS ARE REQUIRED TO INDICATE, IN ONE BLOCK, THE NUMBER OF POINTS THEY ARE CLAIMING FOR SPECIFIC GOALS IN THE TABLE IN PAGE 38 (PARAGRAPH 4.1). IN THE EVENT WHERE A BIDDER MAKES A

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

MARK (ONE MARK), ECIC WILL CONSIDER THE CORRESPONDING POINTS TO BE THE ONE WHICH THE BIDDER IS CLAIMING FOR. WHERE A BIDDER MAKES MULTIPLE MARKS OR DOES NOT MAKE ANY MARK OR INDICATION AT ALL IN THE TABLE, THE BIDDER WILL BE ALLOCATED ZERO (0) POINTS FOR SPECIFIC GOALS, NOTWITHSTANDING EVIDENCE PROVIDED.]

- 13.4. The total points achieved under this evaluation criterion will be rounded to the nearest two decimal places.

14. Document(s) required to substantiate claims for Specific Goals

- 14.1. For this bid, bidders are requested to provide the following documents in substantiation for their claim of Specific Goals in line with the 2022 Preferential Procurement Regulations:

Table 4

Specific Goals	Document required to substantiate the Specific Goals claim
B-BBEE Procurement Recognition Level	Copy of a valid B-BBEE Certificate or Copy of a valid Sworn Affidavit

- 14.2. Any bid received from a bidder who did not provide the document requested in this paragraph 14 and do not indicate the number of Specific Goals they are claiming for in the SBD6.1 Form, **in the table on page 38 (paragraph 4.1)** shall be awarded zero points for Specific Goals (i.e. both the document required to substantiate the Specific Goals Claimed and the SBD6.1 must be submitted with the response to this bid).
- 14.3. Points for Specific Goals will be allocated as indicated in paragraph 13 of this RFP and in the SBD 6.1 Form. Bidders are required to indicate how they claim points for each preference point on the SBD6.1 Form, **in the table on page 38 (paragraph 4.1)**. In the event that a bidder does not indicate the preference points they are claiming, the bidder will be awarded zero (0) points for Specific Goals.

15. Phase Four: Objective criteria

- 15.1. In this evaluation stage, ECIC will check if the bidder has a person who meets the following criteria in awarding the bid:
- 15.1.1. The bidder has a significant shareholder or owner (or equivalent) (directly or indirectly) who is classified or can be classified as a Prominent Influential Person (PIP) in accordance with the Financial Intelligence Centre Act, 38 of 2001 (FICA).
 - 15.1.2. The bidder has a shareholder or member or owner or director (or equivalent) who has questionable integrity status.
 - 15.1.3. The bidder has a director or equivalent who is classified or can be classified as a PIP in accordance with FICA.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

- 15.2. Should it be found during this evaluation stage that the bidder who has attained the highest points under Evaluation Stage Four (Preference Point System) has persons listed in paragraphs 15.1.1 to 15.1.3, ECIC reserves the right to conduct further due diligence on the person(s). Should the outcome of further due diligence not be satisfactory to ECIC, or if such a person(s) poses an unacceptable high risk reputation and/or integrity of the person(s) be questionable, ECIC reserves the right not to award the bid to that bidder. This process may be repeated for the next bidder if so required.

16. Standard bidding documents

- 16.1. Bidders are required to complete and attach the following Standard Bidding Documents:

Table 5

DETAILS	REFERENCE NUMBER
Invitation to bid	SBD 1
Declaration of Interest	SBD 4
Preference Points Claim Form for Preferential Procurement Regulations 2022 Should a bidder not complete and sign the SBD6.1, the bidder will be allocated 0.00 points for Specific Goals.	SBD 6.1

- 16.2. ECIC will not award a bid to a bidder who has not submitted complete and signed Standard Bidding Documents, and the Standard Bidding Documents forms part of the condition of award.

