



STATE INFORMATION TECHNOLOGY AGENCY (SOC) LTD

Registration number 1999/001899/30

BID SPECIFICATION

RFA REF. NO:	RFA 2494-2021
DESCRIPTION	REQUEST FOR ACCREDITATION FOR INFORMATION SECURITY PRODUCTS AND SERVICES TO SITA AND ON BEHALF OF GOVERNMENT DEPARTMENTS FOR A PERIOD OF FIVE (5) YEARS
PUBLICATION DATE:	24 NOVEMBER 2021
NON-COMPULSORY VIRTUAL BRIEFING SESSION	DATE: 01 DECEMBER 2021 TIME: 10:00 AM (SOUTH AFRICAN TIME) LINK: Click here to join the meeting
CLOSING DATE FOR QUESTIONS / QUERIES	08 DECEMBER 2021 TIME: 16:30 PM (SOUTH AFRICAN TIME)
RFB CLOSING DETAILS	DATE: 15 DECEMBER 2021 TIME: 11:00 AM (SOUTH AFRICAN TIME) Venue: Tender office, Pongola in Apollo, 459 Tsitsa Street, Erasmuskloof, Pretoria (Head office)
PUBLIC OPENING OF RFB RESPONSES	N/A
RFB VALIDITY PERIOD	120 DAYS FROM THE CLOSING DATE

PROSPECTIVE BIDDERS MUST REGISTER ON NATIONAL TREASURY'S CENTRAL SUPPLIER DATABASE PRIOR TO SUBMITTING BIDS.

Contents

ANNEX A: INTRODUCTION	4
1. PURPOSE AND BACKGROUND	4
1.1. PURPOSE	4
1.2. BACKGROUND	4
1.3. PROPOSED CONTRACTING AND ENGAGEMENT MODEL	4
2. SCOPE OF BID	5
2.1. SCOPE OF WORK	5
2.2. CUSTOMER CURRENT INFRASTRUCTURE AND ENVIRONMENT	5
3. TECHNICAL REQUIREMENT OVERVIEW	5
3.1. GENERAL	5
3.2. END POINT PROTECTION	6
3.3. END POINT DETECTION AND RESPONSE	7
3.4. FIREWALL	8
3.5. DIGITAL SIGNATURE	10
3.6. ELECTRONIC MAIL PROTECTION, ARCHIVE AND JOURNALING	11
3.7. WEB APPLICATION PROTECTION (WAP) AND PROXY SERVICE	12
3.8. INTRUSION DETECTION AND PREVENTION TECHNICAL REQUIREMENTS OVERVIEW	14
3.9. DATA LOSS/LEAKAGE PREVENTION	16
3.10. VULNERABILITY MANAGEMENT	19
3.11. IDENTITY AND ACCESS MANAGEMENT	20
4. BID EVALUATION STAGES	22
ANNEX A.1: ADMINISTRATIVE PRE-QUALIFICATION	23
5. ADMINISTRATIVE PRE-QUALIFICATION REQUIREMENTS	23
5.1. ADMINISTRATIVE PRE-QUALIFICATION VERIFICATION	23
5.2. ADMINISTRATIVE PRE-QUALIFICATION REQUIREMENTS	23
ANNEX A.2: TECHNICAL MANDATORY REQUIREMENTS	24
6. TECHNICAL MANDATORY	24
6.1. INSTRUCTION AND EVALUATION CRITERIA	24
6.2. APPROVAL PROCESS	24
6.3. TECHNICAL MANDATORY REQUIREMENTS	25
THE BIDDER NEEDS TO ACCEPT ALL THE SPECIAL CONDITIONS OF CONTRACT BY COMPLETING THE DECLARATION OF ACCEPTANCE IN SECTION 9.3 AND ATTACH IT AS PART OF THE BID SUBMISSION.	27
THE BIDDER NEEDS TO COMPLETE THE RATE CARD OF AREA OF EXPERTISE ANNEX D ADDENDUM 2 AS PER THE REQUIREMENTS INDICATED IN ANNEX A4, SECTION 10.	27
7. TECHNICAL FUNCTIONALITY (NON-MANDATORY SPECIFICATIONS)	28
7.1. TECHNICAL FUNCTIONALITY REQUIREMENTS	28
8. PROOF OF CONCEPT REQUIREMENT	28
ANNEX A.3: SPECIAL CONDITIONS OF CONTRACT (SCC)	29
9. SPECIAL CONDITIONS OF CONTRACT	29
9.1. INSTRUCTION	29
9.2. SPECIAL CONDITIONS OF CONTRACT	29
9.3. DECLARATION OF ACCEPTANCE	36
ANNEX A.4: COSTING AND PRICING	37

10.1 COSTING AND PRICING EVALUATION	37
10.2 COSTING AND PRICING CONDITIONS	37
10.3 RATE CARD OF AREA OF EXPERTISE.....	38
10.4 DECLARATION OF ACCEPTANCE.....	38
ANNEX A.5: TECHNICAL SCHEDULES	39
11. TECHNICAL SCHEDULES	39
ANNEX A.6: TERMS AND DEFINITIONS	40
12. ABBREVIATIONS	40
13. DEFINITIONS.....	41
ANNEX B: BIDDER SUBSTANTIATING EVIDENCE	42
14. MANDATORY REQUIREMENT EVIDENCE.....	42
THE BIDDER NEEDS TO ACCEPT ALL THE SPECIAL CONDITIONS OF CONTRACT BY COMPLETING THE DECLARATION OF ACCEPTANCE IN SECTION 9.3 AND ATTACH IT AS PART OF THE BID SUBMISSION.....	44
THE BIDDER NEEDS TO COMPLETE THE RATE CARD OF AREA OF EXPERTISE ANNEX D ADDENDUM 2 AS PER THE REQUIREMENTS INDICATED IN ANNEX A4, SECTION 10.	44

ANNEX A: INTRODUCTION

1. PURPOSE AND BACKGROUND

1.1. PURPOSE

The purpose of this Request for Accreditation (RFA) is to invite Suppliers (hereinafter referred to as “bidders”) to submit bids to establish an Information Security Panel of Service Providers for the supply of information security products and services to SITA and on behalf of Government Departments for a period of five (5) years.

1.2. BACKGROUND

The industry shift in response to the 4IR point to an urgent need to establish mechanisms to monitor and respond to real and specifically-directed threats to the confidentiality, integrity and availability of information and assets. The threats, risks and attack vectors referred to in this document are not generalized, but are specific to SITA and the South African Government.

SITA’s mandate is to improve Government’s service delivery to the public through the provisioning of information technology, information systems and related services in a secured environment to Government Departments and Public Entities. This can be achieved by enabling the Government Departments to timeously and conveniently procure Information Security products and services, and at Government preferred prices.

As part of the deliverables, the RFA must ensure that the SITA Act and National Treasury Regulations are followed by requiring that all equipment and services be SITA-certified.

There is a lack of an effective, efficient, and cost-effective mechanism for the government to procure Information Security Products and services. It is currently conducted in a very disparate approach. As a result, there are multiple Information Security Products and services in the government landscape with minimal standardisation, and long implementation turn-around times due to the prolonged duration of engaging the market to procure the products and services.

SITA has embarked on the establishment of an Information Security Panel for Service Providers for the supply of Information Security products and services to enable SITA and government departments to procure information security solution with a faster turn-around time.

1.3. Proposed contracting and engagement model

Subsequent to award, the contract engagement model will be as follows: SITA will compile a customer user requirement specification and a business case for each customer and follow the SITA engagement model.

Master service agreements will be signed with successful bidders to be placed on the Master Agreement with SITA that will thereafter follow due process in terms of the engagement model.

2. SCOPE OF BID

2.1. SCOPE OF WORK

- (1) The information security products / technologies include the following:
 - (a) End point protection
 - (b) End Point detection and response
 - (c) Firewall
 - (d) Digital signatures
 - (e) Electronic mail protection, archive and journaling
 - (f) Web application protection and proxy services
 - (g) Intrusion detection and prevention
 - (h) Data loss/leakage prevention
 - (i) Vulnerability management
 - (j) Identity and Access Management
- (2) The scope of work to be delivered by the bidders for the categories are:
 - (a) Supply, install and configure the ISS products, including software licenses
 - (b) Maintenance and support (including onsite and remote)
 - (c) Professional services, including planning, design, engineering, audit/assessment, migration services)
 - (d) Solution administrator training (certification)
- (3) The bidders are required to deliver technologies and/or services with regional capability throughout South Africa.

2.2. CUSTOMER CURRENT INFRASTRUCTURE AND ENVIRONMENT

N/A

3. TECHNICAL REQUIREMENT OVERVIEW

3.1. General

- (1) **Interpretation of requirement.** Unless specifically stated otherwise, each requirement statement includes the prefix “The product must...” or “The product must have the capability to ...” as the case may be.
- (2) All products must be MIOS compliant.
- (3) All products should be aligned with MISS requirements.

