SITA SOC Ltd, 459 Tsitsa Street, Erasmuskloof, Pretoria, South Africa • PO Box 26100, Monument Park, 0105, South Africa Tel: +27 12 482 3000 • Fax +27 12 367 5151 • Reg. No 1999/001899/30 • www.sita.co.za

Our Ref: RFP 3174-2025

To whom it may concern

Questions and Answers: Pack 1

RFP 3174-2025: REQUEST FOR PROPOSAL FOR THE PROCUREMENT FOR CYBERSECURITY SOLUTION/S FOR SITA CLIENT FOR PERIOD OF FIVE (05) YEARS.

No.	Questions	Answers
1.	1. Can we confirm that SITA wants all these solutions/products under one service provider? 2. Can we confirm that SITA wants on-premise solutions and not cloud solutions? 3. Lastly, can we confirm that the Email Gateway is also expected to be an on-premises solutions and not a cloud service?	1. The client will contract with one single service provider and not multiple service providers. 2. Yes, the client requires an on-premises solution. 3. Yes, email gateway should be an on-premises solution.
2.	1. What is on your Air Gapped Network? We are having a problem understanding your requirement. One example is that if you require Email Gateway Protection. “Email Routing & Delivery Directs incoming and outgoing emails to the appropriate destination (e.g. server or user). Ensures email delivery to correct recipients using protocols like SMTP (Simple Mail Transfer Protocol).” Mimecast for example is a Cloud Solution, how’s this going to wor?	1. Air Gapped network means there is no connection to the internet. Network is isolated and is for internal staff only. A segmented area is established for updates. The Email Gateway will be implemented on the internet facing network, where email routing and delivery will executed. Mimecast being a cloud solution will not be considered by the client.

	2. With Regards to DLP. How deep do you want to go? Where does data loss prevention start and stop in terms of services, backups, EDR with ransomware rollback.	2. The DLP solution will cover all our client's data. Desktops, laptops, cellphones, USBs, servers, backups, EDR with ransomware rollback and all applications such as email etc.
3.	a). Please kindly confirm if Trellix is the preferred technology vendor for this tender. We ask because the scope of work seem to suggest that. In fact, it is clearly demonstrated by the requirement 1.26 End Point Protection for Insights for profiling "Top Attacks" with guidance to improve protection, and access to deploy Anti-Virus Strategic Innovation Alliance (SIA) partner products." Strategic Innovation Alliance (SIA) is a Trellix initiative to support integration of 3rd party products in to Trellix's endpoint management console, ePolicy Orchestrator. As such it is only applicable to Trellix solutions. Furthermore, there are additional instances of Trellix based terminology used such as Adaptative Threat Protection - 1.9. "Endpoint Security with Adaptive Threat Protection."; Threat Intelligence Exchange - 1.13 "Local threat intelligence Exchange" Please do confirm if Trellix is the designated technology vendor. b). Technical Scoring Methodology – Unfair Elimination of Compliant Bidders. Another concern is the scoring system. The minimum technical threshold required to progress/be considered is 80%. This combined with the scoring system where meeting the core requirements in each section only results in 3 points out of 5 means that even if all the core requirements are met you would only achieve 60% and be disqualified . To score more than 3 points in a section, you have meet all the core requirements and all the non-core requirements. In which case you would score 5. Failure to meet even one non-core requirement means a maximum of 3 out 5 points and if even one core functional requirement is missed then you score 0. In some areas there are 25 to 35 core requirements which means even having over 90% of the functionality would result in a zero score.	a. No, Trellix is not the preferred technology vendor for this tender as a single-source-method of procurement is not used for the bid. The wording Strategic Innovation Alliance (SIA) used is common language used in information technology cyber security field. Strategic Innovation Alliance (SIA) is a capability and not necessarily a specific product, referring to the use of different products to achieve a strategic goal. Vendors could use different products to achieve the bid requirement. Please, note that ePolicy Orchestrator was not mentioned in the tender. The Endpoint Security with Adaptive Threat Protection (ATP) and Threat Intelligence Exchange, refers to advanced endpoint protection, adaptive capabilities, and robust threat intelligence, capabilities that are provided by most cybersecurity solutions. b. The minimum scoring threshold for Stage 3: Technical Functional requirements and Stage 4: Proof of Concept has been updated to 60% per stage. The revised Bid Specification has been published on the SITA website and eTenders portal.

	<u>In summary</u> 1. It is mathematically **impossible** to reach the **80% threshold by meeting all core requirements** . This is unheard of in standard SCM practice, where a bidder can fully satisfy the mandatory "core" functionality and still be disqualified. 2. It contradicts the principle of equal treatment and proportional scoring. 3. It constitutes "restrictive and unfair scoring criteria", which violates: • PFMA Section 38(1)(a)(iii) 1. "Effective systems of procurement must be fair, equitable, transparent, competitive and cost effective." • PPPFA and 2017 Preferential Procurement Regulations 1. "Evaluation criteria must not be designed in a manner that limits competition or creates discriminatory scoring outcomes." 2. This scoring mechanism is, by design, exclusionary and unfairly eliminates a majority of prospective bidders.	
4.	Will a further extension be granted or the 8 th is the final submission date?	The closing date of the bid has been extended to 20 January 2026, then again to 23 January 2026.
5.	Can bidders propose a multi-vendor or consortium solution where different OEMs provide different components (e.g., Endpoint Protection, XDR, DLP, NDR, Email Security, Web Gateway), or must all functionalities be provided by a single OEM/OSM?	Refer to Technical mandatory requirements No 5. One single vendor must provide the required solution using a single or multiple **products OEM/OSM.**
6.	Please confirm whether the XDR platform must operate entirely offline including local correlation, analytics, threat intelligence, or if cloud-assisted analytics are permitted.	XDR platform to be hosted on-prem and all analysis should be done onprem. No logs should leave the environment to be analyzed on the cloud.
7.	Please confirm what security technologies are currently deployed for Endpoint, EDR, Email Security, Web Gateway, DLP, NDR/IDS/IPS, and SIEM.	SITA cannot disclose that information.

8.	Does the customer currently have a centralised security management environment (e.g., ePO, Forcepoint Security Manager, Cisco SMA)?	Yes, in terms of endpont security
9.	Please confirm whether bidders are expected to provide a SIEM platform or integrate with an existing SIEM only.	Siem was not specified
10.	Please confirm that SOC, MDR, or security monitoring services are not part of the required scope.	No, not part of the scope.
11.	Please confirm whether manual offline updates via USB or isolated management network are required for updating signature files, engines, threat intel, sandbox models, and device reputation databases. Will this be performed by SITA?	Yes, the client will perform the updates
12.	Please confirm whether flow-based NDR (NetFlow/IPFIX) is acceptable or if packet-based NDR is required.	Packet-based NDR is required
13.	Please confirm whether NDR appliances may be virtual or if physical appliances are mandatory.	NDR appliance can be virtual or Physical
14.	Please confirm whether a single unified DLP platform is required, or if separate DLP modules per channel are acceptable.	Single Unified DLP platform is required
15.	Has any data Classification been done - if so please specify.	Yes
16.	Please confirm that the Web Gateway must operate exclusively on-premises with on-prem SSL inspection, URL categorisation, anti-malware, sandboxing, and zero cloud connectivity.	Web gateway will be installed on internet facing environment. Yes all the features are required and analysis should be done on-prem. No cloud solution will be required.
17.	Please confirm whether the Email Gateway must function as a full MTA within the ringfenced environment.	Yes

On behalf of SITA