DEPARTMENT OF NATIONAL REGISTRATION
REQUEST FOR PROPOSAL

RFP 2025-02

Announcement Date

04th August 2026

Proposal Submittal Due Date

13th August 2026

(10:00)

To

Department of National Registration
Velaanaage, 4th Floor
Ameer Ahmed Magu
Male'

Statement of Requirements - Application Delivery Controller, Network-Attached Hardware Security Module, Compact Hardware Security Modules, HSM Infrastructure Penetration Test and AI-Generated and Manipulated Image Detection System.

Reference: RFP 2025-02

Date: 04th August 2026

1. Background

The Department of National Registration (hereinafter "the Department" or "DNR") intends to procure an application delivery controller (ADC) appliance, a network-attached hardware security module (HSM), compact hardware security modules, a post-deployment penetration test of the HSM infrastructure, and an on-premises AI-generated and manipulated image detection system, together with their associated manufacturer support and maintenance services.

This Statement of Requirements defines the minimum technical, commercial and service requirements for the supply, delivery, installation, configuration, integration (for Items 1 and 2) and support of the items described below. The proposed equipment must integrate natively with, and complement, the Department's existing application delivery and security infrastructure.

The successful Bidder shall provide end-to-end responsibility for the supply of all items, and for the design, implementation, integration and ongoing support of the ADC (Item 1) and the network-attached HSM (Item 2). The compact HSMs (Item 3) are supply only with manufacturer warranty. Item 4 is a post-deployment penetration test engagement. Item 5 comprises detection software developed and delivered in-house by the Bidder under a perpetual software license, together with the supply of two (2) dedicated AI compute devices on which that software is deployed. The system is deployed and integrated by the Bidder and hosted entirely within the Department's own infrastructure, with three (3) years of support. A Manufacturer's Authorization Letter is required in respect of the supplied compute appliances; no such authorization is required for the detection software, of which the Bidder shall be the owner and developer. The contract period is three (3) years.

The Bidder must be an authorized reseller or partner of the original equipment manufacturer (OEM) of the proposed ADC and network-attached HSM, and shall provide a valid Manufacturer's Authorization Letter (MAL) / Authorised Partner Letter for these product lines as detailed in Section 5. Failure to provide a valid authorization letter where required shall render the bid non-responsive.

2. Bill of Quantity

Note: Bidders must bid for the entire scope and provide fully itemized pricing for every line item in the Bill of Quantity and the Statement of Compliance. Partial bids shall not be accepted.

2.1 Indicative Bill of Materials

The following defines the products and services required. Bidders shall propose the OEM's current-generation product meeting or exceeding every mandatory specification in Section 4 and shall provide fully itemized pricing for each line.

Item 1 - Application Delivery Controller (ADC) Appliance - Purpose-built hardware appliance, 1U rackmount, with a platform-level hypervisor/operating system layer and integrated local traffic management, Global Server Load Balancing, DNS Services, and DNSSEC capabilities, including installation, configuration, integration and a 3-year manufacturer premium support contract.

Item 2 - Network-Attached Hardware Security Module (HSM) Bundle - 1U rackmount, FIPS 140-3 Level 3 validated, PED-based multi-factor authentication, minimum 5 cryptographic partitions, including dedicated hardware backup HSM, with installation, configuration, integration and 3-year manufacturer enhanced maintenance.

Item 3 - Compact Hardware Security Modules (Qty 2) - Supply-only. FIPS 140-3 Overall Level 3 validated, portable form factor, with PKCS#11 and Microsoft CNG/KSP support for certificate authority key protection and code signing.

Item 4 - HSM Infrastructure Penetration Test - Post-deployment penetration test of the deployed HSM infrastructure (Items 2 and 3), to be conducted upon notification by the Department, with a written report delivered within seven (7) calendar days of commencement.

Item 5 - AI-Generated and Manipulated Image Detection System - On-premises detection software for fully AI-generated (synthetic) imagery, face morphing and face-swap attacks, and conventional digital manipulation and retouching in facial photographs and scanned supporting documents submitted to the Department, together with the supply of two (2) dedicated AI compute devices. The detection software shall be developed and delivered in-house by the Bidder and licensed to the Department perpetually. Includes installation, configuration, integration with Department intake and issuance workflows, training, a 3-year support and detection model update contract provided by the Bidder, and 3-year hardware warranty on the supplied compute devices.

3. Scope of Work

Success Bidder shall provide supply of all items, and end-to-end responsibility for the delivery of the ADC solution (Item 1) and the network-attached HSM solution (Item 2), including design, installation, configuration, integration, knowledge transfer, documentation

and support throughout the contract period. Item 3 is supply-only with manufacturer warranty. Item 4 is a post-deployment penetration testing engagement to be conducted on notification. Item 5 is an on-premises detection platform for which the Bidder carries end-to-end responsibility for supply, deployment, integration, tuning, acceptance testing, model updates and support.

3.1 Application Delivery Controller

Supply, install, configure and integrate one (1) purpose-built Application Delivery Controller (ADC) hardware appliance with the DNS/GSLB module, redundant (1+1) AC power, SFP+ transceivers, and a 3-year manufacturer premium support contract.

- Supply one (1) ADC appliance, new, unused and sourced from an OEM-authorized channel. The appliance shall be a purpose-built hardware platform (not a general-purpose server running software only) designed specifically for application delivery. The appliance shall incorporate a platform-level hypervisor/operating system layer that runs directly on the bare-metal hardware, with the ADC traffic-management software operating as a managed tenant workload on top of this platform layer.
- Configure local load balancing, intelligent traffic management, health monitoring, SSL/TLS offload using dedicated hardware cryptographic acceleration, and high-availability services for the Department's applications.
- Configure the integrated DNS/GSLB module to deliver Global Server Load Balancing, authoritative DNS services and DNSSEC signing.
- Provide a programmable traffic manipulation engine with a scripting language that permits custom inspection, transformation, and routing of Layer 4–7 traffic flows at line rate without requiring third-party plug-ins or external orchestration.
- Integrate with the broader application delivery architecture and, where required, with the network-attached HSM (Item 2) for hardware-protected, external storage of SSL/TLS private keys, using industry-standard PKCS#11 interfaces.
- Forward logs to the Department's log management / SIEM platform via syslog, structured event format (CEF/LEEF) and/or REST API.
- Provide a 3-year manufacturer support contract (24×7) with same-business-day hardware replacement, firmware updates, and direct access to manufacturer technical support.
- Provide configuration documentation and operational handovers to Department staff.

3.2 Hardware Security Module - Network-Attached

Supply, install, configure and integrate one (1) network-attached Hardware Security Module (HSM) bundle with PED-based multi-factor / trusted-path authentication, Enterprise-class cryptographic performance, minimum 16 MB of secure key storage, minimum 5 partitions, including a dedicated hardware backup HSM, with a 3-year manufacturer Enhanced Maintenance Service.

- Supply one (1) network-attached HSM bundle, new, unused, sourced from an authorized OEM reseller/channel. The bundle shall include the primary HSM appliance, one (1)

dedicated hardware backup HSM, and all required PED authentication hardware, cabling and accessories for complete operational deployment.

- Deploy the network-attached HSM in the Department's data Centre; rack, cable, power, initialize and harden the appliance.
- Configure hardware PED (trusted-path / multi-factor) authentication using a dedicated PIN-entry device that ensures authentication credentials never traverse the host operating system or network. The PED shall provide a physically isolated, cryptographically secure channel for administrative authentication.
- Configure security officer and partition roles with segregation of duties, and M of N / quorum-based multi-person control requiring a configurable threshold of authorized administrators to perform sensitive operations.
- Create and configure the required application partitions (minimum 5 as supplied) with independent cryptographic boundaries, access controls and key material. Register client applications, including - where required - the ADC appliance (Item 1) as an HSM client for protection of SSL/TLS private keys.
- Configure secure backup and restore all key material using the bundled dedicated hardware backup HSM, ensuring keys never leave hardware protection throughout their lifecycle. Configure high-availability / load-balancing groups as required.
- Configure cryptographically secured, tamper-evident audit logging and forward HSM audit events to the Department's log management / SIEM platform, with guaranteed log integrity and non-repudiation.
- Provide a 3-year manufacturer Enhanced Maintenance Service, 24×7 with same-business-day or next-business-day hardware replacement.
- Provide configuration documentation, key-ceremony documentation and operational handover / knowledge transfer to Department staff.

