

REQUEST FOR PROPOSALS

Reference Number:

Issued date:

Request for Proposals (RfP): Establishment of the Situational Awareness and Coordination Centre (SACC) – Phase 1

Ministry of Homeland Security, Labour & Technology

Malé, Republic of Maldives

CONTENTS

1. Background and Objectives
2. Instructions to Bidders
3. Terms of Reference
4. Bid Evaluation Methodology
5. Standard Proposal Forms & Compliance Sheets

1. BACKGROUND AND OBJECTIVES

1.1 Introduction

The Ministry of Homeland Security, Labour & Technology (hereinafter referred to as the “Ministry”) is establishing a Situational Awareness and Joint Assessments Centre (SACC) to provide a centralised national platform for situational awareness, operational monitoring, inter-agency coordination, decision support, crisis management and strategic oversight.

The SACC will integrate information from relevant agencies to support homeland security, public safety, border management, corrections, cyber security, migration management, rehabilitation and other related operational functions. Given the sensitivity of the information processed, the SACC must be delivered as a secure and sovereign capability, hosted within government-controlled infrastructure and protected by strong cybersecurity and access controls.

To achieve this, the Ministry intends to engage a qualified contractor to design, supply, install, configure, test, commission, train and operationalise Phase 1 of the SACC, comprising the following three (3) integrated components:

- **Component 1** – Hosting Infrastructure & Hyper-Converged Infrastructure (HCI) Platform
- **Component 2** – Cybersecurity Hardening & Access Control
- **Component 3** – Data Ingestion, Analytics, Dashboards & Visualisation

These components shall be delivered as a single, fully integrated solution under one Contract awarded to a single Contractor.

1.2 Primary Objectives

The main objectives of this RFP are to:

- a) Establish a secure and sovereign national monitoring platform hosted within government-controlled infrastructure.
- b) Strengthen strategic decision-making through real-time information and situational awareness.
- c) Improve crisis management and emergency coordination across the homeland security domain.
- d) Enhance national security coordination and information sharing between participating agencies.
- e) Improve operational oversight of participating agencies and support resource allocation and operational readiness.
- f) Enable performance monitoring and reporting and establish early warning and predictive analytics capabilities.
- g) Improve public accountability and institutional efficiency, while ensuring that all data remains the property of the Government of Maldives and is stored within the Maldives.

- h) Deliver a Phase 1 foundation built on open standards (no proprietary lock-in) that supports future phases, additional agencies and expanded analytics.

2. INSTRUCTIONS TO BIDDERS

2.1 General Information

2.1.1 Project

- a) Design, supply, installation, configuration, testing, commissioning, training and operationalisation of Phase 1 of the SACC for The Ministry, covering Components 1–3 as defined in Section 3.

2.1.2 Proposal

- a) Prospective Bidders are invited to submit proposals for this Contract. The Proposal submitted by the Bidder will form the basis for contract negotiations and, ultimately, the signed Contract with the selected Bidder.
- b) Bidders shall familiarise themselves with local conditions and Government infrastructure constraints and take them into account when preparing their proposals.
- c) The Ministry is not bound to accept any proposal and reserves the right to annul the selection process at any time prior to contract award, without thereby incurring any liability to any Bidder.
- d) Each Bidder may submit only one proposal as a single entity. No company shall participate in more than one bid. Where a proposal contains alternative technical solutions, such alternatives shall be clearly indicated.
- e) Bidders shall submit a complete proposal covering all four (4) Components. Partial bids that do not cover all Components will be rejected as non-responsive. Evaluation of eligibility, technical and financial scores will be based on the combined proposal covering all Components.

2.1.3 Eligibility of Bidders

- a) This bidding process is open only to Bidders registered in accordance with the requirements stated in this RfP and the Bid Data Sheet.
- b) The Bidder shall be a company registered to operate in the Maldives in accordance with applicable Maldivian laws and regulations.
- c) The proposal shall include the following valid documents for the Bidder: (i) Company Registration Certificate; (ii) SME Registration Certificate; and (iii) MIRA Tax Clearance Certificate.

- d) The Bidder shall submit a valid Manufacturer Authorisation Letter (MAL) from the manufacturer of the proposed Hyper-Converged Infrastructure (HCI), authorising the Bidder to supply, implement and support the HCI platform for this project. This is mandatory; bids without a valid HCI MAL will be considered non-responsive.
- e) All proposed solutions and implementation work must be delivered and carried out by the Bidder using its own internal resources. No component of the work may be subcontracted. This requirement reflects the sensitive, security-classified nature of the SACC and the Ministry's data security and NDA obligations.
- f) The Bidder shall demonstrate a minimum average annual turnover of five million Maldivian Rufiyaa (MVR 5,000,000) over the past three (3) years, supported by audited financial statements.
- g) The Ministry may request evidence to verify full-time employment of proposed staff (salary slips, payroll records, employment contracts) and may require security vetting of personnel who will access SACC systems or data. Failure to comply may result in rejection or termination.