17. Instructions to respondents

17.1. Correspondence

- 17.1.1. No telephonic or any other form of communication with any other ECIC member of staff other than the named individual below, relating to this RFP, will be permitted. All enquiries must be in writing only.
- 17.1.2. All questions relating to the contents of the tender (conditions, rules, terms of reference, etc.) must be forwarded in writing via email to procurement@ecic.co.za by not later than Monday, 21 September 2026. Questions received after this date will not be entertained.
- 17.1.3. All questions must reference specific paragraph numbers, where applicable.
- 17.1.4. All enquiries (received on or before the closing date for enquiries) will be consolidated, and ECIC will publish one response document on the ECIC

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

website (www.ecic.co.za) within three working days after the date indicated in paragraph 17.1.2, on or before Friday, 25 September 2026.

- 17.1.5. No requests for information shall be made to any other person or place, and in particular not to the existing provider of this service.

17.2. Submission of the proposals

- 17.2.1. Bid documents must be clearly marked for ease of reference and be submitted in PDF format on/or before the closing date and time to the following email address:

procurement@ecic.co.za

- 17.2.2. The following email submission procedures or protocols must be adhered to ensure safe and secure submission of the tender documents and supporting documents:

17.2.2.1. The tender document, including the supporting or returnable documents, should be submitted via email in PDF format.

17.2.2.2. If the PDF tender document, including the supporting or returnable documents, is less than 20 Megabytes (MB), it should be submitted as one document. If the electronic bid document is more than 20MB, the electronic tender document should be split in order to adhere to the 20MB email capacity.

17.2.2.3. Bidders are also encouraged to submit a USB detailing their tender proposals.

- 17.2.3. In the event that bidders are experiencing challenges with emailing documents, tenders can be hand-delivered at the ECIC Offices on/or before the closing date and time at:

Byls Bridge Office Park
Building 9, Fourth Floor
11 Byls Bridge Boulevard
Highveld Extension 73
Centurion
0157

- 17.2.4. **Any proposal received after the closing date and time will not be accepted.**

- 17.2.5. All proposals and all subsequent information received from respondents will not be returned. The proposals should be addressed to the Head of Procurement of ECIC.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

18. Timeline of the bid process

- 18.1. The period of validity of the tender and the withdrawal of offers, after the closing date and time, is 90 days, expiring on Monday, 04 January 2027. If there is a need to extend the bid validity period, ECIC will request, in writing, permission to extend the validity period from all bidders before the expiry of the current validity period.
- 18.2. After the due date for response from bidders on the request to extend the validity period, ECIC will assume that all bidders have agreed to the request to extend and continue evaluating all bids received at the closing date and time as received on the closing date and time. Any award will be on the quoted bid amount as indicated in the proposal as at the closing date and time of the bid. If a bidder does not agree to extend the validity period on the original terms (as at the closing date of the bid), ECIC will stop evaluating the proposal received from such bidder.
- 18.3. The project timeframes of this bid are set out below:

Table 6

STAGE	DESCRIPTION OF STAGE	ESTIMATED COMPLETION DATE (OR WORK WEEK ENDING)
1.	Advertisement of bid on the Government e-tender portal /ECIC Website	Friday, 11 September 2026
2.	Questions relating to the bid from the bidder(s)	Monday, 21 September 2026
3.	Response to the questions from the bidders	Friday, 25 September 2026
4.	Bid closing	Tuesday, 06 October 2026
5.	Compliance Evaluation	Friday, 16 October 2026
6.	Functional Evaluation	Friday, 23 October 2026
7.	Preference Points	Friday, 30 October 2026
8.	Bid Adjudication	Friday, 06 November 2026

- 18.4. All dates and times in this bid are in South African Standard Time.
- 18.5. Any time or date in this bid is subject to change at the discretion of ECIC. The establishment of a time or date in this bid does not create an obligation on the part of ECIC to take any action or create any right in any way for any bidder to demand that any action be taken on the date established. The bidder accepts that, if ECIC extends the deadline for bid submission (the Closing Date) for any reason, the requirements of this bid otherwise apply equally to the extended deadline.
- 18.6. ECIC will notify all bidders of the outcome of the bid within 30 days from the date of acceptance of bid by the identified bidder.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

19. Bid rules

19.1. Awarding a bid

19.1.1. ECIC will not award a bid to a bidder:

19.1.1.1. Who is or the bidder's director(s), trustee(s), shareholder(s), member(s), partners(s) or any person(s) having controlling interest in the bidder are restricted to conduct business with the State.