3.3 Hardware Security Modules - Compact

Supply two (2) compact, portable Hardware Security Modules (HSMs) with FIPS 140-3 Overall Level 3 validation to provide a portable, low-cost hardware root of trust for use cases such as certificate authority (CA) key protection, code signing and secrets management.

- Supply two (2) compact, FIPS 140-3 Overall Level 3 validated HSM devices, new, unused, sourced from an OEM-authorized distribution channel.
- Provide all OEM documentation, including SDK/API references, configuration guides, and FIPS-mode operational procedures.

Note: Implementation, configuration and integration of the compact HSMs will be undertaken by the Department. The Bidder's responsibility under this item is limited to supply, delivery and manufacturer warranty only.

3.4 HSM Infrastructure Penetration Test

Conduct a post-deployment penetration test of the entire HSM infrastructure comprising the network-attached HSM (Item 2) and the compact HSMs (Item 3), including their integration with the ADC appliance (Item 1) where relevant. The test shall commence within five (5)

working days of written notification from the Department, and a comprehensive written report shall be delivered within seven (7) calendar days of test commencement.

- Conduct a comprehensive penetration test targeting the deployed HSM infrastructure, including but not limited to: the network-attached HSM appliance and its backup HSM, PED authentication mechanisms, partition isolation and access controls, key management and cryptographic operations, API interfaces (PKCS#11, REST), network communication channels, audit logging integrity, and the integration path between the ADC and the HSM for SSL/TLS key protection.
- Test for vulnerabilities including but not limited to: authentication bypass, authorization/privilege escalation, cryptographic implementation weaknesses, side-channel exposure, key-material extraction attempts, partition-boundary violations, network protocol attacks, API abuse, configuration weaknesses, and tamper-detection circumvention.
- The penetration test shall follow a recognized industry methodology (e.g., OWASP WSTG, PTES, NIST SP 800-115, or OSSTMM) adapted for cryptographic infrastructure assessment. Testing shall be non-destructive and shall not risk key-material loss or service unavailability. The Bidder shall coordinate with the Department on any potentially disruptive test cases before execution.
- Deliver a comprehensive written report within seven (7) calendar days of test commencement. The report should include: an executive summary, methodology description, detailed findings with CVSS 4.0 severity ratings, step-by-step reproduction evidence, root-cause analysis, risk assessment, and prioritized remediation recommendations with specific, actionable guidance.
- Provide a post-report presentation/walkthrough to Department technical staff covering all findings, exploitation paths and recommended remediation measures.

3.5 AI-Generated and Manipulated Image Detection System

Supply, install, configure and integrate one (1) AI-Generated and Manipulated Image Detection System, comprising the Bidder's detection software and two (2) dedicated AI compute devices, deployed entirely within the Department's data center. The detection software should be developed and delivered in-house by the Bidder and licensed to the Department on a perpetual basis. The item includes integration with the Department's intake and issuance workflows, training, and a 3-year support and detection model update contract provided by the Bidder.

- Supply two (2) AI computed devices meeting the specification in Section 4.5, and install, configure and commission the detection software on them within the Department's data Centre. One device shall be commissioned as the production instance and the second as the non-production instance for testing, model tuning and disaster recovery. The Bidder shall harden both devices prior to handover, including disabling all wireless interfaces, enabling self-encryption on the internal storage and configuring secure boots. The system shall operate wholly on Department-controlled infrastructure and shall remain fully functional with no connectivity to the public internet.

- Configure detection pipelines covering all four attack families specified in Section 4.5: fully synthetic (AI-generated) imagery, face morphing, face swap / deepfake substitution, and conventional digital manipulation and retouching of otherwise genuine photographs and scanned documents.
- Where required, configure digital signing of forensic analysis reports using keys held in the network-attached HSM (Item 2) via PKCS#11, so that the integrity and origin of a report can be verified independently at a later date.
- Forward all analysis events, adjudication decisions, overrides, exports and configuration changes to the Department's log management / SIEM platform via syslog (RFC 5424) and/or Common Event Format (CEF).
- Conduct a Site Acceptance Test against a blind test set supplied by the Department, comprising genuine and manipulated images representative of the Department's actual intake, and demonstrate that the system meets or exceeds the detection and false-positive rates stated in the Bidder's response.
- Deliver reviewer and administrator training, complete system and model documentation, and operational handover to Department staff.
- Provide the perpetual software license, together with a 3-year support contract covering the detection software.

Note: The output of this system is decision-support evidence for trained human adjudicators. No adverse determination affecting an applicant shall be made on the basis of an automated score alone.

4. Statement of Compliance

Bidders shall complete the "Bidder Response" column for every requirement below, stating Comply / Partially Comply / Not Comply, and provide supporting detail or references in the "Remarks" column. Each item is a minimum mandatory requirement unless otherwise stated. Where a product specification is stated as "minimum," bidders may propose equipment exceeding the stated minimums.

IMPORTANT: All requirements marked as "MANDATORY" must be fully met. A "Not Comply" or "Partially Comply" response against any mandatory requirement shall render the bid non-responsive.

4.1 Application Delivery Controller Appliance (Qty 1)

Category	Specification Requirement	Bidder Response (Comply / Partially / Not Comply)	Remarks
Quantity	One (1) ADC appliance.		
Platform Operating System	MANDATORY: The appliance shall include a purpose-built platform operating system / hypervisor layer ("Platform OS") that is installed directly on the bare-metal hardware. The Platform OS shall be a vendor-designed, minimal-footprint system whose sole function is to host, isolate and manage the ADC traffic-management software. General-purpose hypervisors (e.g., VMware ESXi, KVM, Hyper-V) or general-purpose operating systems (e.g., Linux, Windows, FreeBSD) used as the platform layer are not acceptable. The Platform OS must be designed, maintained and supported by the same vendor as the ADC software.		
Platform-Layer Orchestration	MANDATORY: The Platform OS shall expose a container-orchestration API (compatible with Kubernetes APIs) for declarative lifecycle management of the ADC tenant software, including deployment, scaling, upgrading and rollback. The platform shall maintain a declarative desired-state model and reconcile the running state automatically.		
Hardware Abstraction & Decoupled Lifecycles	MANDATORY: The Platform OS shall provide a hardware abstraction layer that fully decouples the ADC tenant software from the underlying physical hardware components (CPU, FPGA/acceleration, network interfaces, storage). This shall enable independent lifecycle management where the Platform OS firmware and the ADC tenant software can be upgraded, patched and rolled back independently without requiring coordinated downtime.		
Tenant-Based Software Deployment	MANDATORY: The ADC traffic-management software (including load balancing, SSL/TLS processing, DNS/GSLB, and scripting engine) shall run as a managed tenant workload on the Platform OS, not as a monolithic installation directly on the hardware. The Platform OS shall isolate the ADC tenant's control plane, data plane and management plane from the underlying platform layer.		
Dedicated Hardware Acceleration	MANDATORY: The appliance shall include dedicated, vendor-designed field-programmable hardware acceleration (FPGA or equivalent programmable logic) for SSL/TLS cryptographic offload and traffic processing. The hardware acceleration shall be programmable/upgradeable via the Platform OS firmware, allowing cryptographic algorithm updates without hardware replacement. CPU-only cryptographic processing (software crypto) is not acceptable for the primary SSL/TLS offload path.		
Control/Data Plane Isolation	MANDATORY: The Platform OS shall enforce strict isolation between the management/control plane and the data plane, such that management-plane operations (configuration changes, monitoring, logging) cannot impact data-plane throughput or latency. Data-plane processing shall continue		