2.1.4 Team & Experience Requirements

- a) All personnel assigned to the Contract must be full-time employees of the Bidder and security vetted. Independent contractors, freelancers and third-party staff are not permitted for data-touching or security roles.
- b) The Bidder shall provide at least four (4) locally based, full-time employed engineers available to provide support and maintenance for the solution. Evidence of full-time employment shall be provided.
- c) As this is a systems-integration project (involving data ingestion, system integration, analytics and dashboard development), the Bidder shall have in-house software development capability, comprising at least two (2) full-time, in-house software developers/engineers. The firm shall demonstrate relevant, hands-on experience in the types of work required under Component 4, including the development of analytics and dashboard integrations, the design and engineering of data ingestion pipelines (covering both automated/API-based integration and structured manual data submission), and the integration of data from multiple source systems. Such experience shall be evidenced through the developers' CVs and supported by reference to relevant projects they have worked on. This development work may not be subcontracted, and CVs of the proposed software developers shall be submitted.
- d) The Bidder shall demonstrate proven experience in establishing, running and/or maintaining a Security Operations Centre (SOC) and/or

Network Operations Centre (NOC), supported by evidence such as reference letters, completion certificates or a description of the engagement.

e) A valid Police Clearance Certificate shall be submitted for every individual whose CV is included in the proposal.

f) The Bidder shall submit client references demonstrating proven experience across all of the following domains, with at least one (1) reference for each (detailed in Section 5.6):

- i. Hyper-Converged Infrastructure (HCI) deployment;
- ii. Software platform with analytics / dashboards;
- iii. Cyber security implementation;
- iv. Consultancy for a similar project (e.g. operations / command / coordination centre);
- v. Security / Network Operations Centre (SOC / NOC).

References should preferably be from organisations of a nature similar to those listed in the monitoring and reporting requirements (Annex A), for example government, security, law-enforcement or border-management entities, so as to demonstrate the Bidder's understanding of the operational context in which the SACC will operate. Each reference shall include verifiable contact details (name, designation, email/phone).

2.1.5 Fraud and Corruption

a) Bidders must maintain the highest ethical standards during the procurement and execution of the Contract.

b) The Ministry will reject a proposal or terminate a contract if the Bidder is found to have engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices.

2.2 Bid Information Documents

2.2.1 Contents of Bidding Documents

a) The Bidding Documents comprise:

- Section 1: Background and Objectives
- Section 2: Instructions to Bidders
- Section 3: Terms of Reference (ToR)
- Section 4: Bid Evaluation Methodology
- Section 5: Standard Proposal Forms & Compliance Sheets

b) Bidders are expected to examine all instructions, forms, terms and other information in the Bidding Documents. Failure to furnish all required information may result in rejection of the bid.

- 2.2.2 Bid Registration**
- a) The registration procedure is specified in Bid Data Sheet (Section 2.7).
 - b) Only registered Bidders will receive clarifications or amendments.

- 2.2.3 Clarification of Bidding Documents**
- a) Bidders may request clarification of any part of the Bidding Documents within the timeframe specified in the Bid Data Sheet.
 - b) All requests for clarification and the Ministry's responses will be issued in writing to all registered Bidders.

- 2.2.4 Amendment of Bidding Documents**
- a) The Ministry may amend the Bidding Documents at any time prior to the deadline for submission of bids.
 - b) Any addenda issued will form an integral part of the Bidding Documents and will be communicated in writing to all registered Bidders.
 - c) The Ministry may extend the bid submission deadline, if necessary, to allow Bidders a reasonable time to incorporate amendments.

- 2.2.5 Confidentiality of Bid Information**
- a) All documents and information supplied by the Ministry to Bidders in connection with this RfP are to be treated as confidential.
 - b) The Bidder shall not disclose such information to third parties or use it for purposes other than preparation of the proposal, without the Ministry's prior written consent.

2.3 Preparation of Bids

- 2.3.1 Language**
- a) The proposal shall be in English. Documents in any other language shall be accompanied by an English translation.

- 2.3.2 Documents Comprising the Bid**
- a) Bidders shall submit bid documents using the forms and formats provided in Section 5.
 - b) Proposals should preferably be typewritten or computer generated. Hand-written alterations, corrections or overwriting may result in rejection.
 - c) Bids shall include all documents listed in the Submission Checklist (Section 5.9).

2.3.3 Bid Price

- a) The bid price shall be quoted in the Bid Submission Form (Section 5.1) and must match the total price stated in the Financial Proposal (Section 5.4).
- b) Prices shall be firm and not subject to escalation during the bid validity or Contract period, except where explicitly allowed under the Contract.
- c) Prices shall include all applicable taxes and fees and represent the complete financial obligation of the Ministry.
- d) All prices shall be quoted in Maldivian Rufiyaa (MVR).
- e) Pricing shall cover all hardware, software, licences, subscriptions, implementation, training and the warranty/support period specified in the Bid Data Sheet.

2.3.4 Bid Validity Period

- a) Bids shall remain valid for a minimum period of one hundred and twenty (120) days after the deadline for bid submission, or as otherwise stated in the Bid Data Sheet.