3.2. End point protection

(1) Core functions and features

(a) Protection

- (i) Protecting the endpoint against threats such as file-based and file-less attacks, static and dynamic malware.
- (ii) Deliver protection in the absence of internet connectivity on the same level that when connected to ensure protection services quality and service continuity.
- (iii) Provide access support of “Least privilege” management.
- (iv) Extended application control capability to include:
 - 1) The workflow for users requesting unknown applications to provide sufficient context for administrators to make educated decisions.
 - 2) Application-focused data protection to support policy-based configuration.
 - 3) Policy definition to dictate what data users can access from specific applications and or network storage.
 - 4) Risk-based policy definition to control whether or not a user or an application has access to a file, depending on, for example, the health of the endpoint and the vulnerability state of the application.
- (v) Multilayer endpoint protection beyond signature detection and blocking ability to utilise signature less technologies as advance machine learning, behavioural analysis, memory exploit mitigating, and emulation with time-tested once intrusion prevention, reputational analysis, application and device control.

(b) Detection and response

- (i) Have threat hunting or data exploration using techniques such as to deploy bait and decoys at scale to lure attackers into revealing their intent, tactics and targets without their knowledge.
- (ii) Review activities that appear suspicious to either human analysts or algorithms, and then pursue those activities until verifying whether they are, in fact, incidents.
- (iii) Use mechanisms such as rule-based detection to identify suspicious-activity, determine its severity scoring using threat-intelligence-based detection.
- (iv) Have ability to in the event of malicious content or behaviour detection provide sufficient information for an analyst to determine the root cause for the event, answering the question, “Where did this file or this behaviour initiate from?”
- (v) Be able to alert identified individuals and/or groups upon detection of suspicious activity that may potentially require additional validation or remediation actions.

(2) Operational Support System / System Administration.

- (a) Centralised management and reporting console and dashboard of real-time events and trending information that enables rapid troubleshooting.
- (b) Visualize trends and patterns of recorded activities to distinguish between normal and anomalous behaviours.

- (c) Have policy configuration for end point devices, including mechanism to present anti-tampering, lockdown configuration, block high risk activities, clean infections and apply remediation to provide a strong resilience against compromise.
- (d) Ability to schedule performance activities to executed unattended during non-business critical hours.
- (e) Policy based configuration, stage rollouts / updates to implement or rollback policies to specified locations and devices.
- (f) Audit log of all events including policy changes and administrative events.
- (g) Mechanisms to deploy and update agents to discovered devices.
- (h) Integration capability with authoritative sources, directory services, incident response systems, etc.
- (i) Role base access management.
- (j) Mechanisms to protect against detected and emerging threats such as quarantine detected threats which cannot be neutralised, deletion of threats of critical risk.
- (k) Alert generation and configurable notification capability.
- (l) Health monitoring for endpoints and agents, such as start-up, shutdown, scanning and updating.
- (m) Distributed for geographical, organizational or performance reasons (for example, to optimize delivery of updates to clients in remote sites).
- (n) Policies and configurations shared across the servers. Servers must provide failover and load-balancing functionality as needed.
- (o) Reports generation concerning malicious activity and anti-malware operations, with ability to filter on report criteria, including system type, endpoint group and user group.

(3) Deployment and integration

- (a) Be deployed and operational on the following ICT common operating environment:
 - (i) End-points: MS Windows, Linux, Android
 - (ii) Back-end server/hosting: On-premise, Private cloud
- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.3. End point detection and response

(1) Core functions and features

- (a) Provide centralised console for collecting, organizing, and analysing data from the endpoints connected to it.
- (b) Conduct endpoint monitoring and collect data such as processes, connections, volume of activity, and data transfers—into a central database.
- (c) Detect potentially malicious behaviours focusing on the tactics and techniques used by modern threat actor.

- (d) Analyse and search detailed endpoint data for traces of malicious activity and actively investigate and respond to suspicious activity.
- (e) Detect the point of initial compromise at an early stage, to trace an attacker across many touched endpoints in an IT environment, and to identify what data is being stolen and how.
- (f) Proactive detection of cybersecurity threats, active cyber hunting, containment and remediation, and incident response to stop the intrusion, thus limiting further damage.
- (g) Identify suspicious application behaviours, raise high-severity alerts and give visual context to an entire chain of events.
- (h) Use pre-configured rules to recognize incoming data that indicates a known type of security breach and triggers an automatic response, such as to log off the end user or send an alert to a staff member.
- (i) Incorporate both real-time analytics, for rapid diagnosis of threats that do not fit the pre-configured rules, and conducting a post-mortem analysis of an attack.
- (j) Detect advanced malware and must discover zero-day malware not detected by the signature-based solutions.

(2) Operational Support System / System Administration.

- (a) Centralised management and reporting console and dashboard of real-time events and trending information that enables rapid troubleshooting.
- (b) Ability to create daily, weekly and monthly executive reports and allow reports export.
- (c) Policy based configuration, stage rollouts / updates to implement or rollback policies to specified locations and devices.
- (d) Audit log of all events including policy changes and administrative events.
- (e) Alert generation and configurable notification capability.
- (f) Distributed for geographical, organizational or performance reasons (for example, to optimize delivery of updates to clients in remote sites).

(3) Deployment and integration

- (a) Be deployed and operational on the following ICT common operating environment:
 - (i) End-points: MS Windows, Linux, Android
 - (ii) Back-end server/hosting: On-premise, Private cloud

Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.4. Firewall

(1) Core Functions and features

- (a) Stateful firewall functionality configured by means of a firewall rule base with network objects and groups.
- (b) Network address translation (NAT) of network traffic.

- (c) Two-tier firewall management implementing role-based administrator access.
- (d) Physical connections, including at minimum 10/100/1000 RJ45 copper, Gigabit Ethernet short range (SR) local connector (LC) small form-factor pluggable (SFPs) and 10 Gigabit Ethernet SR LC (XFPs), must be available so as to accommodate several data centre architectures and paradigms.
- (e) Policy-based controls must utilise application identification, user identification and content identification. The “learning” process results in a form of intelligence that provides next generation firewall policy controls.
- (f) Rule sets must be applicable to ensure and enable the following:
 - (i) Stateful inspection functionality.
 - (i) Anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside).
 - (ii) User permit rules (e.g. allow HTTP to public webserver).
 - (iii) Management permit rules (e.g. SNMP traps to network management server).
 - (iv) Noise drops (e.g. discard OSPF and HSRP chatter).
 - (v) Deny and alert (alert systems administrator about traffic that is suspicious).
 - (vi) Deny and log (log remaining traffic for analysis).
- (g) The protection must be capable to analyse and inspect traffic with the inclusion of encrypted traffic such as SSH or TLS/SSL with no assumptions that such traffic is legitimate.
- (h) Must be capable to analyse packet headers not only on Layer 3 and 4 to allow or block traffic. It must therefore be more application aware verifying traffic on all ports for any application.
- (i) Must detect non-standard port hopping therefore not assuming standard port assigned utilisation.

(2) Operational Support System / System Administration

- (a) Centralized console for policy management.
- (b) "On box" logging and reporting via both a live log viewer and a log analyser/query tool.
- (c) Object-based configuration, with dynamic object support that periodically update, such as block lists and whitelists.
- (d) The management system that allows a rule to be changed and then saved before being committed to the firewalls. The commit function must require an additional step on the part of the administrator.
- (e) The management interface that provides a mechanism to record the reason for a rule change.
- (f) The firewall management system that provides a mechanism to integrate user IDs and groups that can be used in firewall rules.

- (g) The capability to support integration through automated deployment and change processes.
- (h) The firewall management system that provides a mechanism to roll back the last rule change after it has been committed.
- (i) Logging and audit
 - (i) All actions of the firewall administrators must be logged to include the action taken, a time stamp, the source IP address of the endpoint used to make the change, and the administrator user ID.
 - (ii) A reporting engine must allow the customer to create custom reports linked to specific queries.
 - (iii) Reports must include and correlate logs from all functions (firewall, IPS, application control, etc.) without requiring for customization or scripting.
 - (iv) The firewall must be capable of sending alerts on logged events.
 - (v) The events that create an alert must be configurable by the customer.
 - (vi) The firewall must have options for sending alerts including email and Simple Network Management Protocol (SNMP).
 - (vii) The firewall (or management system) must be capable of exporting log information in comma-separated values (CSV) and text formats.