	uninterrupted during management-plane restarts, upgrades or failures.		
Multi-Tenancy Capability	The Platform OS shall support the ability to run multiple isolated ADC software instances on the same physical appliance, enabling future expansion without additional hardware procurement. Each tenant instance shall have dedicated resource allocation (CPU cores, memory, FPGA offload capacity) and isolated configuration and data-plane contexts.		
Form Factor	1U rack-mount appliance for a standard 19-inch rack.		
Processor / Memory / Storage	MANDATORY: Minimum 16-core Intel Atom processor; minimum 64 GB DDR4 RAM; minimum 480 GB M.2 SSD storage.		
Network Interfaces	MANDATORY: Minimum 4 × 10G/1G copper RJ45 ports and 4 × 25G/10G/1G fiber SFP28/SFP+ ports, all concurrently usable. Interfaces shall support L2/L3 VLAN trunking, link aggregation (LACP), and interface failover.		
Transceivers	Minimum two (2) SFP+ (10 Gbps) transceiver modules supplied with the appliance.		
L4 / L7 Throughput	MANDATORY: Minimum Layer 4 throughput of 40 Gbps and Layer 7 throughput of 30 Gbps, measured with standard HTTP profiles.		
Connection Capacity	MANDATORY: Minimum 1.3 million Layer 7 requests per second (HTTP) and minimum 60,000 SSL/TLS transactions per second (RSA 2048-bit), utilizing the dedicated hardware acceleration. Performance figures must be published in the manufacturer's current datasheet for the proposed model.		
Traffic Management Engine	MANDATORY: The appliance shall include a fully programmable, event-driven scripting/rules engine based on an industry-standard scripting language (e.g. TCL) that permits custom inspection, transformation, redirection, and routing of application traffic at Layers 4–7 based on payload content, headers, client geography, and server state. The scripting engine shall execute inline at line rate within the data-plane processing pipeline without requiring external services, VMs, or containerized micro-services.		
Load Balancing Methods	Must support: Round Robin, Least Connections, Fastest Response, Weighted, Dynamic Ratio, and custom methods via the scripting engine. Must support session persistence via cookies, SSL session ID, source IP address, and custom methods.		
SSL/TLS Offload	MANDATORY: Hardware-accelerated SSL/TLS offload using the dedicated programmable hardware acceleration (FPGA or equivalent). Must support TLS 1.3, Perfect Forward Secrecy with ECDHE, and configurable cipher suites including those appropriate for government/FIPS use. Must support mutual (client-certificate) TLS authentication and certificate-based client access control.		
Integrated DNS/GSLB	MANDATORY: The ADC tenant software shall include an integrated DNS and Global Server Load Balancing (GSLB) module, providing authoritative DNS services, GSLB based on topology, geography, availability and performance metrics, and DNSSEC zone signing with hardware-protected keys. DNS services must be capable of at least 1,000 DNS queries per second.		

HSM Integration	MANDATORY: The ADC tenant software shall support integration with an external, network-attached Hardware Security Module meeting the specification in Section 4.2 via PKCS#11 (v2.20 or later) for hardware-protected generation, storage and use of SSL/TLS private keys, ensuring keys never exist in software or appliance memory outside the HSM.		
High Availability	Must support active-standby and/or active-active high-availability clustering with automatic configuration synchronisation and stateful connection failover between two or more appliances.		
Health Monitoring	Must support active and passive health monitors at Layers 3, 4, and 7, including scripted/custom monitors. Must support monitor chaining and the ability to designate specific monitors for different server pool members.		
Power	MANDATORY: Dual (1+1) redundant, hot-swappable AC power supplies. Both power supplies must be field-replaceable without powering down the appliance.		
IP Version Support	Full dual-stack IPv4 and IPv6 support, including IPv6-to-IPv4 gateway functionality and the ability to load balance IPv6 clients to IPv4 servers and vice versa.		
Programmatic Management	Must provide a RESTful management API (HTTPS/JSON) for all configuration, monitoring and automation tasks, at both the Platform OS level (hardware inventory, health, firmware) and the ADC tenant level (traffic configuration, policies). Must support declarative, API-driven configuration suitable for infrastructure-as-code workflows.		
Logging / SIEM Integration	MANDATORY: Must support structured log export in at least syslog (RFC 5424) and Common Event Format (CEF) to the Department's log management / SIEM platform. Must support high-speed logging (at least 50,000 log messages per second) without impacting data-plane performance. Logging shall be separately configurable for Platform OS events and ADC tenant events.		
FIPS Compliance	MANDATORY: The appliance operating system and cryptographic modules shall be FIPS 140-2 Level 2 (or FIPS 140-3 Level 2) validated, with the ability to operate in a FIPS-compliant mode. Bidder to state NIST CMVP certificate number(s).		
Regulatory Compliance	Appliance must carry FCC Class A, CE Mark, RoHS, UL/cUL, and CB Scheme certifications.		
Support	MANDATORY: 3-year manufacturer premium support (24×7) with same-business-day or next-business-day hardware replacement, unlimited technical support cases, and firmware/software updates covering both the Platform OS and the ADC tenant software. Third-party / reseller-only support is not acceptable; the manufacturer must be the primary support provider or must underpin the reseller's support with direct tier-3/engineering escalation.		
Installation & Commissioning	Full installation, configuration, integration, testing and commissioning including Platform OS initialization, ADC tenant deployment, redundant power cabling, local and GSLB load-balancing setup, health monitoring, SSL/TLS offload, high-availability configuration (for future expansion), HSM integration		

	for SSL key protection, DNS/DNSSEC setup, SIEM log integration, knowledge transfer and documentation.		
MSP Partner Status	MANDATORY: The Bidder must be the current Managed Service Provider (MSP) partner of the original equipment manufacturer (OEM) of the proposed ADC appliance. The Bidder shall provide evidence of active MSP partner status.		
Manufacturer Authorization	MANDATORY: Valid Manufacturer's Authorization Letter (MAL) or equivalent authorized partner/reseller letter from the OEM of the proposed ADC appliance. The Bidder must hold current authorized reseller or partner status with the OEM. Higher-tier partnership levels (e.g., Platinum, Elite, Premier, Expert) will be viewed favorably during evaluation.		

4.2 Hardware Security Module - Network-Attached (Qty 1 Bundle)

Category	Specification Requirement	Bidder Response (Comply / Partially / Not Comply)	Remarks
Quantity	One (1) network-attached HSM bundle including the primary HSM appliance and one (1) dedicated hardware backup HSM.		
Platform Type	MANDATORY: The HSM shall be a dedicated, network-attached cryptographic appliance (not a PCIe card, USB device or software-only solution). All cryptographic key materials shall be generated, stored and used exclusively within the tamper-resistant hardware security boundary. Keys shall never exist in plaintext outside the HSM. The HSM shall run a vendor-hardened, minimal-footprint operating system designed solely for cryptographic key protection.		
Certification	MANDATORY: FIPS 140-3 Level 3 validated (overall Level 3 certification, not merely physical Level 3 with software/firmware Level 1). Bidder to provide the current NIST CMVP certificate number. Additionally, Common Criteria EAL 4+ (or higher) certification with a recognized protection profile is required.		
Form Factor	1U network-attached appliance for a standard 19-inch rack, with a minimum of two Gigabit Ethernet interfaces for segregated management and application connectivity.		
Authentication	MANDATORY: The HSM shall provide hardware-based, trusted-path multi-factor authentication using a dedicated, physically isolated PIN Entry Device (PED). Authentication credentials shall never traverse the host operating system, network, or any connected client system. The trusted path between the PED and the HSM shall be cryptographically secured with mutual authentication. Software-only, web-based, or network-exposed administrative authentication mechanisms are not acceptable for security-officer operations.		
Multi-Person Control	MANDATORY: The HSM shall support M of N / quorum-based multi-person access control for all sensitive administrative operations, requiring a		

