



NATIONAL LIBRARY OF SOUTH AFRICA

228 Johannes Ramakhoase Street
Private Bag X397
Pretoria
0001

5 Queen Victoria Street
Cape Town
8001

TERMS OF REFERENCE FOR THE PROCUREMENT OF CYBERSECURITY ANTI DATA EXFILTRATION(ADX) SOLUTION (150 SEATS LICENCED FOR 12 MONTHS)

CLOSING DATE: 18 November 2024

TIME: 11:00

NB. Should you want to submit quotation, please submit to the email: Quotations@nlsa.ac.za

1. BACKGROUND

The National Library of South Africa (NLSA) is a premier African institution tasked with the collection, preservation, and dissemination of South Africa's national documentary heritage. As a custodian of this heritage, NLSA promotes awareness, appreciation, and access to published works both nationally and internationally, contributing significantly to the country's cultural development and prosperity. The NLSA operates from its campuses located in Pretoria and Cape Town.

2. SCOPE OF WORK

2.1. NLSA seeks to appoint a qualified service provider to procure a comprehensive cybersecurity solution aimed at preventing data exfiltration and enhancing the overall security posture of the organization.

2.2. Solution Configuration and Setup

The proposed cybersecurity solution must incorporate the following key capabilities:

2.3. Ransomware Prevention

Ransomware is one of the most significant threats facing organizations today, particularly those with valuable data and intellectual property. The solution must provide:

- 2.3.1. Real-Time Threat Detection: Implement advanced detection mechanisms that identify ransomware behavior in real time. This includes monitoring for unusual file access patterns, unexpected file encryption activities, and unauthorized changes to critical data.
 - 2.3.2. Automated Response Mechanisms: The solution should offer automated response protocols that isolate infected systems from the network upon detection of ransomware activity, thereby preventing further spread and damage.
 - 2.3.3. Regular Backups and Recovery Solutions: Ensure that there are robust data backup solutions in place that regularly back up critical data, allowing for quick restoration in the event of an attack. These backups should be stored securely and be readily accessible for recovery purposes.
 - 2.3.4. User Education and Awareness Training: Provide comprehensive training for all employees to recognize phishing attempts and suspicious links, which are common entry points for ransomware attacks. This includes simulated phishing exercises and ongoing security awareness programs.
- Data Privacy - Visibility into the unauthorised collection and transmission of user data across every device, within and beyond the NLSA's network.

2.4. Anti-Data Exfiltration

To protect sensitive information from unauthorized access and leakage, the solution must encompass:

- 2.4.1. Endpoint Protection: Deploy comprehensive endpoint protection solutions that monitor and control data transfers from all devices connected to the network. This includes establishing policies that restrict data movement based on user roles and device security status.
- 2.4.2. Data Loss Prevention (DLP) Technologies: Implement DLP solutions that monitor, detect, and respond to potential data exfiltration activities. This includes the use of machine learning algorithms to identify and flag unusual data transfer patterns, such as large file uploads or emails sent to unauthorized external recipients.
- 2.4.3. Network Monitoring and Analytics: Continuous monitoring of network traffic to detect anomalies that may indicate data exfiltration attempts. This includes analyzing data flow for any unauthorized access or unusual behavior and generating alerts for immediate investigation.
- 2.4.4. Geofencing and Location-Based Restrictions: Implement geofencing measures that restrict data access and transfer capabilities based on the geographic location of users or devices. This can help mitigate the risk of data exfiltration through unauthorized access points.

2.5. Privacy Protection

Protecting the privacy of individuals and ensuring compliance with data protection regulations is paramount. The solution should include:

2.5.1. User Data Monitoring: Maintain visibility into how user data is collected, stored, and transmitted. This includes monitoring access to personal data and ensuring that data handling practices comply with applicable privacy regulations, such as the Protection of Personal Information Act (POPIA) in South Africa.

2.5.2. Data Anonymization Techniques: Employ data anonymization techniques that obscure personal identifiers, making it difficult to associate data with specific individuals. This is particularly important for data used in analytics or reporting, where privacy must be maintained.

2.5.3. Access Control Mechanisms: Implement strict access control measures that ensure only authorized personnel can access sensitive data. This includes role-based access controls (RBAC), multi-factor authentication (MFA), and regular audits of user permissions.