19.1.1.2. Who is in the employ of the State or has a director(s), trustee(s), shareholder(s), member(s), partners(s) or any person(s) having controlling interest in the bidder who is in the employ of the State as contemplated in the Public Administration Management Act, 11 of 2014 and is prohibited from conducting business with the State in terms of section of PAMA.

19.1.1.3. Who is in the service of the State or has a director(s), trustee(s), shareholder(s), member(s), partners(s) or any person(s) having controlling interest in the bidder and has not declared their business interest as required in the applicable SBD4 form.

19.1.1.4. Has been found to have transgressed Prevention and Combating of Corrupt Activities Act, 12 of 2004 (as amended).

19.1.1.5. Has been found to have transgressed or is transgressing the Competition Act, 89 of 1998 (as amended).

19.1.2. ECIC shall not award a bid or contract or order to a bidder whose tax affairs are not compliant, except to foreign bidders with no tax obligations in South Africa.

19.1.3. For a bidder or the bidder's director(s), trustee(s), shareholder(s), member(s), partners(s) or any person(s) having controlling interest in the bidder who have declared their business interest as required in the applicable SBD4 form, ECIC will not award a bid to a bidder who has declared their interest and:

19.1.3.1. Is prohibited from conducting business with the State; or

19.1.3.2. Does not have permission to conduct remunerative work outside their employment.

19.1.4. ECIC will verify with the relevant Organ of State to determine if paragraphs 19.1.3.1 and 19.1.3.2 are not applicable.

19.1.5. ECIC will assume that, the person contemplated in paragraph 19.1.3 is prohibited from conducting business with the State or the person does not

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

have permission to conduct remunerative work outside their employment if it does not receive any response within 21 days from such verification request to an Organ of State.

- 19.1.6. ECIC will then recommend to award the bid to the bidder who achieved the second highest preference points, and should it be established that the bidder who achieved the second highest preference points has a person contemplated in paragraph 19.1.3, ECIC will conduct verification as contemplated in paragraphs 19.1.4 and 19.1.5. This step can be performed up to the bidder who achieved the third highest preference points.

19.2. Documents/information required as a condition of award

- 19.2.1. Proof of registration: Valid registration on the National Treasury Central Supplier Database (CSD).

- 19.2.2. Completed and signed Standard Bidding Forms as follows:

Table 7

Invitation to bid (all bidders must ensure that this Form is duly completed and signed)	SBD 1
Declaration of Interest	SBD 4
Preference Points Claim Form	SBD 6.1

19.3. Sub-contracting

- 19.3.1. ECIC fully endorses the South African Government's transformation and empowerment objectives and in awarding the tender or contract, preference may be given to bidders (Generics) who are willing to subcontract not less than 30% of the contract to a company which is Black Owned, Black Women Owned, Black Youth Owned, owned by Black People with Disabilities, an EMEs and QSE. EME's and QSE's are allowed to bid without subcontracting.

- 19.3.2. If contemplating subcontracting, please note that a bidder will not be awarded points for Specific Goals if it is indicated in its Proposal that such bidder intends subcontracting more than 30% (thirty percent) of the value of the contract to an entity/entity that do not qualify for at least the same points that the bidder qualifies for, unless the intended subcontractor is a company which is Black Owned, Black Women Owned, Black Youth Owned, owned by Black People with Disabilities, an EME and QSE, with the capability to execute the subcontract.

- 19.3.3. A person awarded a contract may not subcontract more than 25% (twenty five) of the value of the contract to any other enterprise that does not have

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

an equal or higher Specific Goals than the person concerned, unless the contract is subcontracted to an EME that has the capability and ability to execute the subcontract.