	configurable threshold (e.g., 2 of 3, 3 of 5, up to N of 16) of distinct authorized administrators with separate PED keys to perform operations such as partition creation, key generation, backup/restore, and policy changes.		
Partitions	MANDATORY: Minimum 5 independent cryptographic partitions as supplied (without additional licensing), each with its own security officer, cryptographic boundary, access controls, keys, capacity allocation, and audit log. Partitions shall be hardware-isolated from one another such that no partition can access another partition's key material.		
Secure Key Storage	MANDATORY: Minimum 16 MB of internal non-volatile secure key storage memory within the hardware security boundary, usable across all partitions.		
Cryptographic Performance	MANDATORY: Enterprise-class cryptographic processing performance. Bidder to state minimum symmetric (AES-256-GCM) operations per second, RSA-2048 signing operations per second, and ECC (P-256/P-384) signing operations per second, as verified by the OEM's published datasheet.		
Algorithm & Key Support	MANDATORY: The HSM shall support the full algorithm suite: RSA (1024–8192 bit), DSA, Diffie-Hellman, ECDSA and ECDH over NIST prime curves (P-256, P-384, P-521), Brain pool curves, and Edwards curves (Ed25519/Curve25519). Must support AES (128/192/256 in GCM and CBC modes), 3DES, HMAC with SHA-256/384/512, and SHA-3. Must include a hardware true random number generator compliant with NIST SP 800-90A/B/C. All algorithms must be implemented in hardware.		
Post-Quantum Readiness	The HSM shall support or have a published roadmap for NIST-standardized post-quantum cryptographic algorithms within the core firmware. Bidder to state current PQC algorithm support and timeline for CRYSTALS-Kyber, CRYSTALS-Di lithium, and FALCON support.		
Integration / APIs	MANDATORY: The HSM shall provide PKCS#11 (v2.40 or later), Java JCA/JCE, Microsoft CNG/KSP, OpenSSL engine, and a REST API for client integration, enabling the ADC appliance (Item 1) and other applications to use HSM-protected keys. All APIs shall support network-attached operation over mutually authenticated TLS (mTLS) connections.		
Backup & Recovery	MANDATORY: A dedicated hardware backup HSM shall be included in the bundle. Backup and restore of cryptographic key material shall use strong cryptographic wrapping (minimum AES-256 key-wrap) within the hardware security boundary, with M of N split-knowledge control. At no point shall plaintext key material leave the hardware boundary during backup or restore operations. The backup HSM shall be a dedicated hardware device (not software-based or virtual).		
High Availability	Must support HA / load-balancing groups across multiple HSM appliances, with transparent client failover and automatic, cryptographically secured key-material synchronization between group members.		

Remote Management	Must support remote administration and Remote PED functionality with a cryptographically secured, mutually authenticated Secure Trusted Channel (STC) between a remote administration workstation and the HSM.		
Tamper Protection	MANDATORY: The HSM shall implement physical tamper-evident and tamper-responsive mechanisms, including but not limited to: active tamper mesh covering all critical components, environmental sensors (voltage, temperature), and secure, immediate zeroization/deletion of all key material upon tamper detection. The appliance shall implement hardware-anchored secure boots with cryptographic firmware signature verification at every boot cycle.		
Power	MANDATORY: Dual (1+1) redundant, hot-swappable power supplies. Appropriate power cords for the local electrical supply (Type G, 240 VAC) shall be supplied for both the primary HSM and the backup HSM.		
Audit Logging	MANDATORY: The HSM shall maintain an independent, cryptographically signed, tamper-evident audit log within the hardware security boundary. Logs shall be exportable via syslog and/or REST API to the Department's SIEM platform. Audit log integrity shall be independently verifiable. Logs must capture all administrative actions, cryptographic operations, authentication events, partition-level events, and configuration changes with timestamp accuracy traceable to a trusted time source.		
Support	MANDATORY: 3-year manufacturer Enhanced Maintenance Service, 24×7, with same-business-day or next-business-day hardware replacement for both the primary HSM and the backup HSM. The maintenance must be provided by or contractually underpinned by the OEM; reseller-only support without OEM back-to-back support agreement is not acceptable.		
Installation & Commissioning	Full installation, initialization, PED configuration, key ceremony, partition creation, client application registration (including Item 1 ADC), backup configuration, HA configuration, SIEM log integration, knowledge transfer and full key-ceremony documentation with chain-of-custody records.		
Regulatory Compliance	FCC Class A, CE Mark, RoHS, UL/cUL, CB Scheme.		
Manufacturer Authorization	MANDATORY: Valid Manufacturer's Authorization Letter (MAL) or equivalent authorized partner/reseller letter from the OEM of the proposed network-attached HSM. The Bidder must hold current authorized reseller or partner status with the OEM. Higher-tier partnership levels will be viewed favorably.		

4.3 Hardware Security Module - Compact (Qty 2)

Note: This item is supplied only with manufacturer warranty. Implementation and configuration will be performed by the Department.

Category	Specification Requirement	Bidder Response (Comply / Partially / Not Comply)	Remarks
Quantity	Two (2) compact HSM devices.		
Platform Type	MANDATORY: The HSM shall be a self-contained, directly attached hardware security module with all cryptographic operations occurring wholly within the hardware device. Smart card-based solutions requiring a separate reader are not acceptable.		
Certification	MANDATORY: FIPS 140-3 Overall Level 3 validated. Bidder to provide the current NIST CMVP certificate number. FIPS 140-2 certification is not acceptable as a substitute; the device must hold an active FIPS 140-3 validation.		
Form Factor	MANDATORY: Nano form factor (not exceedingly approximately 15 mm × 15 mm × 5 mm), suitable for permanent deployment directly on a server or workstation USB-A port without obstructing adjacent ports. Must be USB 2.0 or later. Must be solid-state with no batteries and no moving parts.		
Environmental Durability	MANDATORY: The device shall be rated IP68 (dust-tight and water-resistant), suitable for long-term deployment in data centre and server-room environments.		
FIPS Operating Mode	MANDATORY: The device shall be configurable to operate exclusively in a FIPS-approved mode of operation whereby only FIPS-validated cryptographic algorithms are available. Non-FIPS algorithms shall be programmatically disabled and shall not be activatable in this mode.		
Algorithm Support	MANDATORY: Must support RSA (2048/3072/4096), ECC (NIST P-256, P-384, P-521), Edwards curves (Ed25519 / Curve25519), AES (128/192/256-GCM and CBC), HMAC with SHA-256/384/512. Must support ECDH key agreement and ECDSA/EdDSA digital signatures. Must support true hardware random number generation.		
Key Storage Capacity	MANDATORY: Minimum 250 stored cryptographic objects, with a minimum of 128 KB total non-volatile secure storage. All keys shall be generated and stored within the hardware security boundary and shall never be exportable in plaintext.		
Session Concurrency	MANDATORY: The device shall support a minimum of 16 concurrent authenticated sessions/applications connecting to the device.		
Integration / APIs	MANDATORY: The device shall provide PKCS#11 (v2.20 or later) interface support, open-source native libraries/SDK for custom application integration, and a Microsoft CNG/KSP provider for use with Active Directory Certificate Services (AD CS) and other Windows cryptographic subsystems.		
Access Control	MANDATORY: The device shall support role-based access control with per-key capabilities and		

	permissions, including the ability to restrict individual keys to specific operations (sign, verify, encrypt, decrypt, wrap, unwrap). Authentication and authorization events shall be auditable.		
Backup & Recovery	MANDATORY: The device shall support secure key backup using cryptographic wrap keys (minimum AES-256 key-wrap), with M of N / split-knowledge control across multiple key custodians. Backup material shall never expose plaintext key data. The two devices supplied shall be configurable for mutual redundancy.		
Audit Logging	The device shall maintain an internal tamper-evident audit log and support export to the Department's log management / SIEM platform to the maximum extent supported by the hardware.		
Supply Chain Security	The devices must be new, unused, and sourced from an OEM-authorised distribution channel with documented chain of custody. Grey-market, refurbished, or pre-owned devices are not acceptable.		
Support / Warranty	3-year manufacturer warranty with device replacement and firmware/software updates.		