(3) Deployment and integration

- (a) Be deployed and operational on the following ICT common operating environment:
 - (i) End-points: MS Windows, Linux, Android, IOS
 - (ii) Back-end server/hosting: On-premise, Private cloud
- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.5. Digital Signature

(1) Core functions and features

- (a) Provide certainty of the source and destination of information.
- (b) Encrypt the document for it not to be altered by unauthorised individual.
- (c) Provide non-repudiation when documents and transactions are submitted as part of the business process.
- (d) Provide certainty of the privacy of information.
- (e) Give assurance that the information can be introduced as evidence in a court or law.
- (f) Provide strong authentication for users accessing the solution.
- (g) Provide electronically signing of documents.
- (h) Provide a way of uniquely identifying users.
- (i) Guarantee sole control for the signer or data.

(2) Deployment and integration

- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) End-user computers and servers: MS Windows, Linux, Android, IOS
- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.6. Electronic mail protection, archive and journaling

(1) Core functions and features

- (a) **Mail achieve and journaling**
 - (i) Analyse, categorise, and prioritise the electronic mail messages on prescheduled time and date (i.e. policy based).
 - (ii) Manage unstructured electronic mail data and provide support of data retention and archiving legislative requirements.
 - (iii) Assign granular, unique retention rules to keep archived content only, as long as needed.
 - (iv) Tag archived items with metadata to speed supervision, search, and discovery.
 - (v) Reclassify your entire archive or a subset to meet evolving information retention requirements.
 - (vi) Store archived messages with the capability to support a ratio of 70% compression.
- (b) **Mail protection**
 - (i) Anti-malware for attachments, including emulation and strong detection results for nonexecutable files
 - (ii) Dynamic analysis of attachments and links through sandboxing
 - (iii) URL inspection on receipt of a message and at time of click
 - (iv) Anti-spam
 - (v) Anti-phishing and impersonation protection
 - (vi) Data protection through data loss prevention (DLP) and encryption

(2) Deployment and integration

- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) End-user computers and servers: MS Windows, Linux, Android
 - (ii) eMail Applications: MS Exchange, GroupWise
- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.7. Web Application Protection (WAP) and Proxy service

(3) Core functions and features

(a) Web Application protection

- (i) Technical architecture requirements for WEB security gateway services;
- (ii) Forwarding proxy service;
- (iii) Reverse proxy service;
- (iv) Security management service;
- (v) SSL inspection service;
- (vi) Content analysis service; and
- (vii) Malware analysis service.
- (viii) Be IPv4 and IPv6 compliant.
- (ix) Be Geo IP location awareness compliant.
- (x) Protect against known attacks such as DoS/Scripting attacks.
- (xi) Have Malware detection, analysis and sandboxing.

(b) Forwarding proxy service

- (i) Have the forwarding proxy service configured and deployed in an active/active mode and provide load balancing and redundancy.
- (ii) Provide progress notification— sends an HTML page that is compliant to the customers security policies to the client computer, informing the user that the requested content is being inspected, and displaying an indication of the download and inspection progress.
- (iii) Have real-time validation of X.509 server certificates to confirm revocation.
- (iv) Support multiple potential URL databases and the potential to run multiple simultaneous URL databases.
- (v) Have the ability to override the list of URLs' to manually blacklist unsafe or uncategorized websites and whitelist safe websites.
- (vi) Have dynamic categorization engine that will attempt to review uncategorized sites for content (for example, pornography, gambling or drugs) that is normally blocked.
- (vii) Provide policy creation to allow for the creation of numerous reusable, customized HTML block/warning pages.
- (viii) Specify groups of sites, for example, banking sites and health websites must be configurable to be excluded from inspection for privacy and/or business reasons.
- (ix) Limit functionality on a website at a more granular level (e.g. Prohibit downloads or uploads, etc.).
- (x) Have customizable error, block or warning pages.

- (xi) Have options to limit bandwidth for particular content types (for example, streaming media), URL categories, applications or protocols (such as FTP), which will limit the bandwidth capacity while performing certain activities or can prioritize activities over others.
- (xii) Have the ability to apply URL filtering policies when a mobile device is “off network” (direct access to the Internet, thereby bypassing the corporate VPN connection) to protect the end user device from harmful content when browsing using mobile roaming.
- (xiii) Have encrypted sites inspected (e.g. HTTPS/SSL, SSH, etc.).

(c) Reverse proxy service

- (i) The policy implementation must not require a reboot.
- (ii) Policy changes must become effective when active session’s end.
- (iii) Must have the ability to do security scanning on all file types and file sizes.
- (iv) All encrypted sessions must be inspected (e.g. HTTPS/SSL, SSH, etc.).
- (v) Must perform IP validation (for external parties to access internal functions on a least privileged access basis).
- (vi) Must separate suspected-virus quarantine for parking suspicious files or blocked file types and multiple disposition options.
- (vii) Must have the ability to identify, unpack and recursively unpack compressed or zipped files and identify password-protected or encrypted files.

(4) Operations Support System / System Administration

- (a) Must be centrally managing the forwarding and reverse proxy solutions with ample storage capacity for logs, configuration backups and providing reporting.
- (b) Have role-based administration and transparent authentication that enable users unrestricted access to the Internet but still records user names for reporting and troubleshooting purposes.
- (c) Have the capability of integrating with authoritative sources, trouble ticket systems, information security technologies, productivity suite applications, etc.
- (d) A task-based management GUI, which simplifies management by hiding complexity but also gives more technically skilled users the ability to drill down into granular detail.
- (e) Centralized management with automatic configuration and policy synchronization.
- (f) Threshold alerting capabilities such as e-mail, Short Message Service (SMS) and Simple Network Management Protocol (SNMP).
- (g) Home page dashboard of real-time events, to enable rapid troubleshooting of events or server issues.
- (h) Re-usable policy objects that is easy to read, that is printable and can be summarised summary for audit and troubleshooting purposes.
- (i) Dashboard configurable for different roles so that each administrator can create a role-specific view.

- (j) Dashboard to drill-down hyperlinks that enable administrators to create the detailed historical reports.
- (k) Incorporate log or alert thresholds with security information management systems or other reporting systems.
- (l) Custom reports creation capability, in HTML, CSV and PDF output types and save them, schedule them for distribution via e-mail, FTP or transferring them automated to a network storage/directory system.

(5) Deployment and integration

- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) The system must support MS Windows and Linux deployment
- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.8. Intrusion detection and prevention technical requirements overview

(1) Core functions and features

- (a) Detect threats / risks and prevent attempts to exploit weaknesses in vulnerable systems or applications.
- (b) Be able to integrate with next generation firewall, threat engines, security operations centre, incident management solutions, etc.
- (c) Detect and prevent specific known exploits, such as:
 - (i) protection from specific reported CVEs,
 - (ii) DNS tunnelling attacks indicating data leakage,
 - (iii) generic attacks types without any pre-defined signatures, and
 - (iv) protocol misuse which may indicate malicious activity.
- (d) Support automated virtual patching to protect against emerging threats between change control activities.
- (e) Support the open industry standard Common Vulnerability Scoring System (CVSS) for assignment of severity levels of the IPS protection.
- (f) Be capable to provide a high level of protection assurance and correctly recognize a specific attack to reduce false positives.
- (g) Dedicated open source threat intelligence service
 - (i) Have ruleset subscription used to enable advanced threat with network-based detection for the opensource Intrusion Detection System (IDS), Intrusion Prevention System (IPS) security enforcement and rule updates.
 - (ii) Enquire a timely and accurate ruleset for detecting and blocking advanced threats with continuous automated update, at minimum daily.
 - (iii) Blocks advanced threats including malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing, denial-of-

service attacks, protocol and application anomalies, exploit kits, supervisory control and data acquisition attacks at minimum.

- (iv) Have ruleset signatures based on real-world threats that surface every day and support a comprehensive number of rule categories, formats and open rulesets.
- (v) Be capable of low false positive rates through the use of sandbox and global sensor network feedback loop.
- (vi) Include network-based detection logic to uncover malware command and control communication.
- (vii) Support accurate detection of advance threats including:
 - 1) Coverage of major malware families by command, control channels and protocols.
 - 2) Detection across all network-based threat vectors – i.e. web servers, latest client-side attacks, exploit kits, etc.
 - 3) Provide accurate signatures for malware call-back, dropper, command and control, obfuscation, exploit-kit related threats and exfiltration.
 - 4) Provides a comprehensive ruleset that including but not limited to regularly prescribed CVE updates, Microsoft Active Protection Program (MAPP) and Patch Tuesday updates.
- (viii) Have ruleset available in multiple formats for a variety of network security applications.
 - 1) Must optimise the next-generation open source IDS and IPS engines.
 - 2) The ruleset used must run transparently on systems, with support to various threat engine.
 - 3) Must be able to create custom OEM versions of the ruleset in order to integrate it into proprietary network security appliances, when needed.

(2) Operations support system / Administration system

- (a) Have centralised management interface with distributed deployment to multiple implementations.
- (b) Track events through detailed reports and logs with ability to simplify threat analysis and reduce operational overhead, including critical security event identification and reporting.
- (c) Have the ability to activate and deactivate IPS protection on demand as business need arises.
- (d) Provide comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy.
- (e) Combine technologies such as deep packet inspection, threat reputation, URL reputation and advanced malware analysis on a flow-by-flow basis to detect and prevent attacks.