2.5.4. Incident Response Planning: Develop and maintain a robust incident response plan that outlines steps to take in the event of a data breach or privacy violation. This plan should include immediate notification protocols to inform affected individuals and regulatory bodies as required by law.

2.6. Global Threat Protection

The solution must include robust defenses against various global security threats, including ransomware, spyware, malware, phishing, and unauthorized data profiling and collection.

2.6.1.1. Mitigate the risk of data loss through geofencing

2.6.1.2. Minimise data collection on NLSA's endpoints

2.6.1.3. Prevent unauthorized data collection and profiling

2.6.1.4. Anonymise user behavior

2.6.1.5. Protect remote workers wherever they are

2.6.2. On device data Security:

2.6.2.1. Prevent data loss using behavioral analytics

2.6.2.2. Reduce the surface area exposed to attackers

2.6.2.3. Access detailed reporting and analysis of threat vectors

2.6.2.4. Lower the cost of compliance

2.6.2.5. Detect network anomalies through anti data exfiltration

2.6.3. Enterprise Console:

- 2.6.3.1. Must consist of endpoint agents and enterprise cloud console used to manage groups of devices and provide a centralized view of all threats and events.
- 2.6.3.2. Console must provide insights into the origin of threats within the NLSA's network environment.
- 2.6.3.3. Analytics to provide detailed impact assessment
- 2.6.3.4. Threat hunting for detailed insight into each threat including crowdsourced impact, confidence level and MITRE classification
- 2.6.3.5. Dark Web breach reporting for monitoring domains for data breaches.

2.7. KEY BENEFITS OF THE PROPOSED SOLUTION

2.7.1. On-Device Data Privacy

- 2.7.1.1. Mitigate risks of data loss through geofencing techniques.
- 2.7.1.2. Minimize unauthorized data collection on NLSA's endpoints.
- 2.7.1.3. Anonymize user behavior and protect remote workers across locations.

2.7.2. On-Device Data Security

- 2.7.2.1. Employ behavioral analytics to prevent data loss.
- 2.7.2.2. Reduce exposure to potential attacks through strategic security measures.
- 2.7.2.3. Enable detailed reporting and analysis of threat vectors.
- 2.7.2.4. Facilitate compliance through cost-effective security strategies.
- 2.7.2.5. Detect network anomalies via anti data exfiltration protocols.

2.7.3. Enterprise Console

- 2.7.3.1. Provide an integrated management console for overseeing endpoint agents and offering centralized threat monitoring.
- 2.7.3.2. Insights into the origins of threats within the NLSA network.
- 2.7.3.3. Advanced analytics for impact assessments and threat hunting.
- 2.7.3.4. Dark web breach reporting for monitoring domains susceptible to data breaches.

2.7.4. Training Requirements

Training must be provided for five administrators, covering the following:

- 2.7.4.1. Navigating the management console
- 2.7.4.2. Adding and managing users and groups
- 2.7.4.3. Device integration
- 2.7.4.4. Overview and effective utilization of all console elements
- 2.7.4.5. Provision of comprehensive training manuals for reference.
- 2.7.4.6. Training may be conducted virtually

3. NLSA'S RIGHTS

- 3.1. The NLSA is entitled to amend any RFQ conditions, RFQ validity period, RFQ terms of reference, or extend the RFQ's closing date, all before the RFQ closing date.

4. DURATION OF THE PROJECT

- 4.1. The appointed service provider shall make an undertaking that the delivery shall be concluded within 30 days after issuing the Purchase Order.

5. CONDITIONS OF RFQ

- 5.1. The NLSA reserves the right not to accept the lowest proposal.
- 5.2. The NLSA reserves the right to appoint one or more Bidders.
- 5.3. The NLSA reserves the right not to award the contract.
- 5.4. The NLSA reserves the right to have any documentation, submitted by the successful Bidder checked or inspected by any other person or organization.
- 5.5. The NLSA will not be held responsible for any costs incurred by the Bidder in the preparation and submission of the RFQ.
- 5.6. No upfront Payment will be done by NLSA.
- 5.7. Delivery of one 86-inch multimedia device must be done at the NLSA Cape Town campus and the other 86 inch and 65-inch device to be delivered at the Pretoria campuses.
- 5.8. The quotation is valid for a period of 30 days and may be extended at the discretion of the NLSA.

