REQUEST FOR TENDERS

RFT: 2021/087
File: AP_9/7/1/1
Date: 17 November, 2021
To: Interested suppliers
From: Christian Slaven, IT Manager

Subject: **Request for Tenders: Enterprise Endpoint Security Solution**

1. Background

1.1. The Secretariat of the Pacific Regional Environment Programme (SPREP) is an intergovernmental organisation charged with promoting cooperation among Pacific islands countries and territories to protect and improve their environment and ensure sustainable development.

1.2. SPREP approaches the environmental challenges faced by the Pacific guided by four simple values. These values guide all aspects of our work:

- We value the Environment
- We value our People
- We value high quality and targeted Service Delivery
- We value Integrity

1.3. For more information, see: www.sprep.org.

2. Specifications: statement of requirement

2.1. SPREP would like to call for tenders from prospective vendors who can provide next-generation threat detection and prevention enterprise endpoint security solutions to strengthen the protection of its systems for a period of 2 or 3 years.

2.2. The successful applicant will provide products and services as identified in the Terms of Reference (attached as Annex 1) and in consultation with SPREP IT.

2.3. The successful consultant must supply the services to the extent applicable, in compliance with SPREP's Values and Code of Conduct. https://www.sprep.org/attachments/Publications/Corporate_Documents/sprep-organisational-values-code-of-conduct.pdf

3. Conditions: information for applicants

3.1. To be considered for this tender, interested suppliers must meet the following conditions:

i. Address all technical requirements attached in Annex 1

ii. Have an office/distributor/business partner in the Pacific that provides technical support to the Pacific region

iii. Provide 3 references of client companies and organisations with similar size and solutions implemented

iv. Complete the **tender application form** – *(please note you are required to complete all areas in full as requested on the form, particularly the statements to demonstrate you meet the selection criteria – DO NOT refer us to your CV or your Technical Proposal. Failure to do this will result in the application **not** being considered)*; and

v. Sign the **Conflict of Interest** form.

4. Submission guidelines

4.1. Tender documentation should demonstrate that the interested supplier satisfies the conditions stated above and is capable of meeting the specifications and timeframes. Documentation must also include supporting examples to address the evaluation criteria.

4.2. Tender documentation should outline the interested supplier's complete proposal and include:

a. The CVs of proposed personnel highlighting related experience relevant to the tender.
b. A Financial Proposal which breaks down costs for all components and outlines two options – 2 years and 3 years.
c. A Completed Tender Application Form and conflict of interest form.

4.3 Tenderers/Bidders must insist on an acknowledgement of receipt of tenders/proposals/bids.

5. Tender Clarification

5.1. Any clarification questions from applicants must be submitted by email to procurement@sprep.org before 30 November 2021. A summary of all questions received with an associated response will be posted on the SPREP website www.sprep.org/tender by 02 December 2021.

6. Evaluation criteria

6.1. SPREP will select a preferred supplier on the basis of SPREP's evaluation of the extent to which the documentation demonstrates that the tenderer offers the best value for money, and that the tenderer satisfies the following criteria.

i. Product core functionality – advance and next-generation protection from malware, ransomware and exploits (20%)

ii. Administration – Central Management Console, integrates with AD, policy management, deployment (10%)

iii. Run on all devices – all platforms, servers and PC's, all OS etc. (10%)

iv. Product performance - scope, speed (scans, updates), reliability (20%)

v. Technical Support– ease in submitting cases, response times, intuitive services (chat, online help) (10%)

vi. Other capabilities (e.g. browser protection, stats, usage notifications etc.) (10%)

vii. Financial proposal – **outlining two options – 2 years and 3 years** (20%)

7. Deadline

7.1. The due date for submission of the tender is: **09 December 2021 midnight (Apia, Samoa local time).**

7.2. Late submissions will be returned unopened to the sender.

7.3 Please send all tenders clearly marked '**RFT 2021/087: SPREP Enterprise Endpoint Security.**' to one of the following methods:

Mail: SPREP
Attention: Procurement Officer
PO Box 240
Apia, SAMOA
Email: tenders@sprep.org (MOST PREFERRED OPTION)
Fax: 685 20231
Person: Submit by hand in the tenders box at SPREP reception,
Vailima, Samoa.

Note: Submissions made to the incorrect portal will not be considered by SPREP. If SPREP is made aware of the error in submission prior to the deadline, the applicant will be advised to resubmit their application to the correct portal. However, if SPREP is not made aware of the error in submission until after the deadline, then the application is considered late and will be returned unopened to the sender.

SPREP reserves the right to reject any or all tenders and the lowest or any tender will not necessarily be accepted.

For any complaints regarding the Secretariat's tenders please refer to the Complaints section on the SPREP website
http://www.sprep.org/accountability/complaints

Annex 1

Terms of Reference

SPREP Enterprise Endpoint Security

SPREP is going to review leading Enterprise Endpoint solutions available in the market to ensure the most effective solution is implemented at SPREP.

SPREP is seeking from vendors quotations to provide the following core services

1. Endpoint protection

In addition, the above core services are broken down further to specific evaluation criteria's below with suggestions but not limited to these:

i.	**Product core functionality – advanced and next generation protection from malware, ransomware and exploits**
ii.	**Administration** **a. Policy Management** **b. Analytics** **c. Central Admin Console** **d. Deployment from Console** **e. Active Directory integration**
iii.	**Run on all devices (all platforms and operating systems, computers, and servers)**
iv.	**Product performance and security below but not limited to** **a. Intuitive threat detection methods,** **b. Low resource utilization,** **c. Easy deployment of client,** **d. Regular updates,** **e. On-access scans**
v.	**Product support** **a. Ease in submitting cases** **b. Responsive** **c. Intuitive services such as Online Chat**
vi.	**Other Capabilities** **a. Web Browser Protection** **b. Statistics** **c. Usage Notifications** **d. Or any other relevant feature**
vii.	**Financial proposal – outlining two options – 2 years and 3 years**