19.4. ECIC's rights

19.4.1. ECIC reserves the right to:

- 19.4.1.1. Amend any bid conditions, bid validity period, bid specifications, or extend the bid closing date, all before the bid closing date. Such amendments will be posted on the ECIC's website under the relevant tender information. All prospective bidders must therefore ensure that they visit the website of ECIC (www.ecic.co.za) regularly before they submit their bid response to ensure that they are kept updated on any amendments in this regard.
- 19.4.1.2. Cancel or withdraw this bid at any time, as a whole or in part without reasons and without attracting any liability.
- 19.4.1.3. Award this bid to more than one bidder.
- 19.4.1.4. Award this bid in total or part.
- 19.4.1.5. Negotiate with all or some of the shortlisted bidders.
- 19.4.1.6. Not accept the lowest priced bid or award the bid to a bidder other than the highest scoring bidder.
- 19.4.1.7. Conduct site visits at bidder's offices and / or at client sites if so required.
- 19.4.1.8. Request any relevant information and/ or documents to verify or clarify information supplied in the bid response in relation, but not limited to the structure of the bidding entity, bidder's capacity, proposed solution, proposed timelines etc.

19.5. Contract fees

- 19.5.1. Where a bidder indicates that its prices are subject to confirmation, or are in any way conditional, such pricing will not be considered.

19.6. Confidentiality

- 19.6.1. Any information relating to the submissions, through the process or otherwise, shall be treated in strict confidence. In submitting a response, a Service provider agrees that it shall not be entitled to any information disclosed by another respondent to ECIC, which ECIC has determined to

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

be of a confidential nature. The content and details of the evaluation of submissions will remain confidential to ECIC.

19.7. Other matters

19.7.1. If the ECIC does not accept any proposal, it will declare this bid process closed and may then elect to:

19.7.1.1. Proceed on a completely different basis; and/or

19.7.1.2. Not to appoint any respondent (in the event it deems all or any of the proposals not appropriate).

19.7.2. The ECIC reserves the right to engage in any processes required to validate all claims made in the proposal.

19.7.3. The ECIC has the right to enter into negotiation with a prospective Service provider regarding any terms and conditions, including fees, of a proposed contract.

19.8. Disclaimer

19.8.1. The ECIC has produced this bid in good faith. However, the ECIC, its agents and its employees and associates, do not warrant its accuracy or completeness. The ECIC will not be liable for any claim whatsoever and howsoever arising (including, without limitation, any claim in contract, negligence or otherwise) for any incorrect or misleading information contained in this bid due to any misinterpretation of this bid.

19.8.2. This bid is a request for proposals only and not an offer document; answers to it must not be construed as acceptance of an offer or imply the existence of a contract between the ECIC and the bidder.

19.9. Terms of engagement

19.9.1. The ECIC's engagement of the service provider will be documented in a contract between the ECIC and the appointed bidder.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

ANNEXES

Annexure A: Protection of personal information

1. ECIC recognises that when the Bidder submit its proposal in response to this Request for Quotations, it will provide personal information, which ECIC will process for the sole purpose of evaluating the Bidder's proposal. By submitting its proposal in responding to this Request for Quotations, the Bidder hereby provide its consent to the processing of its Personal Information by ECIC.
2. The following terms shall have the meaning ascribed to them:
 - 2.1. **"Personal Information"** shall bear the same meaning as ascribed to it under POPI;
 - 2.2. **"POPI"** means Protection of Personal Information Act, No. 4 of 2013;
 - 2.3. **"Responsible Party"** shall bear the same meaning as ascribed to it under POPI; and
 - 2.4. **"bid"** means this Request for Quotations.
3. ECIC as the Responsible Party undertakes to:
 - 3.1. comply with the provisions of POPI as well as all applicable legislation as amended or substituted from time to time;
 - 3.2. treat all Personal Information strictly as defined within the parameters of POPI;
 - 3.3. process Personal Information only in accordance with the consent it was obtained for, for the purpose agreed, as permitted by law;
 - 3.4. secure the integrity and confidentiality of any Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage, unauthorised destruction, access, use, disclosure or any other unlawful processing of Personal Information;
 - 3.5. not transfer any Personal Information to any third party in a foreign country unless such transfer complies with the relevant provisions of POPI regarding transborder information flows; and
 - 3.6. not retain any Personal Information for longer than is necessary for achieving the purpose in terms of bid or in fulfilment of any other lawful requirement.
4. ECIC will ensure that all reasonable measures are taken to:
 - 4.1. identify reasonably foreseeable internal and external risks to the Personal Information in its possession or under its control;