4.4 HSM Infrastructure Penetration Test

Category	**Specification Requirement**	**Bidder Response (Comply / Partially / Not Comply)**	**Remarks**
Scope	MANDATORY: The penetration test shall cover the complete deployed HSM infrastructure comprising the network-attached HSM appliance and its backup HSM (Item 2), the compact HSMs (Item 3), their respective management and application network interfaces, the PED authentication mechanism, all exposed APIs (PKCS#11, REST, CNG/KSP), the HSM audit logging subsystem, and the cryptographic integration path between the ADC (Item 1) and the network-attached HSM.		
Timing & Commencement	MANDATORY: The test shall commence within five (5) working days of written notification from the Department. The notification will be issued once the Department has completed internal deployment and configuration of Items 2 and 3. The Bidder shall confirm receipt of notification within one (1) working day and provide a test commencement date within the 5-working-day window.		
Report Delivery	MANDATORY: A comprehensive written penetration test report shall be delivered to the Department within seven (7) calendar days of test commencement. Failure to deliver the report within this timeframe shall constitute non-performance.		
Methodology	MANDATORY: The penetration test shall follow a recognized industry methodology adapted for cryptographic infrastructure assessment (e.g., OWASP WSTG, PTES, NIST SP 800-115, OSSTMM, or equivalent). The Bidder shall state the methodology to be used. Testing shall be non-destructive and shall not risk key-material loss, service unavailability, or HSM zeroization.		

	Any test case carrying risk of disruption shall be pre-approved in writing by the Department before execution.		
Test Coverage	The penetration test shall include, at minimum: authentication bypass testing, authorization/privilege escalation testing, partition-boundary validation, cryptographic implementation review, API abuse testing (PKCS#11, REST), network protocol analysis, audit-log integrity and tampering assessment, and configuration hardening review. The Bidder shall provide a detailed test plan for Department approval prior to commencement.		
Report Contents	MANDATORY: The report shall include: (a) an executive summary suitable for senior management; (b) a detailed description of the testing methodology and scope; (c) all findings individually enumerated with CVSS 4.0 severity ratings, detailed technical descriptions, step-by-step reproduction instructions with evidence (screenshots, packet captures, command output), root-cause analysis, and business-impact assessment; and (d) prioritized, actionable remediation recommendations for each finding, ranked by risk severity.		
Presentation	The Bidder shall present the findings to Department technical staff in a walkthrough session (in-person or remote) within ten (10) calendar days of report delivery, covering all identified findings, exploitation paths and recommended remediation measures.		
Tester Qualifications	MANDATORY: The penetration test shall be led and executed by personnel holding at least one recognized penetration testing certification (e.g., OSCP, OSCE, GPEN, CREST CRT/CCT, or equivalent). The Bidder shall provide the CV(s) and certification evidence of the lead tester(s) assigned to this engagement.		

4.5 AI-Generated and Manipulated Image Detection System (Qty 1)

Note: This item comprises detection software developed in-house by the Bidder and licensed to the Department perpetually, together with the supply of two (2) dedicated AI compute devices on which it is deployed, and integration, training and a 3-year support and model update contract. The system is decision-support tooling for trained human adjudicators; no adverse determination affecting an applicant shall be made on the basis of an automated score alone.

Category	**Specification Requirement**	**Bidder Response (Comply / Partially / Not Comply)**	**Remarks**
Quantity & Licensing	MANDATORY: Two (2) AI compute devices as specified below, with the detection software deployed on both. All detection software, detection models installed at handover, management console and API components shall be licensed to the Department on a perpetual, irrevocable, non-expiring basis. The license shall place no cap on the number of images analyzed and shall cover a minimum of ten (10) named reviewer accounts and unlimited machine/API service accounts. Subscription, term-limited, per-image, per-seat or consumption-based licensing is not acceptable.		

	The license shall permit deployment on both supplied devices — one (1) production instance and one (1) non-production instance for testing, model tuning, staging and disaster recovery — at no additional charge. The license shall not be tied to specific hardware, and the Department shall be entitled to redeploy the software onto replacement or upgraded infrastructure without additional charge. The Bidder shall state the licensing model in full and disclose any restriction of any kind on volume, seats, throughput, features, hardware binding or duration.		
License Continuity	MANDATORY: The perpetual license shall survive expiry, non-renewal or termination of the support contract. On expiry of the 3-year support term the software shall continue to operate indefinitely and without degradation using the detection models and software version last installed, retaining full access to all historical case records, audit logs and stored analysis results. The software shall contain no time-limited license key, license server dependency, remote activation check, feature disablement, throughput throttle or other mechanism capable of restricting or terminating operation. The Bidder shall confirm this in writing and shall state the mechanism by which the perpetual license is evidenced and transferred to the Department.		
Deployment Model	MANDATORY: The system should be deployed and executed entirely on the compute devices supplied under this item, located within the Department's data center and under the Department's sole control. The system should be capable of operating permanently disconnected from the public internet. Cloud-hosted, hybrid, SaaS or API-brokered architectures in which any part of the analysis occurs off-premises are not acceptable.		
Data Sovereignty & Confidentiality	MANDATORY: No image, biometric template, derived feature vector or embedding, metadata, hash, score or analysis result shall be transmitted outside Department infrastructure under any circumstances, including license validation, telemetry, crash reporting, usage analytics, model improvement, or vendor support and diagnostics. License activation and model updates shall be achievable entirely by offline, cryptographically signed package. The Bidder shall declare every outbound network connection the software attempts and the means of disabling each.		
Synthetic (AI-Generated) Image Detection	MANDATORY: Detection of fully synthetic imagery produced by generative adversarial network (GAN) and diffusion-based architectures, including current-generation text-to-image and image-to-image generators. Detection shall not rely solely on a fixed signature list of known generators or on embedded watermarks; the system shall demonstrate generalization to generator architectures absent from its training data. Bidder to state measured performance on unseen / out-of-distribution generators and to name the evaluation datasets used.		
Face Morphing Attack Detection	MANDATORY: Both single-image, no-reference morphing attack detection (S-MAD) on a submitted photograph and differential morphing attack detection (D-MAD) comparing a submitted		

	photograph against a trusted live capture or previously enrolled reference image. Detection shall cover landmark-based, GAN-based and diffusion-based morphs, including morphs subjected to print-and-scan reproduction and JPEG re-compression. Evaluation shall be aligned to ISO/IEC 20059. Bidder to state MACER at fixed BPCER values of 1% and 0.1%.		
Face Swap / Deepfake Detection	MANDATORY: Detection of face substitution, face reenactment and identity-blending applied to an otherwise genuine photograph, including attacks that have been re-compressed, resized or subjected to post-processing intended to suppress detection artefacts.		
Digital Manipulation & Retouching Detection	MANDATORY: Detection of conventional editing of genuine images, including splicing and compositing, copy-move duplication, generative inpainting and object removal, airbrushing and beautification, geometric warping of facial geometry or inter-landmark distances, colour and luminance manipulation, and alteration of printed text or data fields within scanned supporting documents (names, dates, reference numbers, seals, stamps and signatures).		
Recapture & Presentation Attack Detection	Detection of print-and-scan reproduction, screen or display recapture, photo-of-photo capture, and printed or mask-based presentation attacks, evaluated in accordance with ISO/IEC 30107-3. Bidder to state APCER and BPCER for each attack species supported.		
Classical Forensic Analysis	MANDATORY: The platform shall additionally provide non-machine-learning forensic analyses, including error level analysis, JPEG quantization table and double-compression analysis, PRNU / sensor pattern noise analysis, colour filter array and demosaicing artefact analysis, noise residual analysis, lighting and shadow consistency assessment, geometric and perspective consistency assessment, and full EXIF / XMP / IPTC metadata extraction with anomaly flagging. These analyses shall be presented as independent evidence alongside the model-based scores.		
Provenance & Content Credentials	The platform shall validate C2PA / Content Credentials manifests where present, verify the signature and ingredient chain, and flag manifests that are absent, stripped, broken or inconsistent with the image content. Absence of provenance data shall not, by itself, be presented as evidence of manipulation.		
Tamper Localisation	MANDATORY: The system shall produce a pixel-level localisation heatmap identifying the regions of an image assessed as manipulated, displayable as an overlay on the source image within the review console and exportable into the forensic report.		
Scoring & Explainability	MANDATORY: Each analysis shall return a calibrated authenticity score on a defined scale, a classification of the manipulation type or types detected, and a human-readable summary of the specific evidence contributing to the score. A bare binary authentic / manipulated verdict without supporting evidence is not acceptable. Referral and escalation thresholds		