2.4 Submission of Bids

2.4.1 Submission

- a) The method, address, and deadlines for submission (including any phased/electronic and hardcopy submissions) are specified in the Bid Data Sheet (Section 2.7).

2.4.2 Late Bids

- a) Any bid received by the Ministry after the deadline for submission prescribed in the Bid Data Sheet will be rejected and returned unopened.

2.5 Bid Evaluation

2.5.1 Clarification of Bids

- a) During evaluation, the Ministry may request clarification from Bidders.
- b) Requests and responses shall be in writing, and no change in the bid price or substantial change in the technical content shall be permitted.

2.5.2 Preliminary Examination of Bids

- a) The Ministry will examine the bids to determine whether they are complete, properly signed, and substantially responsive.
- b) The Ministry may correct purely arithmetical errors. If the Bidder does not accept the correction, its bid will be rejected.
- c) The Ministry may waive minor nonconformities, provided such waiver does not prejudice or affect the ranking of any Bidder.

d) Bids that do not provide a complete proposal and pricing for all three (3) Components shall be rejected and will not proceed to Technical Evaluation.

2.5.3 Evaluation and Comparison of Bids

- a) The Ministry shall evaluate and compare substantially responsive bids in accordance with Section 4 – Bid Evaluation Methodology.
- b) The Ministry is not required to accept the lowest-priced bid and may consider overall value and quality.

2.5.4 Contacting the Ministry

- a) Bidders shall not contact the Ministry on matters relating to their bid during the evaluation process, except in response to the Ministry's requests for clarification.
- b) Any attempt by a Bidder to influence the Ministry's decision may result in rejection of the bid.

2.5.5 Rejection of Bids

- a) The Ministry reserves the right to accept or reject any or all bids, and to annul the bidding process, without thereby incurring any liability to the affected Bidder(s).

2.6 Award of Contract

2.6.1 Award Criteria

- a) Subject to the stated evaluation methodology, the Ministry will award the Contract to the Bidder whose bid has been determined to be substantially responsive and achieves the highest combined Technical and Financial score, based on the combined proposal covering all Components.

2.6.2 Notification of Award

- a) Prior to expiry of the bid validity period, the Ministry shall notify the successful Bidder in writing that its bid has been accepted, subject to contract negotiations (if any).
- b) The Ministry shall promptly notify other Bidders of the outcome.

2.6.3 Negotiations and Award

- a) Negotiations may cover the Terms of Reference, timelines, methodology and special conditions.
- b) Where negotiations fail to result in an acceptable agreement, the Ministry may terminate the negotiations and invite the next ranked Bidder.

2.6.4 Signing of Contract

- a) The Ministry shall send the final Contract to the successful Bidder after notification of award.

b) The Contract shall be signed within the period specified by the Ministry.

2.7 Bid Data Sheet

(To be completed by your team before issuing the RfP)

Ref	Item	Description
2.7.1	Publication Date	[Date]
2.7.2	Registration Deadline	[Date & Time] and registration procedure.
2.7.3	Clarification Deadline	[Date & Time] and email address for queries.
2.7.4	Clarification Responses	Date by which the Ministry will issue written responses to all clarifications.
2.7.5	Bid Submission	[Date & Time, Address].
2.7.6	Bid Validity Period	[e.g. 120 days from submission deadline].
2.7.7	Warranty / Support Period	[e.g. minimum 12 months from final acceptance].
2.7.8	Delivery / Implementation Period	Forty-five (45) days from commencement.

3. TERMS OF REFERENCE (ToR)

3.1 Introduction

The Ministry invites proposals from eligible contractors to design, supply, install, configure, test, commission and operationalise Phase 1 of the SACC. The SACC will provide a centralised, secure and sovereign platform for situational awareness, operational monitoring, inter-agency coordination, decision support and crisis management across the homeland security sector.

3.2 Objectives

The selected Contractor shall:

- Establish a secure and sovereign national monitoring platform hosted within government-controlled infrastructure.
- Provide a resilient, high-availability hosting environment based on Hyper-Converged Infrastructure (HCI), with backup, recovery and monitoring services.
- Implement cybersecurity hardening, layered access controls and audit capabilities consistent with Government cyber security requirements.
- Design and deploy a data ingestion, analytics, dashboard and visualisation capability that consolidates information from participating agencies.
- Provide training, knowledge transfer, documentation and a fully commissioned, accepted Phase 1 platform.

- f) Ensure the solution is built on open standards (no proprietary lock-in) and is capable of future expansion to additional agencies, data sources and analytics.

3.3 Scope of Work (By Component)

Bidders shall bid for all three (3) Components. Partial bids for selected Components only are not permitted. The Components shall be delivered as a single integrated solution.

