DEPARTMENT OF NATIONAL REGISTRATION

REQUEST FOR PROPOSAL

RFP 2023-03

(IUL)133-AS/133/2023/42

Announcement Date

04- September -2023

Proposal Submittal Due Date

13- September-2023

(11:15)

To

Department of National Registration

Velaanaage, 4th Floor

Ameer Ahmed Magu

Male'

RFP 2023-03

Definitions

RFP	Request for Proposal
DNR	Department of National Registration

Introduction

The Department of National Registration (DNR) intends to purchase hardware equipment's specified in this RFP. This RFP is not an offer to purchase but is a request to receive proposals.

DNR reserves the right to accept or reject any or all responses, as well as the right to negotiate with one or more, or none of the responding vendors. Omissions, alterations, or irregularities of any kind shall constitute sufficient cause for rejection of a proposal. DNR reserves the right to advertise for new proposals if, in its judgment, the best interests of the department will be served.

It is the responsibility of each vendor to be aware of, and comply with, all relevant laws. All proposals submitted will be properties of DNR and is not, and will not be, responsible for any costs incurred by the vendor in preparations of the proposal.

- **Bidders are required to direct all the questions to:**
  Email: procurement@dnr.gov.mv

SCOPE OF WORK

Request for Proposal (RFP) for Advanced Endpoint Security Solution and Windows Server Auditing Software

1. Introduction

Department of National Registration is seeking a desirable vendor to provide an advanced endpoint security solution that offers comprehensive protection for 100 endpoint devices and 50 server devices. Additionally, we are also seeking a Microsoft Windows Server security auditing software.

2. Technical Requirement and Scope of Work

The scope of work includes supply, installation, configuration, and integration of the advanced endpoint security solution and Microsoft Windows Sever security auditing software. The vendor must provide training and support during and after the implementation. The project and all related services shall be delivered in maximum 20 Days. The proposed solution must comply with all the features and specifications listed below:

#	Requirements	Technical Compliance, Reference and Relevant Part Number
1	**Advanced Endpoint Security**	
	Antivirus Protection: • Real-time scanning and protection against known and unknown malware, viruses, trojans, and other threats. • Behavioral analysis to detect and block fileless attacks. • Automatic updates and virus signature updates.	
	Firewall Protection: • Protection against unauthorized access to the network and devices. • Centralized management of firewall rules and policies.	
	Device Control:	

#	Requirements	Technical Compliance, Reference and Relevant Part Number
	• Ability to control access to devices such as USB drives and external hard drives. • Whitelisting and blacklisting of devices. • Centralized management of device policies.	
	Web Protection: • Protection against web-borne threats, including malicious websites and drive-by downloads. • URL filtering and blocking of malicious sites. • Behavioral analysis to detect and block fileless attacks. • Centralized management of web policies.	
	Centralized Management: • Ability to manage all devices from a central console. • Management console can be either secure cloud console or on-premise console • Real-time monitoring of device status and security events. • Role-based access control.	
	Reporting: • Detailed reporting of security events and device status. • Customizable reports and alerts.	
	Virtualization Security: • Protection for virtualized environments. • Centralized management of virtualization policies.	
	Advanced Threat Detection: • Detection and prevention of advanced threats, including zero-day attacks and file-less malware. • Behavioral analysis to detect and block fileless attacks. • Machine learning and artificial intelligence to identify and block advanced threats.	
	Endpoint Detection & Response (EDR): • Ability to detect and respond to advanced threats, including threat hunting, incident investigation, and automated response. • Fileless Malware Detection: Ability to detect and prevent fileless malware attacks. • Root Cause Analysis: Ability to identify the root cause of security incidents. • Threat Hunting: Ability to proactively search for and identify security threats. • Incident Investigation: Ability to investigate security incidents. • Automated Response: Ability to automatically respond to security incidents. • Live Response: Ability to take real-time actions on endpoints to contain and remediate security incidents.	