- (f) Proactively approach to security to provide comprehensive contextual awareness and deeper analysis of ICT network traffic.
 - (g) Have real-time machine learning capability techniques to deliver the ability to detect and mitigate threats in real-time.
 - (h) Provide threat analysis and security filters against vulnerabilities to protect against potential attacks and attack permutations.
 - (i) Have the ability to virtually patch to scale frontline defence mechanisms for protection of known threats based on vulnerability filters.
 - (j) Correlate events to protect against multi-stage attacks.
 - (k) Have inline blocking and multi-protocol call-back to stop attacks immediately.
 - (l) Action insights to accelerate response.
 - (m) Have ingestion of indicators from third-party tools to provide access to customer intelligence.
- (3) Deployment and integration**
- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) Servers: MS windows and Linux
 - (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.9. Data loss/leakage prevention

- (1) Core functions and features**
- (a) Discover where data lives across every channel: cloud, email, web, endpoints, and storage.
 - (b) Improve data classification accuracy searching for sensitive data, categorizing and monitoring.
 - (c) Monitor how data is being used on and off the corporate network.
 - (d) Protect sensitive data footprint by real time monitoring.
 - (e) Protects sensitive data from being exposed and leaked to the Web.
 - (f) Monitor and analyse all corporate web traffic, and optionally removes sensitive HTML content or blocks requests.
 - (g) Integrate with HTTP, HTTPS or FTP proxy server.
 - (h) Support all of the file types that may hold sensitive data, including PDFs, CVS, .xls, .doc and .txt files.
 - (i) Keep data safe while in use on endpoints by
 - (i) Scanning local hard drives and gives visibility into sensitive files that users are storing on their laptops and desktops.
 - (ii) Providing a wide range of responses including local and remote file quarantining, and policy-based encryption and digital rights.

- (iii) Monitoring users' activities and gives fine-grained control over a wide range of applications, devices and platforms.
 - (iv) Providing a wide range of responses including identity-based encryption and digital rights for files transferred to USB.
- (j) Protect data in motion over the network by:
 - (i) Capture and analyses outbound traffic on the corporate network, and detects sensitive content and metadata over standard, non-standard and proprietary protocols.
 - (ii) By performing deep content inspection of all network communications with zero packet loss.
- (k) Protect email by:
 - (i) Protecting sensitive messages from being leaked or stolen by employees, contractors and partners.
 - (ii) Monitoring and analysing all corporate email traffic, and optionally modifies, redirects, or blocks messages based on sensitive content or other message attributes.
- (l) Protection of data at rest by:
 - (i) Finding confidential data by scanning network file shares, databases, and other enterprise data repositories. This includes local file systems on Windows, Linux, AIX, and Solaris servers; Lotus Notes and SQL databases; and Microsoft Exchange and SharePoint servers.
 - (ii) Cleaning up and secures all of the exposed files detected, including quarantining or moving files, copying files to a quarantine area, or applying policy identity-based encryption and digital rights to specific files.
- (m) Protect data in the cloud by:
 - (i) Inspecting content extracted from cloud app and web traffic, and automatically enforces sensitive data policies.
 - (ii) Providing accurate, real-time monitoring of corporate email traffic.
 - (iii) Providing real-time protection against data leaks.
 - (iv) Identity-based encryption and digital rights for email bodies and attachments.
- (n) Have data confidentiality capability which includes:
 - (i) Detection of content by looking for matches on specific keywords, regular expressions or patterns, and file properties.
 - (ii) Detecting data by fingerprinting or indexing structured data sources such as databases, directory servers, and other structured data files.
 - (iii) Applying fingerprinting methods to detect data stored in unstructured documents, including Microsoft Office documents; PDFs; and binary files such as JPEGs, CAD designs, and multimedia files. Also detects "derived" content, such as text that has been copied from a source document to another file.

- (iv) Detecting text embedded in images such as scanned forms, documents, screenshots, pictures and PDFs.
- (o) Have data protection capability which includes
 - (i) Enable users to classify and label sensitive files and protect them based on sensitivity.
 - (ii) Apply persistent encryption and digital rights to data when it leaves the managed premises, control who can use it, track it everywhere, and revoke access if necessary.
 - (iii) Prevent unauthorized access to sensitive data via strong authentication when data is shared with business partners.
 - (iv) Ensure sensitive data doesn't get leaked over untrusted web traffic, even encrypted traffic.
- (p) Support the following encryption capabilities:
 - (i) Encrypt hard drives, files and folders with policy enforced encryption, which can be fully automated.
 - (ii) Must incorporate workflows, and be compliant with industry standards and regulations.
 - (iii) Must encrypt all traffic traversing a network or selected traffic.
 - (iv) Protect servers and provide default data protection up to a specified classification level.
 - (v) Separate strong cryptographic algorithm to deploy in areas where the data classification exceeds a default / specified classification level.
 - (vi) Provide secure remote access for mobile users.
 - (vii) Support use of different key length and industry cryptographic algorithm.
 - (viii) Support deployment with virtualisation and appliance.
 - (ix) Enable network segmentation, source to host encryption capability for on demand secure VPN services and remote access support.
 - (x) Have management of encryption key and cryptography algorithms must support customisation and centralised management.

(2) Operation Support System / System Administration

- (a) Be easy to manage with simple policies that can be centrally managed with role-based access control.
- (b) Work across platforms, networks, and devices, including cloud repositories, Windows / macOS, file server, USB drives.

(3) Deployment and integration

- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) Operating System: MS Windows, Linux, Android

- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.10.Vulnerability management

(1) Core functions and features

- (a) The solution must identify and detect vulnerabilities in the infrastructure or environment including:
 - (i) Networks and IP ranges that must be scanned.
 - (ii) URL's that must be included in web application vulnerability scans
- (b) After identifying a vulnerability, it must be documented in a common repository or risk map. This enables further analysis and reporting.
- (c) The system should check whether there is any susceptibility and to assess the risk of the detected vulnerability in order to determine the criticality and hence the urgency of the required remediation.

(2) Operations Support System / System Administration

- (a) The solution must be centrally managed with role-based access control.
- (b) The system reports must have an option to export the report in a CSV format
- (c) The system must have central reporting capability not limited to the following report.
- (d) There must be the executive summary for reviewing the vulnerability scan's results. It gives readers a look into how well or poorly a system performed. It can then classify the organization as having a low, medium, high, or critical risk level.
- (e) There must be the assessment overview section to clearly and concisely state the validation, investigation, and deliverables given by the vulnerability assessment.
- (f) There must be the results and mitigations recommendation section which must lists and describes each security vulnerability, including (ideally):
 - (i) Name of the vulnerability
 - (ii) Date of discovery
 - (iii) Vulnerability score
 - (iv) Detailed description
 - (v) Process to detect the vulnerability
 - (vi) Proof of concept of the vulnerability
 - (vii) Guidance for remediation
 - (viii) Prioritization of vulnerability

(3) Deployment and integration

- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) Operating System: MS Windows, Linux, Android, IBM zOS

- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

3.11.Identity and Access Management

(1) Core functions and features

- (a) Identity authentication and authorization by granting appropriate access rights to entities via their identities.
- (b) Implementing services to prove identities and control access to resources.
- (c) Single sign-on (SSO) capability that enables users to authenticate with multiple applications or systems using just one login and one set of credentials.
- (d) Access control policy management, role-based access control (RBAC), attribute-based access control (ABAC) and resource grouping models.
- (e) Control access to all digital assets, including devices, network equipment, servers, portals, content, applications and/or products.
- (f) Identity federation by enabling systems that share user access to log in based on authenticating against one of the systems participating in the federation.
- (g) Creation, deletion, modification of identity data either assisted or self-service.
- (h) Safely enabling remote access governance and administration
- (i) Identity governance and administration (IGA) and privileged access management (PAM) as well as logging, reporting and analytics.
- (j) Scalable approach to manage identity life cycles across heterogeneous systems and real-time data access regardless of the number of users accessing the data store.
- (k) Reusable identities, including social identities and other third-party identities, greatly reducing friction for new users.
- (l) Correlate user access, information sensitivity, privileges and policies in order to make better IAM decisions.
- (m) Access certification by routinely review what users have access to which systems and data.
- (n) Multifactor authentication by granting access to an entity only after successfully presenting more than one piece of evidence (or factors) to an authentication mechanism.
- (o) Protect the organization from data breaches.
- (p) Have authentication built for the enterprise.
- (q) Have critical component of zero trust access concept.
- (r) Secure access to sensitive data.
- (s) Have risk-based authentication to identify login anomalies.
- (t) Ability to secure password less login on any device.
- (u) Enforce device trust and strong authentication.