3.3.1 Component 1 – Hosting Infrastructure & Hyper-Converged Infrastructure (HCI)

3.3.1.1 Description	Supply, install, configure, test and commission the hosting and server infrastructure for the SACC, based on a Hyper-Converged Infrastructure (HCI) platform deployed within government-controlled facilities. The environment shall provide high availability, redundancy, backup, recovery and infrastructure monitoring to host the SACC analytics, dashboard, security and display workloads.
3.3.1.2 Platform & Technical Requirements	(Full detail in Compliance Sheet – Component 1. Summary) a) HCI platform (compute, storage and virtualisation) sized for the Phase 1 workloads with headroom for growth. b) High availability and resilience with no single point of failure (clustered nodes, redundant power and network). c) Integrated backup, restore and disaster-recovery capability with defined RPO/RTO. d) Centralised infrastructure monitoring, alerting and health reporting. e) Server and power (UPS/redundant power) infrastructure for the operations environment. f) Hosted entirely within government-controlled infrastructure; no data leaves the Maldives. g) Architecture based on open standards, with the ability to scale out by adding nodes with minimal downtime.
3.3.1.3 Implementation & Service Requirements	a) Detailed infrastructure and HA architecture design, submitted for Ministry approval prior to deployment. b) Installation, configuration and commissioning of the HCI cluster, backup and monitoring services. c) Configuration of high availability, failover, backup schedules and recovery procedures, with documented test results. d) As-built documentation, runbooks and administrator handover. e) All engineers assigned to Component 1 shall be full-time employees of the Bidder, in line with the Ministry’s data security and NDA requirements.

3.3.2 Component 2 – Cybersecurity Hardening & Access Control

3.3.2.1 Description	Design and implement cybersecurity hardening, access control and audit measures across the SACC environment, applying a layered security model (network, application, data and identity controls) consistent with Government cyber security requirements.
3.3.2.2 Platform & Technical Requirements	(Full detail in Compliance Sheet – Component 3. Summary) a) Security hardening of servers, hypervisor, network and applications to recognised baselines. b) Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) for all administrative and user access. c) Comprehensive audit trails and security logging for user, administrator and system activity. d) Encryption of data at rest and in transit, with appropriate key management. e) Layered controls across network, application, data and identity domains (defence in depth). f) Built on open standards with no proprietary lock-in. g) Compliance with applicable Government cybersecurity policies, privacy regulations and information classification requirements. h) Support for centralised monitoring/logging and integration with the SACC analytics platform and/or national security monitoring as directed by the Ministry.
3.3.2.3 Implementation & Service Requirements	a) Security architecture and hardening plan, submitted for The Ministry approval. b) Implementation of hardening, RBAC, MFA, logging, encryption and audit controls. c) Security testing/validation of the deployed environment, with documented results. d) Security documentation, audit framework, runbooks and handover. e) At least one (1) engineer with relevant cyber security certifications assigned to this Component. f) All staff assigned to Component 3 shall be full-time employees of the Bidder, in line with the Ministry's strict data security and NDA requirements.

3.3.3 Component 3 – Data Ingestion, Analytics, Dashboards & Visualisation

3.3.3.1 Description	Design and deploy the data ingestion, analytics, dashboard and visualisation capability of the SACC, consolidating information from participating agencies (via automated integration where available, or
----------------------------	---

	structured submission otherwise) into strategic, operational and tactical views. Detailed agency data-collection items and reporting requirements are set out in Annex A and will be finalised with the selected party.
3.3.3.2 Platform & Technical Requirements	(Full detail in Compliance Sheet – Component 4. Summary) a) Data ingestion from multiple agency sources via APIs/automated integration where available, and structured manual submission where not. b) Analytics platform supporting real-time and historical analysis, trend analysis and forecasting. c) Executive, operational and analytical dashboards tailored to senior leadership, operational managers and duty officers. d) GIS mapping and geospatial visualization, heat maps and trend analysis. e) Predictive analytics and risk indicators, automated alerts and escalation notifications. f) Historical comparison and forecasting tools; real-time operational dashboards. g) Mobile and web-based access with role-based access controls. h) Support for the reporting classifications (Public, Official Use Only, Restricted, Confidential, Secret) defined in Annex A. i) Built on open standards; scalable to additional agencies, data sources and analytics in future phases.
3.3.3.3 Implementation & Service Requirements – Component 4	a) Data model, integration and dashboard design, developed with the Ministry and aligned to Annex A. b) Implementation of ingestion pipelines, analytics, dashboards, GIS and alerting. c) Configuration of role-based views (strategic, operational, tactical) and classification handling. d) User acceptance testing of dashboards and reporting against agreed requirements. e) Analyst/operator training, documentation and handover. f) All staff assigned to Component 4 shall be full-time employees of the Bidder.

3.4 Deliverables and Tasks

Key deliverables include:

- a) Operational platform hosting infrastructure and a high-availability HCI environment.
- b) Security hardening, access control and audit framework.

- c) Data ingestion and analytics platform with executive, operational and analytical dashboards.
- d) Technical documentation and system architecture documents.
- e) Training and knowledge transfer for administrators, operators, analysts and security staff.
- f) Final acceptance and handover report.