#	Requirements	Technical Compliance, Reference and Relevant Part Number
	• Indicators of Compromise (IOC): Ability to identify indicators of compromise and track them across endpoints. • User Behavior Analysis: Ability to identify anomalies in user behavior that could indicate a security threat. • Network Traffic Analysis: Ability to analyze network traffic for indicators of compromise. • Application Control: Ability to control the behavior of applications on endpoints to prevent malicious activity. • Vulnerability Assessment: Ability to identify vulnerabilities on endpoints and prioritize remediation. • Forensics: Ability to collect and analyze forensic data to aid in incident response and investigations.	
	Mobile Device Management (MDM): • Ability to manage and secure mobile devices such as smartphones and tablets. • Centralized management of mobile device policies. • Mobile device encryption and containerization. • Application control and blacklisting/whitelisting.	
	The solution shall be compatible with our existing network and perimeter firewalls which are Fortigate devices and integrate with our Microsoft 365 mail services.	
	The vendor shall provide 3-Year subscription license for 100 endpoint device licenses and 50 server device licenses for the solution.	
	The vendor shall provide installation, configuration, and any integration services for the solution.	
	The vendor shall provide OEM certified classroom based abroad training for two (02) IT staff on the management and use of the proposed solution.	
	The vendor shall provide 3-Year technical support and maintenance for the solution, including updates and upgrades.	
2	**Installation, Configuration and Training for Advanced Endpoint Security**	
	<u>Project Team</u> To ensure successful implementation, the project delivery team must consist of OEM certified engineers who will be onsite for the duration of the installation, and configuration. The project team should include • OEM certified engineers for the proposed Advanced Endpoint Security Solution. • Fortinet certified network security engineers with proven experience who can complement network security and any related configuration that maybe required. These engineers should have the necessary certifications and expertise to ensure that the products are configured correctly and to troubleshoot any issues that may arise during the implementation. The vendor	

#	Requirements	Technical Compliance, Reference and Relevant Part Number
	should provide evidence of the certifications held by the engineers and their relevant experience in similar projects. <u>Required Professional Services</u> • Conduct a site survey to assess the current infrastructure and plan the installation process. • Install and configure the required licenses. • Install and configure the security agents on all 100 endpoint devices and 50 server devices. • Configure policies and rules for the proposed advanced endpoint security products to meet the organization's security requirements. • Configure email security policies and rules to meet the organization's security requirements. • Configure the EDR features to monitor all endpoints and servers, including setting up the incident response process. • Configure any required integration. • Conduct testing and validation to ensure that the products are functioning correctly and meeting the organization's requirements. • Provide end-user training on how to use the products and EDR features effectively. • Document the installation and configuration process, including all settings and configuration changes made during the process.	
3	**Microsoft Windows Server Security Auditing Software**	
	ManageEngine AD Audit Plus Professional Edition for 2 Domain Controllers - 3 Year Subscription ManageEngine AD Audit Plus Addons for 5 Windows Servers – 3 Year Subscription ManageEngine AD Audit Plus Addons for 5 File Servers – 3 Year Subscription Training: The vendor shall provide OEM classroom-based abroad training for two (02) IT staff for ManageEngine AD Audit Plus	
4	**Installation, Configuration and Training for Microsoft Windows Server Security Auditing Software**	
	<u>Required Professional Services</u> • The vendor shall provide installation services for ManageEngine AD Audit Plus, which includes the following standard onboarding service offerings: • Pre-requisites check: The vendor shall verify that the system requirements and pre-requisites for AD Audit Plus are met before starting the installation process. • Configure dedicated VM(s) to install AD Audit Plus and all relevant components. • Configure storage LUN provisioning on HPE MSA storage for the VM • Configure multipathing and high availability for the LUN.	

#	Requirements	Technical Compliance, Reference and Relevant Part Number

	• Installed and configure any required application server and the database server.
	• Install and configure web server with required SSL configuration.
	• Server and domain configuration:
	  - The vendor shall configure the domain, domain controllers, Windows member servers, ADFS, LDAP, FIM, group policy, removable storage, Printer, and Sysmon.
	• File Servers configuration:
	  - The vendor shall configure the file servers to ensure they are compatible with AD Audit Plus.
	• The vendor shall import historic EVT/EVTX files into AD Audit Plus.
	• The vendor shall configure automatic device configuration in AD Audit Plus.
	• Agent deployment: The vendor shall deploy agents on the required systems and perform any necessary agent-level registry changes.
	• Log filtering: The vendor shall configure log filtering to ensure that only relevant logs are collected.
	• Dashboard customization: The vendor shall customize the dashboard to meet the DNR's specific needs.
	• Custom reports and alerts setup: The vendor shall configure custom reports and alerts based on the DNR's requirements.
	• Report schedule creation: The vendor shall create schedules for regular reports to be generated.
	• Security hardening & privacy: The vendor shall configure security hardening and privacy settings in AD Audit Plus, including SSL configuration and single sign-on configuration.
	• Email and SMS server configuration: The vendor shall configure email and SMS server settings in AD Audit Plus.
	• Role-based access control configuration: The vendor shall configure role-based access control in AD Audit Plus to ensure that only authorized users have access to the system.
	• Archive configuration: The vendor shall configure archive settings in AD Audit Plus to ensure that data is stored in compliance with DNR's requirements.
	• Documentation: The vendor shall provide documentation for the installation, configuration, and usage of AD Audit Plus.
	• Training: Provide on the job training on administration and maintenance of the system.
	• User acceptance testing:
	  - The vendor shall perform user acceptance testing to ensure that the system is functioning as expected.
	• Post-implementation health check:	