- (v) Prevent large scale identity attacks.
- (w) Identity as a Service (IDaaS) and managed identity services.

(2) Deployment and integration

- (a) Be deployed or compatible with the following ICT common operating environment:
 - (i) Operating System: MS Windows, Linux, Android, IBM zOS
- (b) Integrate/interoperate with a central Security Operation Centre (SOC) solution for information security event monitoring, correlation and response.

4. BID EVALUATION STAGES

- (1) The bid evaluation process consists of several stages that are applicable according to the nature of the bid as defined in the table below.

Stage	Description	Applicable for this bid
Stage 1A	Administrative pre-qualification verification	YES
Stage 2A	Technical Mandatory requirement evaluation	YES
Stage 2B	Technical Functionality requirement evaluation	NO
Stage 2C	Technical Proof of Concept requirement evaluation	NO
Stage 3	Special Conditions of Contract verification	YES
Stage 4	Price / B-BBEE evaluation	NO

- (2) **The bidder must qualify for each stage to be eligible to proceed to the next stage of the evaluation.**

(3) **Notice of outcome of the RFAProcess**

Bidders that are pre-qualified will be informed of the success of their bid to pre-qualify as an accredited Information Security Service Provider for the supply of information security products and services.

ANNEX A.1: ADMINISTRATIVE PRE-QUALIFICATION

5. ADMINISTRATIVE PRE-QUALIFICATION REQUIREMENTS

5.1. ADMINISTRATIVE PRE-QUALIFICATION VERIFICATION

- (1) The bidder **must comply** with ALL of the bid pre-qualification requirements in order for the bid to be accepted for evaluation.
- (2) If the Bidder failed to comply with any of the administrative pre-qualification requirements, or if SITA is unable to verify whether the pre-qualification requirements are met, then SITA reserves the right to –
 - (a) Reject the bid and not evaluate it, or
 - (b) Accept the bid for evaluation, on condition that the Bidder must submit within 7 (seven) days any supplementary information to achieve full compliance, provided that the supplementary information is administrative and not substantive in nature.

5.2. ADMINISTRATIVE PRE-QUALIFICATION REQUIREMENTS

- (1) **Submission of bid response:** The bidder must submit a bid response documentation pack –
 - (i) delivered at the correct physical or postal address and within the stipulated date and time as specified in the “Invitation to Bid” cover page, and;
 - (ii) in the correct format as one original document, two copies and a copy on a memory stick.
- (2) **Attendance of briefing session:** A Non-Compulsory Briefing Session will be done virtually. **Registered Supplier.** The bidder is, in terms of National Treasury Instruction Note 4A of 2016/17, registered as a Supplier on National Treasury Central Supplier Database (CSD).

ANNEX A.2: TECHNICAL MANDATORY REQUIREMENTS

6. TECHNICAL MANDATORY

6.1. INSTRUCTION AND EVALUATION CRITERIA

- (1) The bidder **must comply with ALL the requirements by providing substantiating evidence** in the form of documentation or information (attached to Annex B), failing which it will be regarded as “NOT COMPLY”.
- (2) The bidder **must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response as “NOT COMPLY”.
- (3) SITA reserves the right verify any of the substantiating evidence.
- (4) **The bidder must comply with ALL the TECHNICAL MANDATORY REQUIREMENTS in order for the bid to proceed to the next stage of the evaluation.**

6.2. APPROVAL PROCESS

The Bidder needs to complete the following process stages which the bidders requires accreditation for evaluation and possible inclusion in the term contract:

Stage 1: BIDDER PRODUCT OFFER

The Bidder must indicate the Information Security products or services Product Category they wish to respond to by completing **ANNEX C: Addendum 1**.

Stage 2: BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS

Attach to Annexure B a copy of documentation (valid certificate, license, official letter, agreement or declaration) indicating that the bidder is a registered OSM/OEM Partner or Reseller who is authorised/accredited to supply OEM/OSM products for each of the Information Security products or service Product Categories which the bidder wish to respond to in Annex C: Addendum 1.

Stage 3: BIDDER EXPERIENCE AND CAPABILITY REQUIREMENTS

Provide reference details from at least one (1) customer to whom the Information Security products or services which the bidder wishes to respond to by completing Annex B, Section 14.2, table 1.

Stage 4: RATE CARD

Complete the Rate Card Annex D: Addendum 2

6.3. TECHNICAL MANDATORY REQUIREMENTS

TECHNICAL MANDATORY REQUIREMENTS	Substantiating evidence of compliance <i>(used to evaluate bid)</i>	Evidence reference <i>(to be completed by bidder)</i>
<p>(1) BIDDER PRODUCT OFFER</p> <p>The bidder must indicate the Information Security products or services Product Category they wish to respond to as indicated in section 2.1(1).</p>	<p>The Bidder must indicate the Information Security products or services Product Category they wish to respond to by completing ANNEX C: Addendum 1.</p> <p>Note: SITA reserves the right to verify the information provided.</p>	<p><provide unique reference to locate substantiating evidence in the bid response – see Annex B, section 14.1 and Annex C: Addendum 1></p>
<p>(2) BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS</p> <p>The bidder must be a registered OSM/OEM partner or reseller for each of the Information Security products or service Product Categories which the bidder selected in ANNEX C: Addendum 1.</p>	<p>Attach to Annexure B a copy of documentation (valid certificate, license, official letter, agreement or declaration) indicating that the bidder is a registered OSM/OEM Partner or Reseller who is authorised/accredited to supply OEM/OSM products for each of the Information Security products or service Product Categories which the bidder wishes to respond to in Annex C: Addendum 1 including the following:</p> <ul style="list-style-type: none"> a) Supply, b) Install c) Configure, 	<p><provide unique reference to locate substantiating evidence in the bid response – see Annex B, section 14.2 and Annex C: Addendum 1 ></p>

TECHNICAL MANDATORY REQUIREMENTS	Substantiating evidence of compliance <i>(used to evaluate bid)</i>	Evidence reference <i>(to be completed by bidder)</i>
	d) Maintenance, e) Support f) Training, and g) Professional Services Note: SITA reserves the right to verify the information provided.	
(3) BIDDER EXPERIENCE AND CAPABILITY REQUIREMENTS The bidder must have provided projects or services for Information Security products or services which the bidder wish to respond to from at least one (1) customer in the past five (5) years.	Provide reference details from at least one (1) customer to whom the Information Security products or services which the bidder wishes to respond to was provided in the past (5) five years which includes the following: a) Supply, b) Install c) Configure, d) Maintenance, e) Support f) Training, and g) Professional Services Note (1): The references may be from the same or multiple customers as long as the bidder provide reference details for each of the Information Security products or services the bidder has selected.	Provide unique reference to locate substantiating evidence in the bid response – see Annex B: 14.3, table 1>

TECHNICAL MANDATORY REQUIREMENTS	<i>Substantiating evidence of compliance</i> <i>(used to evaluate bid)</i>	<i>Evidence reference</i> <i>(to be completed by bidder)</i>
	Note (2): SITA reserves the right to verify the information provided.	
(4) SPECIAL CONDITIONS OF CONTRACT Bidder needs to Accept all the Special Conditions of contract.	The Bidder needs to Accept all the Special Conditions of Contract by completing the declaration of Acceptance in section 9.3 and attach it as part of the Bid submission.	Provide unique reference to locate substantiating evidence in the bid response – see Annex B: 14.4>
(5) RATE CARD OF AREA OF EXPERTISE	The Bidder needs to complete the Rate Card of Area of Expertise Annex D Addendum 2 as per the requirements indicated in Annex A4, section 10.	Provide unique reference to locate substantiating evidence in the bid response – see Annex B: 14.5>

6.4. DECLARATION OF COMPLIANCE

	Comply	Not Comply
The bidder declares by indicating with an “X” in either the “COMPLY” or “NOT COMPLY” column that – <ul style="list-style-type: none"> (a) The bid complies with each and every TECHNICAL MANDATORY REQUIREMENT as specified in SECTION 6.3 above; AND (b) Each and every requirement specification is substantiated by evidence as proof of compliance. 		

7. TECHNICAL FUNCTIONALITY (NON-MANDATORY SPECIFICATIONS)

7.1. TECHNICAL FUNCTIONALITY REQUIREMENTS

N/A

8. PROOF OF CONCEPT REQUIREMENT

N/A

ANNEX A.3: SPECIAL CONDITIONS OF CONTRACT (SCC)

9. SPECIAL CONDITIONS OF CONTRACT

9.1. INSTRUCTION

- (1) The successful supplier will be bound by Government Procurement: General Conditions of Contract (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the successful Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
- (2) SITA reserves the right to –
 - (a) Negotiate the conditions, or
 - (b) Automatically disqualify a bidder for not accepting these conditions.
 - (c) Award to multiple bidders for multiple product suites.
 - (d) To award a specific item on the RFB should it be the first latest technology offered and not provided by other bidders on the list within a specific category.
- (3) In the event that the bidder qualifies the proposal with own conditions, and does not specifically withdraw such own conditions when called upon to do so, SITA will invoke the rights reserved in accordance with subsection 9.1(2) above.
- (4) The bidder must **complete the declaration of acceptance** as per section 9.3 below by marking with an “X” either “ACCEPT ALL” or “DO NOT ACCEPT ALL”, failing which the declaration will be regarded as “DO NOT ACCEPT ALL” and the bid may be disqualified.