6. EVALUATION CRITERIA

- 6.1. **Pre evaluation (standard bid documents)**

6.1.1. Fully completed SBD 4 and SBD 6.1, forms.

6.2. Mandatory:

6.2.1. **Bidder to produce letter/certificate stating that the bidder is authorized to provide the proposed solution.**

6.2.2. **Datasheet for the solution proposed to ensure that all requirements are met.**

6.2.3. **Qualifications for Project Roles**

Cyber Security Engineer – Provide a detailed CV to support the below requirements:

Education: National Diploma in Information Technology or equivalent.

Experience: Minimum of 5 years in cybersecurity, with a focus on data protection and threat mitigation.

Certifications:

- CompTIA Security+
- Certified Information Systems Security Professional (CISSP) or Systems Security Certified Practitioner (SSCP) or Certified Ethical Hacker (CEH)

Skills:

- Comprehensive knowledge of cybersecurity threats and prevention methods.
- Experience with anti-data exfiltration technologies and solutions.
- Ability to conduct security assessments and develop incident response strategies.
- Proficient in configuring and managing security systems and tools.

6.2.4. **The following table will be used to evaluate the bidder against the proposed solution. Bidder must tick the applicable functional requirements for their proposed solution. Bidders who fail to meet all the technical requirements would not be considered for the pricing evaluation stage.**

Requirement	Yes/No
Configuration and setup	
Anti-Data Exfiltration	
Data Privacy	

Breach Prevention	
Administrator training	
On device data privacy	
On device data Security	
Enterprise Console	

6.3. Preference Point System

In terms of Regulation 5 of the Preferential Procurement Regulations of 2022/23, Gazette Number 47452 dated 4 November 2022 pertaining to the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000), responsive bids will be adjudicated by the State on the 80/20-preference point in terms of which points are awarded to bidders based on: -

- The bid price (maximum 80 points)
- Specific Goals (maximum of 20 points):

The following formula will be used to calculate the points out of 80 for price in respect of an invitation for a tender, inclusive of all applicable taxes.

$$P_s = 80 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

Where-

P_s = Points scored for price of tender under consideration;

P_t = Price of tender under consideration; and

P_{min} = Price of lowest acceptable tender.

- Specific Goals (maximum of 20 points): 100% Black owned (20 points), 10 points for other than 100% black owned.

6.4. Evaluation Criteria Stage 2: Pricing

6.4.1. Quotation must provide a pricing schedule which clearly sets out the cost of providing the services including any applicable charges.

6.4.2. The pricing schedule must clearly indicate the unit or item price as well as total price for the requested.

6.4.3. All cost items must be inclusive of VAT.

6.5. Pricing schedule for NLSA Cybersecurity Solution

Item	Description	Unit Cost (ZAR)	Quantity	Total Cost (ZAR)
1. Solution Procurement				
1.1. Anti-Data Exfiltration Solution	Comprehensive anti-data exfiltration software and licenses			
1.2. Ransomware Prevention Software	Comprehensive ransomware protection software and licenses			
1.3. Data Loss Prevention (DLP)	DLP solution licenses and implementation			
2. Configuration and Setup				
2.1. Initial Configuration	Setup of cybersecurity solutions and integration into existing systems			
2.2. Customization	Tailoring the solutions to fit NLSA's specific needs			
3. Training				
3.1. Administrator Training	Training for m administrators on solution navigation and management			
3.2. Training Manuals	Comprehensive training manuals for administrators			
4. Maintenance and Support				
4.1. Annual Maintenance	Yearly maintenance and support services for the cybersecurity solution			
4.2. Technical Support	Ongoing technical support and troubleshooting			
6. Total Project Cost				

7. ENQUIRIES

All enquiries regarding this RFQ must be directed to the SCM Office:

For any RFQ related enquiries please sent to the following email address quoting the RFQ Reference Number, Bid. Description as a Reference; lorraine.mongwe@nlsa.ac.za and quotations@nlsa.ac.za OR (012) 401 9766