#	Requirements	Technical Compliance, Reference and Relevant Part Number
	- The vendor shall perform a post-implementation health check to ensure that the system is functioning as expected after the installation.	
5	**Service Level Expectations** • The support service vendor should provide the contact number of a single point of contact to facilitate immediate contact by client's representative and he or she shall be responsible to liaise with all vendors for rectification of faults within the Next Business Day. • Defective equipment shall be replaced by the bidder at his own cost including the cost of transport if any; • The support service vendor shall provide all normal toolkit and test equipment needed for the maintenance services. • System maintenance and support services will include the following activities. ✓ 24 x 7 on-line Support. ✓ Patch updating and major / minor software version upgrading support. ✓ Phone/Email TAC support must be provided during support period ✓ Issue resolution / Onsite Visits within 1 hour of critical security issues reported • Local TAC support plan must be maintaining by the Bidder for 3-Year maintenance period.	

3. Price Form

#	Item Description	Quantity	Unit Price (MVR)	Extended Price (MVR)
1	Advanced Endpoint Security	1 Bundle		
2	Installation, Configuration and Training for Advanced Endpoint Security	1 Service		
3	Microsoft Windows Server Security Auditing Software	1 Bundle		
4	Installation, Configuration and Training for Microsoft Windows Server Security Auditing Software	1 Service		
5	Service Level Expectations	1 Service		
			Sub Total	
			GST 8%	
			Net Total	

Note: ALL LOTS will be evaluated and awarded together.

4. MINIMUM BIDDER'S QUALIFICATION REQUIREMENTS:

2.1. Experience:

The Proposer should provide approach and reference of successful implementation and technical support of similar system and should include descriptions of system implementations they have completed. The mentioned project references must include names and contact information of the respective clients.

2.2. Manufacturer's Authorization Letter / Certificate:

Bidder that does not manufacture or produce the Goods it offers to supply shall submit the Manufacturer's Authorization Letter or Certificate, to demonstrate that it has been duly authorized by the manufacturer or producer of the Goods/Services to supply these Goods/Services in the Maldives.

2.3. Completed similar projects (Value above MVR 30,000.00):

The bidder shall provide reference letter / documents of successful completion of similar system (endpoint security, network security, security monitoring, security auditing) within last five (5) years. The mentioned project references must include names and contact information of the respective clients, if requires the client can contact and verify the project summaries. The submitted reference documents shall be complying the followings:

- Document shall be from the client (signed and stamped)
- Client opinion on regarding the vendor performance and completion of the project.
- Project names and project value

2.4. Team Composition for Technical Support:

It is mandatory that the vendor will maintain the required technical team as deemed as suited based on the requirements and milestones. However, the client expects that the proposer would have allocated the following more team compositions having specific skill sets and professional experience. Importantly it is expected that the vendor will maintain necessary resources for on-site technical support during crucial stages of the project that requires closer interaction with the client during installation, configuration, integration, training, testing, etc. The bidder **MUST** have a full time Vendor Certified Professional/Engineer under its payroll.

The bidder shall submit the following documents:

- Certifications copy of the relevant training.
- ID card OR Passport Copy of the engineer

5. EVALUATION CRITERIA

5.1 Evaluation of the bid shall be based on the following marking criteria.

Criteria	Marks
Price with GST *(marks break down below)*	75%
Delivery *(marks break down below)*	5%
Technical *(marks break down below)*	20%
Total	100%

Price:

5.1.1 Each bidder's price is used to identify their relative position on a 0 – 75 price scale. This is done by allocating the lowest priced bid 75 points and calculating the remaining bidder's score in relation to this scale.

5.1.2 Price percentage = 75 x (lowest price / bid price)

Delivery:

5.1.3 Each bidder's Delivery is used to identify their relative position on a 0 – 5 price scale. This is done by allocating the lowest Delivery bid 5 points and calculating the remaining bidder's score in relation to this scale.

5.1.4 Delivery percentage = 5 x (Lowest Delivery / Bid Delivery)

5.1.5 The maximum delivery period shall be 90 days from the date of confirmation.

Technical (marks break down below)

Technical Criteria Detail	Marks
Completion of the Technical Proposal including supporting documents	Mandatory
Service Level Expectations	Mandatory
Trained/Qualified staff (Team Composition)	Mandatory
Completed Similar Systems and Support Services Projects *Reference letters or completion certificate:* - 2 points for each reference letter / completion certificate signed and stamp by client - Completed similar systems and projects (value above MVR 30,000.00 per project) within the last five (5) years. - Reference letter(s) for successful completion of similar system (endpoint security, network security, security monitoring, security auditing)	20%
Total	20%