9.2. SPECIAL CONDITIONS OF CONTRACT

(1) CONTRACTING CONDITIONS

- (a) **Formal Contract.** The Supplier must enter into a formal written Contract (Agreement) with SITA (internal) or Government Department.
- (b) **Right of Award.** SITA reserves the right to award the contract for required goods or services to multiple Suppliers.
- (c) **Right to Audit.** SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct a financial audit or probity to ascertain whether a qualifying bidder has the financial wherewithal or technical capability to provide the goods and services as required by this tender.

(2) DELIVERY ADDRESS

The supplier must deliver the required products or services at the delivery address which will be indicated during the engagement process.

(3) SERVICES AND PERFORMANCE METRICS

- (a) The Supplier is responsible to provide the following services as specified in the Service Breakdown Structure (SBS):

SBS	Service Element	Service Grade	Service Level
1.	Call Centre	Normal	8h x 5d, business hours of client
2.	Incident Response	Normal	Maximum 4 hours
3.	Incident Restore	Normal	Maximum 8 hours

(4) CERTIFICATION, EXPERTISE AND QUALIFICATION

- (a) The Supplier represents that,
 - (i) it has the necessary expertise, skill, qualifications and ability to undertake the work required in terms of the Statement of Work or Service Definition;
 - (ii) it is committed to provide the Products or Services; and
 - (iii) perform all obligations detailed herein without any interruption to the Customer.
- (b) The Supplier must provide the service in a good and workmanlike manner and in accordance with the practices and high professional standards used in well-managed operations;
- (c) The Supplier must perform the Services in the most cost-effective manner consistent with the level of quality and performance as defined in Statement of Work or Service Definition;
- (d) **Original Equipment Manufacturer (OEM) or Original Software Manufacturer (OSM) work.** The Supplier must ensure that work or service is performed by a person who is certified by Original Equipment Manufacturer or Original Software Manufacturer, including at least the following:
- (e) **Professional Services** Information will be specified in the engagement process.

(5) LOGISTICAL CONDITIONS

- (a) **Hours of work.** Information will be specified in the Work Packages.
- (b) In the event that SITA grants the Supplier permission to access SITA's Environment including hardware, software, internet facilities, data, telecommunication facilities and/or network facilities remotely, the Supplier must adhere to SITA's relevant policies and procedures (which policy and procedures are available to the Supplier on request) or in the absence of such policy and procedures, in terms of, best industry practice.
- (c) **Tools of Trade.** Information will be specified in the Work Packages.
- (d) **On-site and Remote Support.** Information will be specified in the Work Packages.
- (e) **Support and Help Desk.** Information will be specified in the Work Packages.

(6) SKILLS TRANSFER AND TRAINING

- (a) The Supplier must provide certified training on the proposed solution or product to management and technical staff to enable SITA or Government to operate and support the product or solution after implementation.
- (b) The nature of the training must be formal, informal, hand-on.

(7) REGULATORY, QUALITY AND STANDARDS

- (a) The Supplier must for the duration of the contract ensure compliance with <ISO/IEC General Quality Standards, ISO9001>
- (b) The Supplier must for the duration of the contract ensure compliance with <IEC/ISO Manufacturing and Workmanship quality condition>
- (c) The Supplier must for the duration of the contract ensure compliance with Protection of Personal Information Act (POPIA).
- (d) The Supplier must for the duration of the contract ensure compliance with <IEC/ISO Environmental conditions>

(8) PERSONNEL SECURITY CLEARANCE

- (a) The Supplier personnel who are required to work with information related to NATIONAL SECURITY must have a **valid South African security clearance** or must apply within 30 days of the signed contract for a security clearance to the level of **CONFIDENTIAL, SECRET or TOP SECRET** at the expense of the Supplier from the South African State Security Agency or duly authorised Personnel Security Vetting entity of SA Government.
- (b) The Supplier personnel who are required to work with GOVERNMENT CLASSIFIED information or access government RESTRICTED areas must be a South African Citizen and at the expense of the Supplier be security vetted (pre-employment screening, criminal record screening and credit screening).
- (c) The Supplier must ensure that the security clearances of all personnel involved in the Contract remains valid for the period of the contract.

(9) CONFIDENTIALITY AND NON-DISCLOSURE CONDITIONS

- (a) The Supplier, including its management and staff, must before commencement of the Contract, sign a non-disclosure agreement regarding Confidential Information.
- (b) Confidential Information means any information or data, irrespective of the form or medium in which it may be stored, which is not in the public domain and which becomes available or accessible to a Party as a consequence of this Contract, including information or data which is prohibited from disclosure by virtue of:
 - (i) the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000);
 - (ii) being clearly marked "Confidential" and which is provided by one Party to another Party in terms of this Contract;
 - (iii) being information or data, which one Party provides to another Party or to which a Party has access because of Services provided in terms of this Contract and in which a Party would have a reasonable expectation of confidentiality;
 - (iv) being information provided by one Party to another Party in the course of contractual or other negotiations, which could reasonably be expected to prejudice the right of the non-disclosing Party;
 - (v) being information, the disclosure of which could reasonably be expected to endanger a life or physical security of a person;

- (vi) being technical, scientific, commercial, financial and market-related information, know-how and trade secrets of a Party;
 - (vii) being financial, commercial, scientific or technical information, other than trade secrets, of a Party, the disclosure of which would be likely to cause harm to the commercial or financial interests of a non-disclosing Party; and
 - (viii) being information supplied by a Party in confidence, the disclosure of which could reasonably be expected either to put the Party at a disadvantage in contractual or other negotiations or to prejudice the Party in commercial competition; or
 - (ix) information the disclosure of which would be likely to prejudice or impair the safety and security of a building, structure or system, including, but not limited to, a computer or communication system; a means of transport; or any other property; or a person; methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme; the safety of the public or any part of the public; or the security of property; information the disclosure of which could reasonably be expected to cause prejudice to the defence of the Republic; security of the Republic; or international relations of the Republic; or plans, designs, drawings, functional and technical requirements and specifications of a Party, but must not include information which has been made automatically available, in terms of the Promotion of Access to Information Act, 2000; and information which a Party has a statutory or common law duty to disclose or in respect of which there is no reasonable expectation of privacy or confidentiality.
- (c) Notwithstanding the provisions of this Contract, no Party is entitled to disclose Confidential Information, except where required to do so in terms of a law, without the prior written consent of any other Party having an interest in the disclosure.
 - (d) Where a Party discloses Confidential Information which materially damages or could materially damage another Party, the disclosing Party must submit all facts related to the disclosure in writing to the other Party, who must submit information related to such actual or potential material damage to be resolved as a dispute.
 - (e) Parties may not, except to the extent that a Party is legally required to make a public statement, make any public statement or issue a press release which could affect another Party, without first submitting a written copy of the proposed public statement or press release to the other Party and obtaining the other Party's prior written approval for such public statement or press release, which consent must not unreasonably be withheld.

(10) GUARANTEE AND WARRANTIES

The Supplier warrants that:

- (a) The warranty of goods supplied under this contract remains valid for **twelve (12) months** after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for **eighteen (18) months** after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier;

- (b) as at Commencement Date, it has the rights, title and interest in and to the Product or Services to deliver such Product or Services in terms of the Contract and that such rights are free from any encumbrances whatsoever;
- (c) the Product is in good working order, free from Defects in material and workmanship, and substantially conforms to the Specifications, for the duration of the Warranty period;
- (d) during the Warranty period any defective item or part component of the Product be repaired or replaced within **3 (three) days** after receiving a written notice from SITA;
- (e) the Products is maintained during its Warranty Period at no expense to SITA;
- (f) the Product possesses all material functions and features required for SITA's Operational Requirements;
- (g) the Product remains connected or Service is continued during the term of the Contract;
- (h) all third-party warranties that the Supplier receives in connection with the Products including the corresponding software and the benefits of all such warranties are ceded to SITA without reducing or limiting the Supplier's obligations under the Contract;
- (i) no actions, suits, or proceedings, pending or threatened against it or any of its third party suppliers or sub-contractors that have a material adverse effect on the Supplier's ability to fulfil its obligations under the Contract exist;
- (j) SITA is notified immediately if it becomes aware of any action, suit, or proceeding, pending or threatened to have a material adverse effect on the Supplier's ability to fulfil the obligations under the Contract;
- (k) any Product sold to SITA after the Commencement Date of the Contract remains free from any lien, pledge, encumbrance or security interest;
- (l) SITA's use of the Product and Manuals supplied in connection with the Contract does not infringe any Intellectual Property Rights of any third party;
- (m) the information disclosed to SITA does not contain any trade secrets of any third party, unless disclosure is permitted by such third party;
- (n) it is financially capable of fulfilling all requirements of the Contract and that the Supplier is a validly organized entity that has the authority to enter into the Contract;
- (o) it is not prohibited by any loan, contract, financing arrangement, trade covenant, or similar restriction from entering into the Contract;
- (p) the prices, charges and fees to SITA as contained in the Contract are at least as favourable as those offered by the Supplier to any of its other customers that are of the same or similar standing and situation as SITA; and
- (q) any misrepresentation by the Supplier amounts to a breach of Contract.