	shall be configurable by the Department independently for each workflow.		
Accuracy & Independent Evaluation	MANDATORY: The Bidder shall state, for each detection category, the true positive rate at fixed false positive rates of 1% and 0.1%, on named and reproducible datasets, together with the test conditions. Where available for the proposed product, evidence of independent third-party or accredited-laboratory evaluation (for example NIST FATE MORPH, NIST FATE / FRVT, or an ISO/IEC 17025 accredited laboratory) shall be submitted with the report reference. Vendor marketing claims unsupported by a stated test protocol will be disregarded during evaluation.		
Demographic Performance & Model Governance	MANDATORY: The Bidder shall supply a model card for each detection model, documenting intended use, training data provenance and licensing, known limitations and failure modes, and measured performance differentials across skin tone, sex and age cohorts. Undisclosed or unmeasured demographic performance variation shall be treated as a material deficiency, given the consequences of a false positive for a genuine applicant.		
Input Format Support	The system shall accept JPEG, PNG, TIFF, BMP, WebP, HEIF/HEIC and JPEG 2000 images, and images embedded within PDF documents, at resolutions from ICAO-compliant facial capture upwards. Batch ingestion from a watched folder or archive shall be supported. Bidder to state whether video frame analysis is supported and any additional licensing required.		
Throughput & Latency	MANDATORY: Minimum sustained throughput of [•] images per minute in batch mode and maximum end-to-end latency of [•] seconds per image for interactive single-image analysis, measured on a single supplied compute device operating as the production instance. Bidder to state the benchmark conditions, the image resolution, and which detection modules were enabled. Where the system fails to meet the stated performance at Site Acceptance Testing on the supplied devices, remediation shall be at the Bidder's cost.		
API & Integration	MANDATORY: A documented REST API over HTTPS/JSON with a published OpenAPI 3.x specification, supporting both synchronous single-image analysis and asynchronous batch submission with callback or webhook notification. The API shall support mutual TLS and token-based authentication. A client SDK in at least one mainstream language shall be provided. The Bidder shall confirm and demonstrate integration with the Department's existing intake and issuance workflows.		
Review & Adjudication Console	MANDATORY: A web-based review console providing case management, side-by-side comparison of a submitted image against enrolled reference images, display of all detector outputs and localisation heatmaps, a prioritised adjudication queue, decision capture with mandatory justification for any override of the system's recommendation, second-reviewer confirmation of adverse determinations, and full case search and history.		

Forensic Reporting	MANDATORY: A per-case exportable report recording the analysed image and its SHA-256 hash, all detector outputs and scores, the software and model version identifiers used, the analysis timestamp from a trusted time source, the identity of the reviewing analyst, and the adjudication decision and its justification - in a form suitable for use in administrative and legal proceedings. Reports shall be digitally signed and shall be capable of being signed with keys protected in the network-attached HSM (Item 2) via PKCS#11.		
Chain of Custody & Retention	Submitted images and their associated analysis records shall be stored with tamper-evident hashing and a write-once retention policy, with retention periods configurable by the Department and secure, auditable deletion at end of retention.		
Detection Model Update Subscription	MANDATORY: Not less than quarterly detection model updates for the full three (3) year support term, delivered as cryptographically signed offline packages with published changelogs stating measured performance deltas per detection category. Model updates shall be included within the 3-year support contract at no additional charge. Given the pace at which generative models evolve, the Bidder shall additionally state its expedited update process for a materially new generator architecture or attack technique, with a target of no more than sixty (60) calendar days from public emergence to an available detection update. Models installed during the support term shall remain licensed to the Department in perpetuity.		
On-Premises Tuning	Desirable: The ability to calibrate decision thresholds and, where supported, to fine-tune detection models against the Department's own retained data, performed entirely on premises with no data egress. Bidder to state what tuning is supported, what skills and effort it requires, and whether it invalidates any vendor performance warranty.		
Authentication & Access Control	MANDATORY: Integration with the Department's directory service via LDAPS and/or SAML 2.0 or OpenID Connect. Role-based access control providing at minimum reviewer, senior adjudicator, administrator and auditor roles with enforced segregation of duties. Multi-factor authentication for all administrative accounts.		
Audit Logging & SIEM Integration	MANDATORY: An immutable audit log capturing every analysis performed, score returned, adjudication decision, override, export, user session and configuration change, with export to the Department's log management / SIEM platform via syslog (RFC 5424) and Common Event Format (CEF).		
Compute Devices (Qty 2)	MANDATORY: The Bidder shall supply two (2) units of the xFusion FusionXpark GB10 appliance (xFusion International Pte. Ltd.). Each unit shall be configured with 4 TB of self-encrypting NVMe M.2 storage and shall be supplied with the NVIDIA DGX OS pre-installed. Units shall be new, unused, of current production, and sourced through an xFusion-authorised channel. This is a specified product requirement; alternative or equivalent devices shall not be accepted, and a bid offering an alternative device shall be treated as non-responsive. The Bidder		

	shall state the serial numbers of the units supplied at handover.		
Manufacturer Authorization (Appliances)	MANDATORY: A valid Manufacturer's Authorization Letter (MAL), or equivalent authorised partner or distributor letter, issued by xFusion International Pte. Ltd. or its authorised regional distributor, confirming that the Bidder is authorised to supply, deliver and support the FusionXpark GB10 appliance within the Republic of Maldives for this procurement. The letter shall be issued on the manufacturer's letterhead, be specific to this tender, be signed by an authorised signatory, and remain valid for the bid validity period. Failure to submit a valid authorisation shall render the bid non-responsive. This requirement applies to the appliance hardware only; no manufacturer authorisation is required in respect of the detection software, which is developed in-house by the Bidder.		
Device Roles & Capacity	MANDATORY: One device shall be commissioned as the production instance and the second as the non-production instance for testing, model tuning, staging and disaster recovery. The Bidder shall confirm that the production device alone meets the throughput and latency requirements of this Section, and shall state the procedure and expected recovery time for promoting the non-production device to production service in the event of failure. The Bidder shall additionally state whether the two devices can be interconnected via their high-speed network interfaces to operate as a single larger compute resource, and the circumstances in which the Department might do so.		
Software Compatibility	MANDATORY: The Bidder shall confirm that its detection software, all detection models, and every third-party and open-source dependency execute natively on the Arm64 architecture and operating environment of the supplied devices, at the stated performance. Reliance on emulation or binary translation is not acceptable. The Bidder shall state any component that does not run natively and how it will be remediated before Site Acceptance Testing.		
Device Hardening & Physical Security	MANDATORY: Prior to handover the Bidder shall disable all wireless interfaces (Wi-Fi and Bluetooth), enable self-encryption on the internal storage with key escrow to the Department, enable secure boot and firmware signature verification, and disable all unused physical interfaces. Given the compact and portable form factor of the devices, the Bidder shall supply a secure mounting or lockable enclosure arrangement suitable for installation in the Department's data centre, and shall document asset serial numbers at handover. The Bidder shall state the power draw and thermal output of each device and confirm compatibility with the Department's rack power and cooling provision, including connection to the Department's uninterruptible power supply.		
Hardware Warranty & Replacement	MANDATORY: Three (3) year hardware warranty on both supplied devices, with advance or next-business-day replacement. Because the devices are not internally redundant, the Bidder shall state its replacement logistics for the Republic of Maldives, the expected replacement lead time, and whether a spare		