3.5 Engagement Period & Implementation Schedule

- a) Phase 1 (server and power infrastructure, HCI platform, security hardening and analytics platform) shall be delivered and completed within forty-five (45) days from commencement.
- b) Bidders shall submit a detailed Implementation Plan and delivery schedule with milestones as part of their proposal, demonstrating how the forty-five (45) day delivery timeline will be achieved. The plan will be evaluated and scored under the Technical Evaluation (Section 4.3).
- c) A finalised implementation schedule shall be agreed with the Ministry following contract award.
- d) Warranty/support for the delivered solution shall be provided for the period specified in the Bid Data Sheet (Section 2.7).

3.6 Governance Structure

The Ministry shall establish a Project Steering Committee and a Technical Working Group. The Contractor shall designate a Project Manager as the primary point of contact. All major decisions, approvals and acceptance milestones shall be endorsed by the Ministry. The project shall support integration and coordination with agencies and departments under the Ministry.

3.7 Data Governance, Security & Staffing Requirements

- a) All data shall remain the property of the Government of Maldives and shall be stored within the Maldives.
- b) Data shall be protected through encryption, access controls, logging, monitoring and backup mechanisms. The Contractor shall maintain confidentiality and comply with applicable security standards.
- c) The successful Bidder shall sign a Non-Disclosure Agreement (NDA) with the Ministry prior to accessing any SACC systems or data, and personnel may be subject to security vetting.
- d) All personnel of the Bidder who will have access to SACC systems or data shall be full-time employees of the Bidder, bound by the Bidder's confidentiality obligations and codes of conduct. A valid Police Clearance Certificate shall be provided for every individual whose CV is submitted, and the Bidder shall maintain at least four (4) locally based, full-time engineers for support and maintenance.

- e) Outsourcing or subcontracting of any part of the services to external entities or individuals is not permitted; all work shall be delivered using the Bidder's own internal resources.
- f) The Ministry may, at its discretion, request salary slips/payroll evidence and employment documentation to verify full-time employment of proposed and deployed personnel.

3.8 Reporting Requirements

The Contractor shall submit an Inception Report; Weekly Progress Reports; Risk and Issue Logs; Testing and Acceptance Reports; Training Completion Reports; and a Final Project Completion Report.

3.9 Acceptance Criteria

Acceptance shall be based on successful installation and configuration; completion of functional and security testing; delivery of agreed dashboards and reporting capabilities; completion of training and knowledge transfer; submission of all required documentation; and formal acceptance by the Ministry.

3.10 Risk Management, Sustainability & Future Expansion

The Contractor shall identify, assess and manage implementation risks throughout the project lifecycle and maintain a risk register for review by the Ministry. The architecture shall support future phases, including expanded data integration, advanced analytics, predictive modelling, AI-assisted monitoring, additional agencies and expanded operational facilities.

4. BID EVALUATION METHODOLOGY

4.1 Overview

Proposals will be evaluated in two stages:

- a) Technical Evaluation – maximum 70 marks
- b) Financial (Price) Evaluation – maximum 30 marks

Only Bidders achieving at least 60 marks out of 70 (approximately 85% of technical marks) in the Technical Evaluation will proceed to Financial Evaluation. The Technical and Financial evaluation is conducted on the combined proposal across Components 1–3.

4.2 Compliance Evaluation

The Ministry will first verify that:

- a) All required forms and documents listed in the Submission Checklist (Section 5.9) are provided.
- b) Bid Submission Form, Bid Declaration Form, Litigation History and Financial Proposal are completed.

c) Legal and registration documents (Company Registration, SME Registration and MIRA Tax Clearance certificates) and a valid HCI Manufacturer Authorization Letter (MAL) are provided.

d) The bid includes complete technical and financial proposals for all four Components.

Bidders satisfying these requirements will be considered for Technical Evaluation.

4.3 Technical Evaluation (70 Marks)

4.3.1 Technical Passing Mark

- Maximum Technical Score: 70 marks
- Minimum passing score: 60 marks (approximately 85% of 70)
- Only Bidders scoring $\geq 60/70$ will be considered for Financial Evaluation.

The Technical Score is calculated on the combined proposal across Components 1–3, and the Bidder must demonstrate adequate compliance and capability for each Component; failure to meet the mandatory requirements of any Component may result in disqualification.

4.3.2 Technical Evaluation Matrix

Category	Sub-Criteria	Max Marks
A. Technical Requirements Coverage & Compliance	A1. Functional compliance with all Component requirements	30
	A2. Solution design, integration & alignment with ToR	5
B. Firm Experience & References	B1. Experience in similar projects (command/operations centres, SOC/NOC operation, HCI, data analytics/dashboards)	10
	B2. Client references & proof of successful delivery	5
C. Technical Team Qualifications & Experience	C1. Project Manager and infrastructure/HCI engineers	10
	C2. Cyber security engineers, in-house software developers, data/analytics engineers & overall team experience	5
D. Delivery & Implementation Plan	D1. Quality and realism of the Implementation Plan and ability to meet the 45-day delivery timeline	5
TOTAL TECHNICAL	—	70

4.4 Financial (Price) Evaluation (30 Marks)

4.4.1 Eligibility

Only Bidders that achieve a minimum Technical score of 60/70 are considered for Financial Evaluation.

