SOUTH AFRICAN TOURISM

REQUEST FOR INFORMATION – INFORMATION SECURITY SOLUTIONS UPGRADE

THE ORGANISATION AND OPPORTUNITY

South African Tourism (SAT) is a Schedule 3A Public Entity, listed in terms of the Public Finance Management, 1999 (Act No. 1 of 1999), and it is accountable to the Minister of Tourism. SAT is a public entity established in terms of section 2 of the Tourism Act, 2014, (Act No. 72 of 2014). In line with its mandate, SAT receives funds for its operations from government.

SAT's business includes three distinct areas of business focus and delivery, with different target markets and segments:

I. International Leisure Tourism (travel trade and consumer); and Domestic Leisure Tourism (travel trade and consumer);
II. Business events through the delivery unit the South African National Convention Bureau (Meetings, Incentives, Conferences, Exhibitions); and
III. Quality Assurance of Tourism establishments through the delivery unit the Tourism Grading Council of South Africa.

Scope of services

SA Tourism is embarking on the initiative for the Upgrade of its Information Security Systems, which will help reduce the risk arising from the use of technology within the organization.

SA Tourism is a global organization that relies heavily on automated business processes to ensure efficiency in its operations. SA Tourisms operates its head office in South Africa with a centralized ICT environment where SAT users and clients from all over the world have secured access to its websites and applications

Through this RFI SA Tourism is seeking proposals from reputable Information Security Solution providers for Upgrade, support and maintenance of Information Security Systems of SA Tourism's Information Systems, Digital platforms, including websites and related digital applications for a period of 3 years.

SA Tourism makes use of various technologies and hosting partnerships in order to deliver its content to the user base in South Africa and across the world, with a user base of **200 users**.

SA Tourism is looking for Information Security solutions, which will help it to achieve:

- An overall best practice security for SA Tourism's systems
- Improved Data and Systems Security
- Increased operational efficiency and reporting on Security insights within all internal systems

- Improved management control and corporate governance for security within the organization.

SA Tourism is looking for a Bundled Information Security Systems Solution that should have information sources completeness, accuracy, reliability, quality and standard automated data and information security processing capabilities but not limited to the following:

- **Network Access Control solution** – This is to address the risk arising from unauthorised devices connecting to the SA Tourism network, thereby exposing it to compromise. The solution should allow for the definition and enforcement of granular network access control policies and offer appropriate measures for dealing with non-compliant and unauthorised devices in such a way that the risk introduced by such devices is effectively dealt with. In this context' 'network' refers to both wired and wireless networks and 'devices' refers to both traditional technology devices and enterprise IoT (Internet of Things) devices.

- **Security Configuration Management Solution** – this solution should enable SA Tourism to define, enforce and report on approved security baselines for multiple asset classes (server endpoints, workstation endpoints, hypervisors, application servers, database platforms and other components) within the technology environment. It should allow for easy baseline building by allowing the editing of templates derived from CIS Benchmarks or similar standards.

- **Privileged Access Management (PAM) solution** – this solution should facilitate the effective monitoring of privileged accounts across SA Tourism. The solution should be able to flag potential abuses of privileged identities, enable audits on the use of privileged identities and provide any other functionality that ensures that the risk from the abuse of privileged identities is minimised. The solution should be able to work with all the authentication systems deployed at SA Tourism.

- **Endpoint Detection and Response (EDR) Solution** – Solution should provide endpoint protection and response capability preferably not based on static signatures, but rather on AI/ML techniques. Should be deployable to on-prem and cloud assets and be managed centrally as well as being able to run on all the company's endpoints (Windows, Android, Apple IoS, Apple macOS, Linux). The solution should provide 'persistent' protection regardless of whether the endpoint in question is currently connected to the SA Tourism network or not.

- **Next-Generation Firewall (NGFW) Solution** – solution should provide boundary network protection and have integrated IPS (Intrusion Prevention Solution), DNS Filtering, Application Awareness, VPN (IPSec & TLS), Malicious Content Filtering and Sandboxing capability that can effectively manage threats to SA Tourism's network. Cloud usage monitoring and control functionality will provide an added advantage.

- **Security Information and Event management (SIEM with integrated UEBA functionality) Solution** – the solution should facilitate the collection, aggregation, and analysis of log events from SA Tourism's technology estate. It should facilitate the easy building of correlation/detection rules for quick and effective incident detection. The solution should have in-built User & Entity Behaviour Analytics (UEBA) functionality. The solution should have flexible licensing modes including those based on the number of managed IP addresses and not just log volumes. The solution should have both soft appliance (virtual) and hardware appliance deployment options. The solution should have the capability to connect to and process log events from common cloud sources. Implementation of this solution will also require the definition and operationalisation of the initial SIEM Business Use Cases.

- **Vulnerability Management Solution** – the solution should facilitate the regular scanning of technology assets to identify and manage vulnerabilities as well as maintaining a detailed real-time asset inventory database. The solution should expedite the quick remediation of vulnerabilities by allowing the creation of risk-based (asset criticality, vulnerability priority (CVSS Score) and other criteria) prioritisation measures for all assets. Both cloud and on-prem deployment options will be considered. The solution should be able to scan both cloud and on-prem assets.

Additional Requirements:

- Training –The prospective bidder provider should have the ability to provide OEM Training on all solutions provided to the SA Tourism ICT team
- Maintenance and Support - Although the SA Tourism ICT would be administering and monitoring the systems, but the winning bidder would be expected to support the system through an SLA with reporting as per business requires

Notes:

Please note that there will be a closed tender RFP for the respondents of this RFI

Above mentioned tender or supplier solution sourcing-related processes should be complaint to Public Finance Management Act requirements.

The above listed processes/requirements are generic, not necessarily specific to SA Tourism.

The solution must provide the above-listed features and not limited as available solutions offers more detailed functionality as per the requirements.

This notice is aimed at gauging the market for potential firms which can provide for the Upgrade, Support and Maintenance of Information Security Systems for South African Tourism for a period of 3 years.

Services providers who specialises in these services are required to forward their contact details, company profiles, proof that they are rendering these services to at least 3 other contactable clients, Financial Proposal and proof that you are successfully registered on National Treasury's Centralised Supplier Database (CSD) using this URL https://e-procurement.southafrica.net by no later than **Monday 16 November 2020 at 12h00.**

It must be noted that responses to this notice are not offers and South African Tourism does not intend to award a contract based on the responses to this notice, to pay for any information submitted, or for the use of such information. South African Tourism may invite suppliers for presentations and thereafter issue a Request for Proposal/Quotations (RFP/RFQ) for Information Security System. Furthermore, this notice shall not limit any rights of SA Tourism, and SA Tourism reserves all its rights including but not limited to its rights to elect not to procure the solutions that are the subject of this notice and its right to procure them from a vendor that has not responded to this notice.