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

- 4.2. establish and maintain appropriate security safeguards against the identified risks;
 - 4.3. regularly verify that the security safeguards are effectively implemented;
 - 4.4. ensure that the security safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards;
 - 4.5. provide immediate notification to the Bidder if a breach in information security or any other applicable security safeguard occurs; provide immediate notification to the Bidder where there are reasonable grounds to believe that the Personal Information has been accessed or acquired by any unauthorised person;
 - 4.6. remedy any breach of a security safeguard in the shortest reasonable time and provide the Bidder with the details of the breach and, if applicable, the reasonable measures implemented to address the security safeguard breach;
 - 4.7. provide immediate notification to the Bidder where the Bidder has, or reasonably suspects that, Personal Information has been processed outside of the purpose agreed to or consented to;
 - 4.8. provide the Bidder, upon request, with all information of any nature whatsoever relating to the processing of the Personal Information for the purpose of the bid and any applicable law; and
 - 4.9. notify the Bidder, if lawful, of receipt of any request for access to Personal Information, in its possession and relating to the Bidder.
5. The Bidder has the right to inspect the Personal Information processing operations, as well as the technical and organisational information security measures employed by the ECIC to ensure compliance with the provisions of this Annexure.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

Annexure B: Format for fee proposal (Pricing Example)

This page has been left blank intentionally. Refer to the attached document titled Annexure B (Format for fee proposal (Pricing Example)).

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

APPLICABLE STANDARD BIDDING DOCUMENTS

SBD 1

PART A INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR THE REQUIREMENTS OF THE EXPORT CREDIT INSURANCE CORPORATION OF SOUTH AFRICA					
BID NUMBER:	ECIC05P-2026/27		CLOSING DATE:	6 OCTOBER 2026	CLOSING TIME: 11:00
DESCRIPTION	CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS				
BID RESPONSE DOCUMENTS MUST BE SENT TO THE FOLLOWING EMAIL ADDRESS:					
Preferably via email: procurement@ecic.co.za					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			TECHNICAL ENQUIRIES MAY BE DIRECTED TO:		
CONTACT PERSON	Lulama Makwela		CONTACT PERSON	Lulama Makwela	
E-MAIL ADDRESS	procurement@ecic.co.za		E-MAIL ADDRESS	procurement@ecic.co.za	
SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELL PHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		OR	CENTRAL SUPPLIER DATABASE No:	MAAA
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES OFFERED?	☐ Yes ☐ No [IF YES ENCLOSE PROOF]		ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES OFFERED?		☐ Yes ☐ No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]
QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS					
IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)?				☐ YES	☐ NO
DOES THE ENTITY HAVE A BRANCH IN THE RSA?				☐ YES	☐ NO
DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA?				☐ YES	☐ NO
DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA?				☐ YES	☐ NO
IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION?				☐ YES	☐ NO
IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.					

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

PART B TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:

- 1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
- 1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED– (NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**
- 1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
- 1.4. ~~THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).~~

2. TAX COMPLIANCE REQUIREMENTS

- 2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
- 2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.
- 2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE: WWW.SARS.GOV.ZA.
- 2.4 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
- 2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
- 2.6 WHERE NO TCS PIN IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.
- 2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

SIGNATURE OF BIDDER:

.....

CAPACITY UNDER WHICH THIS BID IS SIGNED:

(Proof of authority must be submitted e.g., company resolution)

.....

DATE:

.....