4.4.2 Price Scoring

- a) Maximum Financial Score: 30 marks.
- b) The lowest evaluated price among technically qualified Bidders will receive 30 marks.
- c) Other technically qualified Bidders receive a score in proportion to their price:
 - a) $\text{Financial Score} = (\text{Lowest Evaluated Price} \div \text{Price of Bid Under Consideration}) \times 30$
 - d) The evaluated price shall be based on the grand total cost of ownership for all four (4) Components combined (including all hardware, software, licences/subscriptions, implementation, training, warranty/support and all applicable taxes).
- b) e) Bidders shall quote a single total price per Component and a single grand total price covering Components 1–3. All four Components must be priced; bids that omit any Component will be rejected.

5. STANDARD PROPOSAL FORMS & COMPLIANCE SHEETS

5.1 Bid Submission Form

[Standard cover form – Bidder name, address, contact details, Components (1–3), total price per Component, grand total, authorised signature, validity, etc.]

Bidder Name: _____

Registered Address: _____

Contact Person / Designation: _____

Email and Telephone: _____

Total Bid Price (MVR, all Components): _____

Bid Validity: _____

Authorised Signature / Date: _____

5.2 Bid Declaration Form

[Declaration about correctness of information, acceptance of RFP terms, absence of conflict of interest, willingness to sign an NDA and submit to security vetting, confirmation that all personnel are full-time employees of the Bidder, and confirmation that no part of the work will be subcontracted.]

5.3 Litigation History

[Table for disclosure of any litigation/arbitration during the last 5 years.]

#	Year	Matter / Parties	Status / Outcome
1			
2			
3			

5.4 Financial Proposal Form

Bidders shall provide an itemised cost breakdown per Component showing one-time supply/implementation costs and any recurring licence/subscription and warranty/support costs for the period specified in the Bid Data Sheet.

Bidders must submit pricing for all three (3) Components. Financial Proposals that do not include a price for any one of the Components will be considered non-responsive. All prices shall be quoted in Maldivian Rufiyaa (MVR), inclusive of all applicable taxes.

Sample Table

Component	Description	Total Price (MVR)
Component 1	Hosting Infrastructure & HCI Platform	_____
Component 2	Cyber Security Hardening & Access Control	_____
Component 3	Data Ingestion, Analytics, Dashboards & Visualization	_____
Grand Total	Components 1 + 2 + 3	_____

5.5 Company / Bidder Information

[Basic company profile, registration details, shareholding, contact person information, audited financial statements / annual turnover for the past three (3) years.]

5.6 Details of Completed/Ongoing Contracts & References

The Bidder shall provide client references demonstrating proven experience across all of the domains listed below, with at least one (1) reference for each. References should preferably be from organisations of a nature similar to those listed in **Annex A** (government, security, law-enforcement or border-management entities). Each reference shall include a reference letter or completion certificate and verifiable contact details (name, designation, email/phone).

#	Reference Domain (min. 1 each)	Project / Client	Contact (name, designation, email/phone)
1	Hyper-Converged Infrastructure (HCI) deployment		
2	Software platform with analytics / dashboards		
3	Cyber security implementation		
4	Consultancy for a similar project (operations / command / coordination centre)		

#	Reference Domain (min. 1 each)	Project / Client	Contact (name, designation, email/phone)
5	Security / Network Operations Centre (SOC / NOC)		

In addition to the above, the Bidder shall list all completed/ongoing contracts of a similar nature (project name, client, description, scale, value, duration and contact person) and shall include evidence of experience operating a SOC and/or NOC.

5.7 CVs of Key Experts

CVs and copies of certifications for: Project Manager; infrastructure/HCI engineer(s); cybersecurity engineer; data/analytics & dashboard engineer; and at least two (2) in-house, full-time software developers.

A valid Police Clearance Certificate shall be submitted together with each CV. All proposed personnel shall be full-time employees of the Bidder. The Bidder shall maintain at least four (4) locally based, full-time engineers for support and maintenance, and at least two (2) full-time, in-house software developers for the integration, analytics and dashboard development work. The CVs of the proposed software developers shall clearly evidence relevant, hands-on experience in analytics and dashboard integration, data ingestion pipeline engineering (both automated/API-based integration and structured manual data submission) and integration of data from multiple source systems, with reference to the specific projects on which such experience was gained.

5.8 Technical Proposal Format

Suggested structure:

- Executive Summary
- Proposed Architecture & Integration Across Components
- Requirement Compliance Matrix (mapping to Section 5.10)
- Implementation Plan & Delivery Schedule (45 days to go-live, with milestones)
- Staffing Plan (confirming all staff are full-time employees of the Bidder; roles for infrastructure, security, data/analytics and in-house software development)
- Data Governance, Security & Classification Approach
- Training & Knowledge Transfer Plan
- Risk Management & Mitigation

5.9 Submission Checklist

Example checklist (Bidders to tick):

- ☐ Bid Submission Form (5.1)