	unit or advance-exchange stock is held in or near country. Any failed storage device shall remain the property of the Department and shall not be returned to the manufacturer.		
Software Architecture & Portability	MANDATORY: The software shall be delivered as a self-contained offline installation bundle - OCI-compliant container images or an equivalent package distribution - with no dependency on external package repositories or model registries at install time or runtime. The Department shall be able to reinstall and reconfigure the licensed software into replacement or upgraded infrastructure, without vendor intervention or network access, using the supplied bundle and documentation, including after the support term has expired. The Bidder shall supply that bundle, the installation and recovery documentation, and all configuration as code or documented configuration export.		
Documentation	Complete architecture, installation, configuration, administration, API and operational runbook documentation, together with the model cards, performance characterization and the declared outbound-connection statement.		
Support	MANDATORY: 3-year software support, with 24×7 response for critical incidents, unlimited support cases, defect correction, and all software version upgrades released during the term. Support shall be provided directly by Bidder's own development and engineering team; Bidder shall name the engineers responsible, state the escalation path to its development function, and state its committed response and resolution times by severity. Support shall additionally cover the two supplied compute devices for the full 3-year term, including firmware and operating environment updates, and shall be underpinned by a back-to-back agreement with the device manufacturer or its authorized distributor, evidence of which shall be submitted. The Bidder shall additionally quote indicative annual renewal pricing for years four (4) and five (5), for the Department's budgetary planning; this indicative pricing shall be shown separately and shall not form part of the evaluated bid price under Section 6.3.		
Assigned AI / ML Engineer	MANDATORY: Both certified AI / machine learning engineers required under Section 5.1 (NVIDIA-Certified Professional (AI) or equivalent) shall be assigned to this item and shall be jointly responsible for deployment, threshold calibration, acceptance testing and management of detection model updates throughout the contract term. At least one of the two shall be available for support escalation at any time during the implementation period. The Bidder shall confirm both named individuals and submit CVs and certification evidence.		
Software Ownership & IP	MANDATORY: The Bidder should warrant in writing that it is the developer and owner of the detection software, or that it otherwise holds all rights necessary to grant the Department the perpetual license required above, and shall indemnify the Department against any third-party intellectual property claim arising from its use.		

Development Capability	MANDATORY: The Bidder shall evidence its in-house capability to develop and maintain the detection software, stating the size and composition of its development team, the location at which development is performed, its development methodology and release process, and its version control, testing and quality assurance practices. The two certified AI / machine learning engineers required under Section 5.1 shall be members of, or directly supported by, this team.		
Secure Development & Application Security	The Bidder shall describe its secure development lifecycle, including code review, dependency vulnerability scanning, static and dynamic application security testing, and its process and committed timeframes for remediating vulnerabilities discovered in the delivered software during the support term. The Department reserves the right to subject the delivered application to independent security testing at any time during the contract term.		

5. Pre-Qualification & Mandatory Submission Documents

Parties interested in delivering the scope of work outlined shall be required to meet the following Pre-Qualification Requirements. Failure to comply with, or to submit, any of the documents below may result in disqualification of the bid.

5.1 Mandatory Submission Documents

Bidders must submit copies of the following valid and applicable documents as part of their submission:

- Manufacturer's Authorization Letters (MALs) or equivalent Authorized Partner/ Reseller Letters from the original equipment manufacturer (OEM) for the proposed ADC appliance (Item 1), the network-attached HSM (Item 2), and the xFusion FusionXpark GB10 appliances supplied under Item 5. A valid authorization must be provided for each of these three product lines; failure to provide a valid authorization for any of them shall render the bid non-responsive. No Manufacturer's Authorization Letter is required for the Item 5 detection software, which is developed and delivered in-house by the Bidder.
- Partnership / Accreditation documentation confirming the Bidder's current authorized-reseller or partner status with the OEM of the ADC appliance and the network-attached HSM (Items 1 and 2). Higher partnership tiers (e.g., Platinum, Elite, Premier, Expert, Advanced) will be viewed favorably during evaluation.
- MSP Partner Status - MANDATORY: The Bidder must be a current Managed Service Provider (MSP) partner of the OEM of the proposed ADC appliance (Item 1). Evidence of active MSP partner status, including partnership tier, shall be submitted. Higher MSP partner tiers will be viewed favorably during evaluation.
- ADC Deployment Reference - MANDATORY: The Bidder shall submit at least one (1) verifiable reference for an ADC deployment delivered to a large-scale infrastructure provider within the Republic of Maldives. The reference shall include the client

organization name, a brief description of the deployment scope, the date of commissioning, and a client contact authorized to confirm the reference. The Bidder may be asked to facilitate a reference call or site visit.

- ADC Staff Certification - MANDATORY: The Bidder shall provide evidence that at least one (1) permanent technical staff member holds a current, valid professional certification from the OEM of the proposed ADC appliance. The certification shall be at the professional/administrator level or higher (vendor associate-level certifications are not sufficient). The certified staff member must be assigned to this project.
- AI / Machine Learning Engineer Certification - MANDATORY: The Bidder shall provide evidence that at least two (2) permanent technical staff members assigned to this project are certified AI engineers. Each nominated engineer shall hold a current, valid professional-level certification in artificial intelligence and/or machine learning engineering - NVIDIA-Certified Professional (AI) or equivalent. Where a Bidder proposes an alternative certification as equivalent, it shall state the certifying body, the examination requirements and the currency period, and the Department's determination of equivalence shall be final. The Bidder shall submit certification evidence together with the CV of each engineer. Introductory or foundational-level certifications alone are not sufficient where a professional-level certification exists within the same certification track. Both nominated engineers shall be assigned to Item 5 and shall remain available to the Department for the duration of the implementation; any substitution shall require the Department's prior written approval and a replacement of at least equivalent qualifications.
- Sovereign AI Deployment Reference - MANDATORY: The Bidder shall submit at least one (1) verifiable reference for a sovereign AI deployment. For the purposes of this Statement of Requirements, a sovereign AI deployment means the deployment of an artificial intelligence or machine learning system that operates entirely on infrastructure under the client's own control and within the client's national jurisdiction, where model inference and all data processing are performed on that infrastructure and no data, model, derived feature or analysis result is transferred to a third-party-hosted or foreign-hosted service. The reference shall state the client organization, the nature and scale of the AI/ML workload, the deployment architecture and the compute platform used, the date of commissioning, and a client contact authorized to confirm the reference. Deployments hosted on public cloud or delivered as SaaS shall not be accepted as evidence of sovereign AI delivery capability. References demonstrating deployment in a government identity, civil registration, border control, law enforcement or regulated financial services context, or involving image authenticity and manipulation detection, will be viewed favorably during evaluation.
- In-House Development Capability Statement (Item 5) - MANDATORY: A statement evidencing the Bidder's in-house software development capability, including development team size and composition, location of development, methodology, release process, and quality assurance and secure development practices, as required by Section 4.5.

- Penetration Testing Reference - MANDATORY: The Bidder shall submit at least one (1) verifiable reference for a penetration testing engagement conducted on a complex transactional system. Each reference shall include the client organization name, a brief description of the system tested, and engagement scope, the date of completion, and a client contact authorized to confirm the reference.
- Penetration Tester Certification(s) - A copy of the recognized penetration testing certification(s) (e.g., OSCP, eCPPT, eWPTX, CREST CRT/CCT, or equivalent) held by the lead tester(s) proposed for this engagement.
- Business Registration Certificate (company registration).
- SME Registration Certificate.
- MIRA Tax Clearance Report (not older than 3 months from the proposal submission date).
- Itemized pricing / quotation covering the complete scope of supply, delivery, implementation and support for all five items (partial bids are not acceptable).
- Any other documents expressly required or referenced elsewhere in this bidding document.

