SOUTH AFRICAN

CIVIL AVIATION
AUTHORITY

South African Civil Aviation Authority (SACAA) Request to develop Cyber Security Strategy, framework, and Roadmap for three years.

RFP Number: RFP/CYBERSECURITYSTRATEGY/ICT/29/2023-2024

Closing Date for submission:

Monday, 19 June 2023, 11h00

1. PURPOSE

The purpose of this document is to invite experienced organisations with the necessary expertise and accreditation in undertaking to execute the work necessary to develop Cyber Security Strategy, framework, and Roadmap for three years.

2. BACKGROUND

The South African Civil Aviation Authority (SACAA) is an agency of the Department of Transport (DoT), established in terms of the Civil Aviation Act, 2009 (Act No.13 of 2009), which came into effect on 31 March 2010. The Civil Aviation Act provides for the establishment of a stand-alone authority, mandated with controlling, promoting, regulating, supporting, developing, enforcing, and continuously improving levels of safety and security throughout the civil aviation industry.

The SACAA's mandate is to administer civil aviation safety and security oversight in the republic of South Africa, in line with Civil Aviation Authority Act (the Act), and in accordance with the standards and recommended practices (SARP's) prescribed by the ICAO.

The above is achieved by complying with the Standards and Recommended Practices (SARPs) of the International Civil Aviation Organisation (ICAO), whilst considering the local context.

The SACAA, as prescribed by the Civil Aviation Act as well as the Public Finance Management Act (PFMA), 1999 (Act No.1 of 1999) is a Schedule 3A public entity.

3. SCOPE OF WORK

SACAA is seeking proposals/ quotations from suitable and accredited Organisations to develop Cyber Security Strategy, framework, and Roadmap for three years. Below are the high-level requirements and deliverables:

	Service Name	**Service Description**
1	Cyber Security Strategy	Review of Cyber Security Strategy in line with ICT and SACAA Strategy and development of appropriate Strategy and Information Security Architecture.
2	Framework Security Governance	Assessment of the current Information Security environment, and documentation of the governance requirements to enable the organization to set clear accountabilities and priorities to meet security governance objectives.

3	Information Security talent and capacity requirements	Assess the current Cyber Security capacity requirements to ensure that there is adequate capacity to deliver on the strategy and plan.
4	A detailed 3-year Cyber Security Roadmap.	Develop a detailed 3-year Cyber Security Roadmap in line with ICT strategy and plan.
5	Information Security Management	Review and Assessment of the current environment and document information security management policies, principles, standards, and architecture.

3.1 Cyber Security Strategy

Define an Cyber Security “AS-IS” state.

a) Assess the current environment and document the ‘AS-IS’ Cyber Security landscape and architecture, including identifying the gaps and enhancements.

b) Review and document all the current technologies or solutions in the environment.

c) Assessment of existing technologies to determine if they are adequate to support current ISM requirements. Document the finding and recommendations for consideration when defining the TO-BE state.

3.2 Revise and Update Cyber Security Strategy

Revise and update the current Cyber Security strategy to ensure alignment with the SACAA ICT Strategy. Define and document the “TO-BE” state of Cyber Security and Architecture based on global best practices.

a) Document the TO-BE state of the Information Security Management.

b) Review the technologies implemented to determine their suitability in addressing both current and future business requirements.

c) Document the best practice, solutions as well as implementation priority based on the proposed roadmap and SACAA organizational objectives.

d) Document the technical specification, functional specifications, and estimated cost per solution based on the benchmarked data.

3.3 Conduct a Gap Analysis

Conduct a gap analysis, document, and define what cyber security interventions will be required.

3.4 Security Governance Framework

a) Assess the current Information Security environment to document the governance requirements to enable organization leadership to set clear accountabilities and priorities to meet security governance objectives.

b) Assess the current SACAA Information Security Governance (Policy, Procedure, Processes, Methodology etc.).

c) Recommend the best practice Information Security Governance program.

d) Policies: Recommend the policy management process that must incorporate the development, approval, awareness, acknowledgment by business users, compliance verification, and exception management. Align Cyber Security policy with enterprise security policy.

e) Principles: Define governance principles required to drive the Cyber security strategy.

f) Standards: Review and recommend security standards required to drive the Cyber security strategy such as ISO.

g) Architecture: Recommend an IS architecture that must be part of the ICT methodology, development process and technology acquisitions, to ensure its adherence to security, policy, principles, and standards.

3.5 Information Security talent and capacity requirements

Assess the current Cyber Security capacity requirements to ensure that there is adequate capacity to deliver on the strategy and plan.

a) Assess the current Cyber Security staff capabilities (Skills and competency, and experience).

b) Recommend the fit-for-purpose IS structure that will deliver on the proposed strategy and roadmap.