- ☐ Bid Declaration Form (5.2)
- ☐ Litigation History (5.3)
- ☐ Financial Proposal (5.4)
- ☐ Company / Bidder Information (5.5)
- ☐ Details of Similar Contracts (5.6) and reference letters
- ☐ References covering all five domains – HCI, Software/Analytics, Cyber Security, Consultancy, SOC/NOC (5.6)
- ☐ Evidence of SOC / NOC establishment / operation experience
- ☐ CVs of Key Experts (5.7) with Police Clearance Certificate for each CV
- ☐ CVs of at least two (2) in-house, full-time software developers, evidencing experience in analytics/dashboard integration and data ingestion pipeline engineering (5.7)
- ☐ Manufacturer Authorization Letter (MAL) for the proposed HCI infrastructure
- ☐ Implementation Plan & 45-day delivery schedule with milestones (5.8)
- ☐ Technical Proposal (5.8)
- ☐ Completed Compliance Sheets for Components 1–4 (5.10)
- ☐ Company Registration Certificate
- ☐ SME Registration Certificate
- ☐ MIRA Tax Clearance Certificate
- ☐ Audited financial statements evidencing minimum average annual turnover of MVR 5,000,000 over the past 3 years
- ☐ Evidence of full-time employment of proposed engineers (at least four locally based)

5.10 Technical Requirements Compliance Sheets (with Tick Boxes)

For each Component, complete the corresponding Compliance Sheet.

- Tick one option only per requirement (☐ Compliant / ☐ Partially Compliant / ☐ Not Compliant).
- If “Partially Compliant” or “Not Compliant” is selected, provide explanation and reference to your Technical Proposal.

5.10.1 Component 1 – Hosting Infrastructure & HCI

Bidder Name: _____

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Ref.
C1.1	Provide a Hyper-Converged Infrastructure (HCI) platform (compute, storage and virtualization) sized for the Phase 1 SACC workloads, with capacity headroom for growth.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.2	Cluster provides high availability and resilience with no single point of failure (clustered nodes, redundant power supplies and network interfaces).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.3	Integrated backup, restore and disaster-recovery capability with defined and configurable RPO/RTO.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.4	Centralised infrastructure monitoring, alerting and health reporting for compute, storage, virtualization and network.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.5	Supply of supporting server and power infrastructure (e.g. UPS / redundant power) for the operations environment.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.6	Entire environment is hosted within Government-controlled infrastructure in the Maldives; no SACC data leaves the Maldives.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.7	Architecture based on open standards (no proprietary lock-in) and able to scale out by adding nodes with minimal downtime.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.8	Provide detailed infrastructure & HA architecture design for Ministry approval prior to deployment, with documented HA/backup/recovery test results.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.9	Provide as-built documentation, runbooks and administrator handover for the HCI environment.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Ref.
C1.10	All engineers assigned to Component 1 are full-time employees of the Bidder (no outsourced resources without the Ministry's prior written consent).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C1.11	A valid Manufacturer Authorisation Letter (MAL) from the HCI manufacturer, authorising the Bidder to supply, implement and support the proposed HCI platform, is provided. (Mandatory)	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

5.10.2 Component 2 – Cyber Security Hardening & Access Control

Bidder Name: _____

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Ref.
C2.1	Apply security hardening of servers, hypervisor, network and applications to recognised baselines/standards.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.2	Provide Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) for all administrative and user access.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.3	Maintain comprehensive audit trails and security logging for user, administrator and system activity.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.4	Provide encryption of data at rest and in transit, with appropriate key management.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.5	Implement layered controls across network, application, data and identity domains (defence in depth).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.6	Solution is built on open standards with no proprietary lock-in.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.7	Comply with applicable Government cybersecurity policies, privacy regulations and information classification requirements.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.8	Support centralised monitoring / logging and integration with the SACC analytics platform and/or national security monitoring as directed by the Ministry.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.9	Provide a security architecture and hardening plan for The Ministry approval and perform security testing/ validation of the deployed environment with documented results.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Ref.
C2.10	Provide security documentation, an audit framework, runbooks and handover.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.11	Implementation team includes at least one (1) engineer with relevant cyber security certifications (e.g. CISSP, CEH, CompTIA Security+ or equivalent).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C2.12	All staff assigned to Component 3 are full-time employees of the Bidder (no outsourced resources without the Ministry's prior written consent).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

5.10.3 Component 3 – Data Ingestion, Analytics, Dashboards & Visualization

Bidder Name: _____

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Ref.
C3.1	Support data ingestion from multiple agency sources via APIs / automated integration where available, and structured manual submission where not.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.2	Provide an analytics platform supporting real-time and historical analysis, trend analysis and forecasting.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.3	Provide executive, operational and analytical dashboards tailored to senior leadership, operational managers and duty officers (strategic, operational and tactical views).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.4	Provide GIS mapping and geospatial visualization, heat maps and trend analysis.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.5	Provide predictive analytics and risk indicators, with automated alerts and escalation notifications.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.6	Provide historical comparison and forecasting tools and real-time operational dashboards.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.7	Provide mobile and web-based access with role-based access controls.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.8	Support the reporting classifications (Public, Official Use Only, Restricted, Confidential, Secret) defined in Annex A, with handling appropriate to each classification.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.9	Built on open standards; scalable to additional agencies, data sources and analytics in future phases.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Ref.
C3.10	Provide data model / integration / dashboard design aligned to Annex A, plus user acceptance testing of dashboards and reporting against agreed requirements.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.11	Provide analyst/operator training, documentation and handover.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.12	All staff assigned to Component 4 are full-time employees of the Bidder.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
C3.13	The Bidder has in-house software development capability (at least two (2) full-time, in-house software developers) for the integration, analytics and dashboard development; this work is not subcontracted. The proposed software developers demonstrate, through their CVs and reference to relevant projects, hands-on experience in analytics and dashboard integration, data ingestion pipeline engineering (automated/API-based and structured manual data submission) and integration of data from multiple source systems.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