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

SBD 4

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

- 1.1. Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.
- 1.2. Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. BIDDER'S DECLARATION

2.1. Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest ² in the enterprise, employed by the state?	YES/NO
---	--------

- 2.1.1. If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

² the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

2.2.	Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution?	YES/NO
------	--	--------

2.2.1. If so, furnish particulars:

Full Name (Name of person employed by Export Credit Corporation of South Africa (SOC) Ltd, the procuring institution)	Relationship

2.3.	Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract?	YES/NO
------	---	--------

2.3.1. If so, furnish particulars:

Name of Related Enterprise	Registration (ID) Number

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

3. DECLARATION

I, the undersigned, in submitting the accompanying bid, do hereby make the following statements that I certify to be true and complete in every respect:

- 3.1. I have read and I understand the contents of this disclosure;
- 3.2. I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;
- 3.3. The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium³ will not be construed as collusive bidding.
- 3.4. In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.
- 3.5. The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.
- 3.6. There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.
- 3.7. I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

³ Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT.

I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

Name of declarer			
Position/Title of declarer			
Name of bidder			
Signature of declarer		Date of signature	

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

SBD 6.1

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

1 GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

1.1.1 the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and

1.1.2 the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 **To be completed by the organ of state**
(delete whichever is not applicable for this tender).

~~1.2.1 The applicable preference point system for this tender is the 90/10 preference point system.~~

1.2.2 The applicable preference point system for this tender is the 80/20 preference point system.

~~1.2.3 Either the 90/10 or 80/20 preference point system will be applicable in this tender. The lowest/ highest acceptable tender will be used to determine the accurate system once tenders are received.~~

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:

1.3.1 Price; and

1.3.2 Specific Goals.

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

1.4 To be completed by the organ of state:

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	80.00
SPECIFIC GOALS	20.00
TOTAL POINTS FOR PRICE AND SPECIFIC GOALS	100.00

- 1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for Specific Goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.
- 1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2 DEFINITIONS

- 2.1 **“tender”** means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- 2.2 **“price”** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;
- 2.3 **“rand value”** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;
- 2.4 **“tender for income-generating contracts”** means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and
- 2.5 **“the Act”** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

3 FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1 POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \\ Ps = 80 \left(1 - \frac{Pt - P_{min}}{P_{min}} \right) & \text{or} & Ps = 90 \left(1 - \frac{Pt - P_{min}}{P_{min}} \right) \end{array}$$

Where

Ps = Points scored for price of tender under consideration
Pt = Price of tender under consideration
Pmin = Price of lowest acceptable tender

~~3.2 FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT~~

~~3.2.1 POINTS AWARDED FOR PRICE~~

~~A maximum of 80 or 90 points is allocated for price on the following basis:~~

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \\ Ps = 80 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right) & \text{or} & Ps = 90 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right) \end{array}$$

~~Where~~

~~Ps = Points scored for price of tender under consideration
Pt = Price of tender under consideration
Pmax = Price of highest acceptable tender~~

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

4 POINTS AWARDED FOR SPECIFIC GOALS

- 4.1 In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for Specific Goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.

Note to tenderers: *The tenderer must indicate how they claim points for each preference point system.*

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer) (Select or tick or indicate or place a mark in one block only)
B-BBEE Procurement Recognition Level of 135% and at least 50.1% ownership by (or combination thereof): a. Black people, or b. Black female, or c. Black Designated Group, or d. Black Voting Rights.	20	
B-BBEE Procurement Recognition Level of at least 110% and at least 30% ownership by (or combination thereof): a. Black people, or b. Black female, or c. Black Designated Group, or d. Black Voting Rights.	10	
B-BBEE Procurement Recognition Level of at least 110% and up to 30% ownership by (or combination thereof): a. Black people, or b. Black female, or c. Black Designated Group, or d. Black Voting Rights.	5	
Any other B-BBEE Procurement Recognition Level up to 110%.	0	

[BIDDERS ARE REQUIRED TO INDICATE, IN ONE BLOCK, THE NUMBER OF POINTS THEY ARE CLAIMING FOR SPECIFIC GOALS IN THE TABLE IN PAGE Error! Bookmark not defined. (PARAGRAPH 4.1). IN THE EVENT WHERE A BIDDER MAKES A MARK

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

(ONE MARK), ECIC WILL CONSIDER THE CORRESPONDING POINTS TO BE THE ONE WHICH THE BIDDER IS CLAIMING FOR. WHERE A BIDDER MAKES MULTIPLE MARKS OR DOES NOT MAKE ANY MARK OR INDICATION AT ALL IN THE TABLE, THE BIDDER WILL BE ALLOCATED ZERO (0) POINTS FOR SPECIFIC GOALS, NOTWITHSTANDING EVIDENCE PROVIDED.]