3.6 A detailed 3-year Cyber Security Roadmap.

Develop a detailed 3-year Cyber Security Roadmap in line with ICT strategy and plan.

4. EVALUATION CRITERIA

Bidders will be evaluated in accordance with the Supply Chain Management Policies as well as the Preferential Procurement Policy Framework, 2000 (Act No. 5 of 2000) and the Preferential Procurement Regulations of 2022. The evaluation criteria will consist of the following three (3) phases:

4.1 PHASE 1 – MANDATORY REQUIREMENTS (NON-COMPLIANCE LEADS TO AUTOMATIC DISQUALIFICATION HOWEVER SACAA RESERVE THE RIGHT TO REQUEST ADDITIONAL INFORMATION).

Submission of Minimum Standards and Mandatory documents listed below:
This phase of evaluation does not carry any weight, however, bidders who do not meet all the requirements below will be immediately disqualified from the bidding process.

Document	Comments	Compulsory requirement
Proof of registration on the Central Supplier Database (CSD) of National Treasury	Prospective bidders must be registered on the Central Supplier Database (CSD) prior to submitting bids. **Please supply the MAAA supplier number.**	Yes
SBD 4 (Bidders Disclosure)	Completed and signed	Yes

4.2 PHASE 2 – TECHNICAL AND/ OR FUNCTIONALITY EVALUATION

1.1.1 The following table is critical to the evaluators and will be a benchmark against your submission as per section 5 (1) of the Preferential Procurement Policy framework, Act 2000: Preferential Procurement Regulations, 2017.

Table 1: Functionality Evaluation

FUNCTIONALITY EVALUATION: Functionality Description			
Technical Requirements:	**Description**	**Min**	**Max**
Company Track Record and Experience	The service provider must possess a minimum of 5 years of experience in developing Cyber Security Strategy ▪ Less than 5 years (0 Points) ▪ 5 years (20 Points) ▪ 6 – 10 years (25 Points) ▪ More than 10 years (30 Points) Please attach a **Company profile** indicating the organisations' experience relating to Cyber security strategy development.	20	30
Contactable references	Provide signed reference letters **(that are not older than five years)** of previous similar work conducted in the private sector and/ or public service (attach reference letters) ▪ Less than 3 reference letters (0 points) ▪ 3 Reference letters. (20 points) ▪ 4-5 references letters (25 points) ▪ More than 5 Reference letters (30 points)	20	30
Demonstrate capacity, Qualifications and technical skills available to execute the project.	A highly competent, experienced, and skilled team with a proven track record in the following **(Attach Detailed CV's)** ▪ Cyber Security of competitive organisations and/ or ▪ The ability to develop Cyber Security Strategies and assist organisations to ensure they strengthen their Cyber Security systems. The proposed team must be in possession of the relevant qualifications in Cyber Security 2 x Personnel CVs including Cyber Security-related qualifications (2 x CV's – 40 points) Description of experience related to IT security and Cyber Security Strategy services.	40	40
Total Points		**80**	**100**

Bidders who scores minimum of 80 points on functionality evaluation will be considered further for phase 3 which is Price and SPECIFIC GOAL (B-BBEE).

4.3 PHASE 3 – SPECIFIC GOAL (B-BBEE) AND PRICE EVALUATIONS

Proposal will be evaluated in accordance with the 80/20 preference point system only on Price and SPECIFIC GOAL (B-BBEE) as follows:

4.3.1 The following PPPFA formula is used to evaluate price:

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

Ps = Points scored for price of the bid under consideration.
Pt = Rand value of bid under consideration.
Pmin = Rand value of lowest acceptable bid.

4.3.2 Only bidders that have achieved the minimum qualifying points on functionality will be evaluated further in accordance with the 80/20 preference point system as follows:

Price & SPECIFIC GOAL (B-BBEE)	SCORE
Price	**80**
SPECIFIC GOAL (B-BBEE)	**20**
TOTAL	**100**

4.3.3 In terms of the Preferential Procurement Regulations 2022, points will be awarded for specific goal in accordance with the table below:

SPECIFIC GOALS (B-BBEE Status Level of Contributor)	Number of points
1	20
2	18
3	14
4	12
5	5
6	6
7	4
8	2
Non-Compliant contributor	0

4.3.4 A contract will be awarded to a bidder who scores the highest number of points on Price and SPECIFIC GOAL (B-BBEE).

5. SUBMISSION OF BID DOCUMENT

All bids submission should be hand delivered to the Tender Box, Building 16, Treur Close, Waterfall Office Park, Bekker Street, Midrand, for attention Ms Zodwa Duma with the bid reference number as indicated above.

For any enquiries you may direct them to duman@caa.co.za

NB: Due Date for submission is Monday, 19 June 2023, 11h00.