ANNEX A – Data Integration & Reporting Requirements (Public Summary)

A.1 Purpose

This Annex defines, in generalised terms, the data-integration, reporting and dashboard requirements the SACC must satisfy: it consolidates information from participating agencies (by automated integration where available, or structured submission otherwise) to enable situational awareness, decision support, coordination, performance monitoring and risk assessment. The platform shall be designed against the technical envelope in A.3 and the classification model in A.4; the specific indicators, fields and sources are released as set out in A.2.

A.2 Tiered Disclosure of Operational Detail

To balance bidder information needs against the sensitivity of the data, operational detail is disclosed in three tiers:

- a) **Tier 1 – Public (this Annex).** Generalised domains, the content-neutral technical envelope (A.3) and the classification and dashboard requirements (A.4–A.5). Sufficient to prepare a responsive technical and financial proposal.
- b) **Tier 2 – Shortlisted bidders, under NDA, in a controlled data room.** Following the technical evaluation, shortlisted bidders whose nominated personnel have signed the NDA and cleared the vetting are given supervised access to a fuller data dictionary (indicator lists, source systems, frequencies and interface specifications up to and including the Restricted/Confidential tiers) for detailed design and firm pricing. Material is not removed from the data room except as the Ministry permits.
- c) **Tier 3 – Awarded Contractor only, post-award, on need-to-know.** The most sensitive (Secret-tier) specifics are finalised with the awarded Contractor during the design phase under contract, on a strict need-to-know basis. Certain specifics may be withheld from any bid document entirely and provided only after accreditation.

A.3 Technical Integration Envelope (content-neutral)

Bidders shall design and price against the following parameters. Indicative values/bands are provided so the solution can be sized; exact figures are confirmed in the Tier 2 data room. (Complete the bracketed values before issue.)

Parameter	Indicative basis for bidding
Participating agency / domain groups	Approximately [...] organisations across [...] domain groups (e.g. policing, border/customs, corrections, drug

Parameter	Indicative basis for bidding
Source systems to integrate	control, labour/migration, cyber/digital, registration/juvenile justice, ministry HQ).
	[...] distinct source systems (confirmed in the data room).
Integration patterns	A mix of automated/API integration and structured manual submission; indicative split [...]% automated / [...]% structured submission.
Update frequencies	A mix of real-time/near-real-time, daily, weekly and monthly feeds; the solution shall support all four cadences.
Data volume band	Indicative steady-state ingest in the band [low / medium / high – e.g. records per day], with capacity headroom per Section 3.
Personal / special-category data	Present (may include data relating to juveniles, migrants and rehabilitation clients). Handle strictly per the DPIA and classification model; data minimisation applies.
Classification tiers to enforce	Five: Public, Official Use Only, Restricted, Confidential, Secret (see A.4).
Dashboard / view types	Strategic, operational and tactical views; executive summaries; GIS/geospatial; heat maps; trend, predictive and forecasting views.
User roles & access	Multiple role types with RBAC and need-to-know segregation by classification tier; indicative [...] role types, [...] concurrent users.
Geospatial requirement	GIS/geospatial visualisation required.
Alerting	Automated alerts and escalation notifications.
Retention	Per the Bid Data Sheet (data) and Section 3.7.2 (audit logs).

A.4 Reporting Classification

All information shared with the SACC shall be classified as one of: Public; Official Use Only; Restricted; Confidential; Secret. Agencies shall ensure data-sharing protocols comply with national legislation, cybersecurity requirements, privacy regulations and approved inter-agency

information-sharing agreements. The SACC shall enforce handling, labelling, access segregation and audit appropriate to each classification, including segregation between tiers.

A.5 Dashboard Visualisation Requirements

The SACC dashboards shall support real-time operational views; GIS/geospatial visualisation; heat maps and trend analysis; executive summaries; predictive analytics and risk indicators; automated alerts and escalation; historical comparison and forecasting; and mobile/web access with role-based controls — providing strategic, operational and tactical views for senior leadership, operational managers and duty officers.

A.6 Classification & Distribution of the Full Annex

The full Annex A (the complete data dictionary released at Tier 2/Tier 3) is itself a classified artefact. It shall carry its own classification marking and a controlled distribution list, be released only in the data room or post-award under the conditions in A.2, and be subject to the NDA, vetting, need-to-know and audit requirements. It shall not be appended to the publicly issued RfP.