4.2 In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—

4.2.1 an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or

4.2.2 any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

DECLARATION WITH REGARD TO COMPANY/FIRM

NAME OF COMPANY/FIRM			
COMPANY REGISTRATION NUMBER (ID NUMBER)			
TYPE OF COMPANY/ FIRM [TICK APPLICABLE BOX]			
Partnership/Joint Venture / Consortium	☐	Personal Liability Company	☐
One-person business/sole proprietor	☐	(Pty) Limited	☐
Close corporation	☐	Non-Profit Company	☐
Public Company	☐	State Owned Company	☐

4.3 I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

4.4 The information furnished is true and correct;

4.4.1 The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;

4.4.2 In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

proof to the satisfaction of the organ of state that the claims are correct;

4.4.3 If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –

4.4.3.1 disqualify the person from the tendering process;

4.4.3.2 recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;

4.4.3.3 cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;

4.4.3.4 recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and

4.4.3.5 forward the matter for criminal prosecution, if deemed necessary.

SIGNATURE(S) OF TENDERER(S)	
NAME AND SURNAME (AUTHORISED SIGNATORY)	
SIGNATURE	
ADDRESS	
DATE OF SIGNATURE	

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

Checklist

Hereunder is a checklist to ensure that the bid document is complete in terms of administrative compliance. Please ensure that the following forms have been completed and signed and that all documents, as requested, are attached to the tender document.

ITEM	DOCUMENT REFERENCE		ACTION TO BE TAKEN	YES/NO
1.	SBD 1	Invitation to bid	Is the form duly completed and signed?	
2.	Bidder's capacity to conduct security and governance assessments		Has the bidder provided CVs and qualifications of the resources that will conduct the ISO27001 and COBIT2019 assessments?	
3.	Bidder's accreditations		Has the bidder provided proof of the Microsoft partnership and the OEM partnership for the DMARC and Vulnerability tools proposed?	
4.	Reference letters		Has the bidder provided contactable reference letters for managed cybersecurity services experience and independent assessments (ISO27001 and COBIT 2019)?	
5.	Managed Cybersecurity Services Proposal		Has the bidder provided a Managed Cybersecurity Services proposal?	
6.	Bidder's team capacity		Has the bidder provided the CVs of the technical lead, technical resources and the project manager with their qualifications?	
7.	Bidder's experience		Has the bidder provided a company profile indicating the number of years the bidder has specialised in information/ cybersecurity?	
8.	SBD 4	Declaration of Interest	Is the form duly completed and signed?	
9.	SBD 6.1	Preference Points Claim Form for Preferential Procurement Regulations 2022	Is the form duly completed, Specific Goals points claimed, and form signed? Refer to the table in page 38 (paragraph 4.1)	
10.	B-BBEE status level verification certificate or Sworn Affidavit		Is proof of B-BBEE Status level of contributor attached? Bidder must attach copy of B-BBEE Certificate or copy of Sworn Affidavit, whichever is applicable.	

REQUEST FOR PROPOSAL: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS

Terms of Reference

ITEM	DOCUMENT REFERENCE	ACTION TO BE TAKEN	YES/ NO
11.	CSD Report or MAAA Number		
12.	Tender submission (if the bidder is submitting physical information/documents).	Two (2) printed copies (one original and one copy) submitted? (if submitting physical copies)	
		One (1) electronic copy submitted?	

I, the undersigned (name) certify that the information furnished on this checklist is true and correct.

Position/Title of declarer			
Name of bidder			
Signature of declarer		Date of signature	