(11) INTELLECTUAL PROPERTY RIGHTS

- (a) SITA retains all Intellectual Property Rights in and to SITA's Intellectual Property. As of the Effective Date, the Supplier is granted a non-exclusive license, for the continued duration of this Contract, to perform any lawful act including the right to use, copy, maintain, modify, enhance and create derivative works of SITA's Intellectual Property

for the sole purpose of providing the Products or Services to SITA pursuant to this Contract; provided that the Supplier must not be permitted to use SITA's Intellectual Property for the benefit of any entities other than SITA without the written consent of SITA, which consent may be withheld in SITA's sole and absolute discretion. Except as otherwise requested or approved by SITA, which approval is in SITA's sole and absolute discretion, the Supplier must cease all use of SITA's Intellectual Property, at of the earliest of:

- (i) termination or expiration date of this Contract;
 - (ii) the date of completion of the Services; and
 - (iii) the date of rendering of the last of the Deliverables.
- (b) If so required by SITA, the Supplier must certify in writing to SITA that it has either returned all SITA Intellectual Property to SITA or destroyed or deleted all other SITA Intellectual Property in its possession or under its control.
 - (c) SITA, at all times, owns all Intellectual Property Rights in and to all Bespoke Intellectual Property.
 - (d) Save for the license granted in terms of this Contract, the Supplier retains all Intellectual Property Rights in and to the Supplier's pre-existing Intellectual Property that is used or supplied in connection with the Products or Services.

(12) GENERAL

- (a) The supplier will be bound by Government Procurement: General Conditions of Contract.
- (b) (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
- (c) SITA reserves the right to:
 - (i) Negotiate the conditions, or
 - (ii) Automatically disqualify a bidder for not accepting these conditions.
 - (iii) Right to Audit: SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct probity to ascertain whether a qualifying bidder has the technical capability to provide the goods and services as required by this tender.
- (d) "The parties in this Agreement agree that the offer price of all the equipment shall be at the wholesale price or below wholesale price as agreed with the OEM. Should, at any time during the existence of the agreement that the offered price which is higher than the wholesale price or as agreed with the OEM, SITA client shall be entitled to such wholesale price with the exclusion of the mark-up which the reseller may have charged".

NOTE: These conditions will form part of the contract obligations and suppliers are expected to comply in order for SITA to conclude an agreement with the potential suppliers. Failure to comply during finalisation of a contract may result to disqualification.

(13) SUPPLIER DUE DILIGENCE

SITA reserves the right to conduct supplier due diligence prior to final award or at any time during the Contract period and this may include pre-announced/ non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid or Contract in whole or parts thereof.

(14) COUNTER CONDITIONS

Bidders' attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

(15) FRONTING

- (a) The SITA supports the spirit of Broad Based Black Economic Empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the SITA any form of fronting.
- (b) The SITA, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in bid documents. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade and Industry, be established during such enquiry/investigation, the onus will be on the bidder / contractor to prove that fronting does not exist. Failure to do so within a period of 14 days from date of notification may invalidate the bid / contract and may also result in the restriction of the bidder/contractor to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies SITA may have against the bidder/contractor concerned.

(16) PRODUCT ADHERANCE / MODEL CHANGE

- (a) In the event where a bidder offers a product/service against an item and the item is subsequently awarded to the bidder, it is required of the contractor to continue to supply the model awarded throughout the contract period.
- (b) In the event that the product/service is discontinued, SITA Contract Management must be notified of such an occurrence and an official amendment will be issued.
- (c) In the case where equipment has been discontinued and or replaced with a new product/service, the contractors are required to submit letters from manufacturer/suppliers stating the changes.
- (d) Furthermore, contractors are to take note that the price of the new product/service should not differ from the current bid price of the original model.
- (e) The new product/service must adhere to the minimum specification for the item category.

- (f) Contractors are not to deliver new products/services prior to approval of model changes by the SITA.

(17) ENGAGEMENT MODEL (Rules of Engagement)

- Master Service Agreements will be signed with successful bidders to be placed on the Master Agreement with SITA that will thereafter follow due process in terms of the engagement model.
- The engagement model could entail direct sourcing, competitive quotations and/ or rotation of suppliers depending on ranking through the RFB process.
- The RFB list will be Refreshed every six (6) months to allow the inclusion of more service providers, however the rates in the Rate card be fixed and will be refreshed annually.
- During the six (6) monthly Refresh bidders are allowed to update new technologies or products on the list within a specific category and provide a Rate to the Rate Card.
- Bidder will be requested to indicate their best price at the time of engagement, however not exceeding the maximum rate indicated in the Rate Card as tendered in this RFB.
- Bidders which exceed their tendered maximum rate indicated in the Rate Card in this RFB will be disqualified during the engagement process.
- Specific requirements will be provided during the engagement process.

9.3. DECLARATION OF ACCEPTANCE

	ACCEPT ALL	DO NOT ACCEPT ALL
(13) The bidder declares to ACCEPT ALL the Special Condition of Contract as specified in section 9.2 above by indicating with an "X" in the "ACCEPT ALL" column.		
NOTE: Bidders must ACCEPT ALL the Special Condition of Contract as specified in section 9.2, failing which will result in Disqualification		

ANNEX A.4: COSTING AND PRICING

10.1 COSTING AND PRICING EVALUATION

- (1) In terms of Preferential Procurement Policy Framework Act (PPPFA), the following preference point system is applicable to all Bids:
 - (a) the 80/20 system (80 Price, 20 B-BBEE) for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); or
 - (b) the 90/10 system (90 Price and 10 B-BBEE) for requirements with a Rand value above R50 000 000 (all applicable taxes included).
- (2) This bid will be evaluated using the preferential point system of **90/10 or 80/20**, subject to the following conditions –
 - (a) If the lowest acceptable bid price is up to and including R50 000 000 (all applicable taxes included) then the 80/20 preferential point system will apply to all acceptable bids; or
 - (b) If the lowest acceptable bid price is above R50 000 000 (all applicable taxes included) then the 90/10 preferential point system will apply to all acceptable bids;
- (3) The bidder must **complete the declaration of acceptance** as per section 10.4 below by marking with an “X” either “ACCEPT ALL”, or “DO NOT ACCEPT ALL”, failing which the declaration will be regarded as “DO NOT ACCEPT ALL” and the bid will be disqualified.
- (4) Bidder will be bound by the following general costing and pricing conditions and SITA reserves the right to negotiate the conditions or automatically disqualify the bidder for not accepting these conditions. These conditions will form part of the Contract between SITA and the bidder. However, SITA reserves the right to include or waive the condition in the Contract.

10.2 COSTING AND PRICING CONDITIONS

1. SOUTH AFRICAN PRICING

The total price must be VAT inclusive and be quoted in South African Rand (ZAR).

2. TOTAL PRICE

- (a) All quoted prices are the total price for the entire scope of required services and deliverables to be provided by the bidder.
- (b) The cost of delivery, labour, S&T, overtime, etc. must be included in this bid.
- (c) All additional costs must be clearly specified.

SITA reserves the right to negotiate pricing with the successful bidder prior to the award as well as envisaged quantities.

3. BID EXCHANGE RATE CONDITIONS

The bidders must use the exchange rate provided below to enable SITA to compare the prices provided by using the same exchange rate:

Foreign currency	South African Rand (ZAR) exchange rate
1 US Dollar	R 14,38
1 Euro	R 16,76
1 Pound	R 19,89

10.3 RATE CARD OF AREA OF EXPERTISE

The Bidder **must** complete the Rate Card for the Information Security products or services Product Category they wish to respond in (ANNEX D: ADDENDUM 2).

- (5) The bidder must **complete the declaration of acceptance** as per section 10.2 below by marking with an "X" either "ACCEPT ALL", or "DO NOT ACCEPT ALL", failing which the declaration will be regarded as "DO NOT ACCEPT ALL" and the bid will be disqualified.