5.2 Manufacturer's Authorization / Authorized Reseller

Any firm that is not the original manufacturer or producer of the goods proposed for supply for Items 1 (ADC), 2 (Network-Attached HSM) and the compute appliances supplied under Item 5 shall be required to submit a valid Manufacturer's Authorization Letter (MAL) or equivalent Authorized Partner Letter for each such product. The authorization letter must:

- Be issued by the original equipment manufacturer or principal producer of the goods (not by a distributor or value-added reseller acting as an intermediary);
- Clearly state that the Bidder is authorized to supply, install, and provide after-sales service and support for the specified goods within the territory of the Republic of Maldives; and
- Be valid, on OEM letterhead, and reference this Statement of Requirements or the associated RFP reference number ().

Failure to submit a valid Manufacturer's Authorization Letter or equivalent, where required, shall render the bid non-responsive.

5.3 Delivery, Implementation and Commencement

The successful Bidder shall complete the supply, delivery, installation and implementation of the ADC appliance (Item 1) and the network-attached HSM (Item 2) within seventy (70) calendar days from the date of receipt of the official Purchase Order/contract. The compact HSMs (Item 3) shall be delivered within the same period. The HSM infrastructure penetration test (Item 4) shall commence within five (5) working days of written notification from the Department following deployment, and the report shall be delivered within seven (7) calendar days of commencement. The AI-generated and manipulated image detection system (Item 5) shall be supplied, deployed, integrated and presented for Site Acceptance Testing within ninety (90) calendar days from the date of receipt of the official Purchase Order/contract, with final acceptance contingent on successful completion of the Site

Acceptance Test defined in Section 4.5. The 3-year manufacturer support and maintenance services shall commence upon commissioning of Items 1, 2 and 5, and upon delivery of Item 3, and continue for the full 3-year contract term.

6. Bid Evaluation Criteria

Bids will be evaluated in two stages. Stage 1 is a pass/fail compliance review; Stage 2 is a weighted scoring of those bids that pass Stage 1. Only bids determined to be substantially responsive at Stage 1 shall proceed to Stage 2.

6.1 Stage 1 - Pass / Fail Compliance Review

A bid shall be rejected without further evaluation, and shall not be scored, where the Bidder fails to submit any mandatory document listed in Section 5.1, fails to provide a valid Manufacturer's Authorization Letter where required under Section 5.2, submits a partial bid not covering all five items, or records a response of "Not Comply" or "Partially Comply" against any requirement identified as MANDATORY in Section 4. Requirements marked MANDATORY are minimum thresholds and are not awarded marks; exceeding a stated minimum attracts no additional score except where expressly provided in Section 6.2.

6.2 Stage 2 - Weighted Evaluation

Responsive bids shall be scored out of one hundred (100) marks against the criteria and weightings below. The bid achieving the highest total score shall be recommended for award.

Evaluation Criterion	Weighting	Basis of Assessment
Price	50 marks	Total evaluated 3-year cost of ownership for the complete scope (all five items), assessed on the formula in Section 6.3.
Experience	30 marks	Demonstrated capability of the Bidder and its assigned personnel, assessed against the sub-criteria in Section 6.4.
Delivery	20 marks	Quoted delivery and implementation period and the credibility of the delivery plan, assessed against the sub-criteria in Section 6.5.
Total	100 marks	

6.3 Price (50 marks)

The evaluated price shall be the total cost of the complete scope over the three (3) year contract term, comprising the supply of all five items, installation, configuration, integration, training, the perpetual software license for Item 5, and all manufacturer support, maintenance and model update charges for the full term. Indicative years 4 and 5 support renewal of the pricing requested under Section 4.5 shall be quoted separately and shall not form part of the evaluated price. Bidders shall provide fully itemized pricing; a bid that omits pricing for any line item shall be treated as non-responsive under Section 6.1.

Prices shall be quoted inclusive of all duties, levies and applicable taxes, and delivered to the Department's nominated site. Where bids are quoted in different currencies, all prices shall

be converted to Maldivian Rufiyaa at the Maldives Monetary Authority mid-rate prevailing on the date of bid opening.

Price marks shall be awarded on a pro-rata basis, with the lowest evaluated responsive bid receiving the full 60 marks:

Price Score = (Lowest Evaluated Bid Price ÷ Bid Price Under Evaluation) × 60

The Department reserves the right to reject any bid it determines to be abnormally low, where the Bidder is unable to demonstrate to the Department's satisfaction that the quoted price is sustainable and covers the full scope, including the 3-year support and licensing obligations.

6.4 Experience (30 marks)

Experience marks shall be awarded only on the basis of documentation submitted with the bid and verifiable by the Department. References that cannot be verified, or that the referenced client declines to confirm, shall score zero. The certification and staffing requirements of Section 5.1 - including the OEM-certified ADC engineer, the certified lead penetration tester and the two certified AI / machine learning engineers - are mandatory qualifying thresholds assessed at Stage 1 and are not separately scored at this Stage.

Sub-Criterion	Marks	Basis of Assessment
OEM Partnership Standing	15	Partnership tier held with the OEMs of Items 1 and 2, and MSP partner tier for Item 1. The manufacturer authorization required for the Item 5 appliances is a mandatory qualifying threshold assessed at Stage 1 and is not scored under this sub-criterion.
ADC Deployment Experience	5	Verifiable ADC deployments to large-scale infrastructure providers within the Republic of Maldives. One reference (the mandatory minimum under Section 5.1) 4 marks; two or more references 5 marks. References that cannot be verified score zero, and a Bidder submitting no verifiable reference is non-responsive under Section 6.1.
Penetration Testing Experience	5	Verifiable penetration testing engagements on complex transactional systems involving PKI and HSM infrastructure. One reference (the mandatory minimum under Section 5.1) 4 marks; two or more references, or a single reference covering cryptographic or HSM infrastructure specifically, 5 marks. References that cannot be verified score zero, and a Bidder submitting no verifiable reference is non-responsive under Section 6.1.
Sovereign AI Deployment Experience	5	Verifiable sovereign AI deployments as defined in Section 5.1. One reference (the mandatory minimum under Section 5.1) 4 marks; 5 marks where the Bidder submits two or more references, or where a single reference is a government organization, or involves image authenticity and manipulation detection. References that cannot be verified score zero, and a Bidder submitting no verifiable reference is non-responsive under Section 6.1.
Total	30	

6.5 Delivery (20 marks)

Delivery marks assess both the period quoted by the Bidder and the credibility of the plan by which it will be achieved. The maximum periods stated in Section 5.3 are binding ceilings: a bid quoting a delivery or implementation period exceeding those ceilings shall be non-responsive under Section 6.1 and shall not be scored.

Sub-Criterion	Marks	Basis of Assessment
Quoted Delivery Period	12	The Bidder's committed period, in calendar days from receipt of the Purchase Order to complete supply, delivery, installation and implementation of Items 1, 2 and 3 and to present Item 5 for Site Acceptance Testing. Scored pro-rata: Score = (Shortest Quoted Period ÷ Quoted Period Under Evaluation) × 12.
Delivery & Implementation Plan	6	Credibility and completeness of the submitted plan, including a task-level schedule with dependencies and milestones, named resources mapped to tasks, stock availability or lead-time confirmation from the OEMs, shipping and customs clearance provisions, cutover and rollback arrangements, and identified delivery risks with mitigations. A plan that is not supported by evidence of OEM lead times shall score no more than 2 marks.
Support Responsiveness	2	Committed response and resolution times offered against the 3-year support obligations for Items 1, 2 and 5, and the committed turnaround for the Item 4 penetration test report, where these improve on the minima stated in Section 4.
Total	20	

6.6 General Provisions

- Scores shall be calculated to two (2) decimal places. In the event of a tie-on total score, the bid with the higher Price score shall be preferred; if still tied, the bid with the higher Experience score shall be preferred.
- The Department may seek written clarification from any Bidder during evaluation. Clarifications shall not permit a change to the quoted price, the delivery period, or the substance of the bid.
- A commitment made in a bid and scored under Section 6.4 or 6.5 - including quoted delivery periods, named personnel and support response times - shall be incorporated into the resulting contract as a binding obligation.
- The Department reserves the right to accept or reject any or all bids, and to annul the bidding process at any time prior to contract award, without incurring any liability to Bidders.