NOTE:

- (1) Bidders must complete ALL the fields for each of the relevant Information Security products or services Product Category for which they are applying for on (ANNEX C: ADDENDUM 1).
- (2) Failing to complete ALL fields will result in disqualification.

10.4 DECLARATION OF ACCEPTANCE

	ACCEPT ALL	DO NOT ACCEPT ALL
<p>(14) The bidder declares to ACCEPT ALL the Costing and Pricing conditions as specified in section (1) above by indicating with an "X" in the "ACCEPT ALL" column, or</p> <p>(15) The bidder declares to NOT ACCEPT ALL the Costing and Pricing Conditions as specified in section (1) above by -</p> <p>(a) Indicating with an "X" in the "DO NOT ACCEPT ALL" column, and;</p> <p>(b) Provide reason and proposal for each of the condition not accepted.</p>		
<p>Comments by bidder: Provide the condition reference, the reasons for not accepting the condition.</p>		

ANNEX A.5: TECHNICAL SCHEDULES

11. TECHNICAL SCHEDULES

Not applicable.

ANNEX A.6: Terms and definitions

12. ABBREVIATIONS

Adv.	Advocate
BBBEE	Broad Based Black Economic Empowerment
BSCOM	Bid Specification Committee
CRM	Customer Relations Manager
CSD	Central Supplier Database
DoA	Delegation of Authority
EME	Exempted Micro Enterprise
GCC	General Condition of Contract
GPS	Global Positioning System
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
ISO	International Standardization Organization
N/A	Not Applicable
NT	National Treasury
OEM	Original Equipment Manufacturer
OSM	Original Software Manufacturer
POC	Proof of Concept
PPPFA	Preferential Procurement Policy Framework Act
QSE	Qualifying Small Enterprise
RFA	Request for Accreditation
RFB	Request for Bid
RFP	Request for Proposal
RFQ	Request for Quotation
RSA	Republic of South Africa
SBD	Standard Bidding Document
SCC	Special Condition of Contract
SCM	Supplier Chain Management
SITA	State Information Technology Agency
SMME	Small Medium and Micro Enterprise
TCV	Total Contract Value
USD	United States Dollar
VAT	Value Added Tax
WCED	Western Cape Education Department
WCG	Western Cape Government
ZAR	South African Rand

13. DEFINITIONS

No.	Digital Signature Classes	Class Definition
1.	Personal Class 2 advanced digital signature certificates.	Class 2 - Digital signature provides at minimum a medium assurance 1024-bit certificates that are for standard commercial use. These certificates are ideal for medium-level authentication, signing and encryption of electronic communications like email.
2.	Personal Class 3 advanced electronic signature certificates	Class 3 - Digital signature provides a high assurance, closed community certificates for commercial use. These certificates are only available to organisations who wish to authenticate users within their own closed user groups (staff and/or customers). They are ideal for high-level authentication, access control, signing and encryption of electronic communications, transactions and processes within a closed environment. No need for face-to-face verification. However, note that Class 3 will not be able to stand in court of law as no face-to-face verification has been conducted.
3.	Personal Class 4 advanced electronic signature certificates:	Class 4– Digital signature available to users and organisations that wish to transact and communicate with clear legal status. A high level of independent identity authentication is provided through the collection of personal identity information, including fingerprints and the verification of the information provided with the Department of Home Affairs. Advanced Electronic Signatures are strongly recommended for strong authentication, signing and encryption of electronic communications, transactions and process.

ANNEX B: BIDDER SUBSTANTIATING EVIDENCE

14. MANDATORY REQUIREMENT EVIDENCE

14.1 BIDDER PRODUCT OFFER

The Bidder must indicate the Information Security products or services Product Category they wish to respond to by completing **ANNEX C: Addendum 1**.

14.2 BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS

Attach a copy of documentation (valid certificate, license, official letter, agreement or declaration) indicating that the bidder is a registered OSM/OEM Partner or Reseller who is authorised/accredited to supply OEM/OSM products for each of the Information Security products or service Product Categories which the bidder wish to respond to in Annex C: Addendum 1 including the following here:

- a) Supply,
- b) Install
- c) Configure,
- d) Maintenance,
- e) Support
- f) Training, and
- g) Professional Services

14.3 BIDDER EXPERIENCE AND CAPABILITY REQUIREMENTS

- a) Complete table below, noting that:
 - i. The bidder must have provided Information Security products or services which the bidder wish to respond to as indicated in Annex C: Addendum 1 from at least one (1) customer in the past five (5) years including the following:
 - a. Supply,
 - b. Install
 - c. Configure,
 - d. Maintenance,
 - e. Support
 - f. Training, and
 - g. Professional Services
 - ii. Project end-date must be current or not older than five (5) years from date this bid is advertised,

- iii. Scope of work must be related to the capability selected for participation.

Table 1: References:

No	Reference in line with Annex C: Addendum 1, table 2.	Company name	Reference Person Name, Tel and/or email	Project Scope of work	Project Start and End-date
1	End Point Protection	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom End Point Protection capability was provided>	Start Date: End Date:
2	End point detection and response	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom End point detection and response was provided>	Start Date: End Date:
3	Firewall	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom Firewall capability was provided>	Start Date: End Date:
4	Digital Signatures	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom Digital Signatures capability was provided>	Start Date: End Date:
5	Electronic mail protection, archive and journaling	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom Electronic mail protection, archive and journaling capability was provided>	Start Date: End Date:
6	Web application protection and proxy services	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom Web application protection and proxy services capability was provided>	Start Date: End Date:
7	Intrusion detection and prevention	<Company name>	<Person Name> <Tel> <email>	< Provide reference from a customer to whom Intrusion	Start Date: End Date:

No	Reference in line with Annex C: Addendum 1, table 2.	Company name	Reference Person Name, Tel and/or email	Project Scope of work	Project Start and End-date
				detection and prevention capability was provided>	
8	Data loss/leakage prevention	Company name>	Person Name> <Tel> <email>	< Provide reference from a customer to whom Data loss/leakage prevention capability was provided>	Start Date: End Date:
9	Vulnerability management	Company name>	Person Name>	< Provide reference from a customer to whom Vulnerability management capability was provided>	Start Date:
10	Identity and Access Management	Company name>	Person Name> <Tel> <email>	< Provide reference from a customer to whom Intrusion detection and prevention capability was provided>	Start Date: End Date:

NOTE: Failure to complete and submit the documents as requested in sections 14.1, 14.2 and 14.3 above at bid closing will result in disqualification.

14.4 SPECIAL CONDITIONS OF CONTRACT

The Bidder needs to Accept all the Special Conditions of Contract by completing the declaration of Acceptance in section 9.3 and attach it as part of the Bid submission.

14.5 RATE CARD OF AREA OF EXPERTISE

The Bidder needs to complete the Rate Card of Area of Expertise Annex D Addendum 2 as per the requirements indicated in Annex A4, section 10.

ANNEX C: ADDENDUM 1

15. BIDDER PRODUCT OFFER

15.1 Bidders must indicate the Product Category they wish to respond to in table 2 below:

Table 2: Information Security products or services Product Categories **(TO BE COMPLETED BY THE BIDDER)** in order to meet the technical mandatory requirement in section 6.

Indicate (using an “X”) the bidder’s Product Category they wish to respond to.

NOTE (1):

Annex C: Addendum 1 must be completed manually and attached with the bid response.

Note (2):

- (a) “OEM/OSM Company” means the Company name who is the registered owner of the product. If a bidder provides an OEM/OSM company name, then
 - (i) the bidder must comply with requirements below, and
 - (ii) the bidder/product will be evaluated for inclusion into the term contract.
- (b) “Product title” means the name of the product or brand as it appears in the OEM/OSM product catalogue. If the bidder intends to offer more than one product per category, then list all the product titles.

Table 2: Bidder Product Offer

Category No	Product Category	Please Tick Product Category (v) (A)	OEM/OSM Company (B)	Product Title (C)
(1)	End point protection	A1	B1	C1
(2)	End point detection and response	A2	B2	C2
(3)	Firewall	A3	B3	C3
(4)	Digital signatures	A4	B4	C4
(5)	Electronic mail protection, archive and	A5	B5	C5

Category No	Product Category	Please Tick Product Category (v) (A)	OEM/OSM Company (B)	Product Title (C)
	journaling			
(6)	Web application protection and proxy services	A6	B6	C6
(7)	Intrusion detection and prevention	A7	B7	C7
(8)	Data loss/leakage prevention	A8	B8	D8
(9)	Vulnerability management	A9	B9	D9
(10)	Identity and Access Management	A12	B12	C12

I, the bidder (Full names) representing (company name) Hereby confirm that understand that it will form part of the contract and is legally binding.

Thus, done and signed at On this.....day of.....20....

.....

Signature

Designation: