



sassa

SOUTH AFRICAN SOCIAL SECURITY AGENCY

RESPONSE TO BIDDER QUERIES

Terms of Reference
07 July 2025

SASSA: 01-25-ICT-HO

Contents

RESPONSE TO BIDDER QUERIES	1
07 July 2025.....	1

QUESTIONS AND ANSWERS

The Terms of Reference indicated that SASSA would respond to the enquiries eight working days after the bid advertisement date.

Number	Bidder	Bidder Query	SASSA response
1.	Lucysecurity (Malcolm West)	We have some background observations leading to several questions: - The title is "Cyber Security Awareness and Training Solution". This is a well understood market segment where buying organizations can obtain good value via competitive tender with a likelihood of 10+ vendors responding to a typical technical specification. However, when we review your specification we note that, in addition to a core typical Awareness and Phishing scope you have also requested further features which are more usually found in Email security platforms (which are more commonly part of an organizations IT infrastructure). The particular features to which we refer are: - section 4.4 Advanced Email Threat protection - section 4.1 the parts referring to Monitoring of Risky Behaviours and escalating alerts on these. - Including these elements in your specification in a two stage tender (technical compliance first, then financial) without indications about requirement priorities (Must have, Should have, Could have, Won't have) will likely mean that vendors would treat all requirements as Must have. As only one, or possibly two, vendors in the market can provide the entire feature combination you have specified, this will likely result in most vendors not bidding as they cannot pass the technical compliance step.	We appreciate your feedback regarding the inclusion of advanced features such as Advanced Email Threat Protection and Monitoring of Risky Behaviours. These elements were intentionally included to reflect SASSA's broader strategic objectives in strengthening its cyber resilience posture. While the core focus remains on awareness and phishing simulation, the additional capabilities are considered complementary and valuable in achieving a holistic solution. In response to your questions: Requirement Prioritization We acknowledge the importance of clarity in requirement prioritization. While the TOR does not explicitly categorize features as "Must have", "Should have", etc., vendors are encouraged to highlight their compliance levels and provide commentary on feature availability. This will assist the evaluation panel in assessing technical merit and alignment with SASSA's operational needs. Alternate Proposals Yes, alternate proposals will be considered, provided they are clearly marked and accompanied by a rationale explaining how they meet the intent of the TOR. Vendors who are submitting alternate proposals should clearly label them as "Alternate Proposal" to ensure proper evaluation.

		We further note that the vendors that can support the combination of features you request do so with their premium offerings, which are priced at around 10x the usual tender market rate for Awareness and Phishing only. Question 1 - Can you please advise on the relative importance of the functionality shown in the specification (section 4 of the Terms of reference)? Ideally with a Must have, Should have format. Or alternatively please confirm that you are only interested in a vendor who can provide the total set of functionality you have specified. Question 2 - Will you accept alternate proposals, or will you only accept fully technically compliant proposals? If alternate proposals are acceptable can you please confirm if you require any different labelling for their submission.	
2.	Mitigate (Eyal Tevet)	Section 4.4 (below) seems to be out of place and is looking for an e-mail security solution: 4.4. Advanced Email Threat Protection 4.4.1. Automatic Blocking of Email Threats: The solution must automatically block email threats that bypass existing security measures. 4.4.2. Crowdsourced and AI-Driven Threat Intelligence: The solution should enhance email security using crowdsourced intelligence and AI-based blocklisting. 4.4.3. Automated Quarantine and Safe Simulations: The solution must quarantine malicious emails and convert reported phishing attempts into safe simulations. Question 1: As I understand, Sassa already has an e-mail	We appreciate your close review of the Terms of Reference and your observations concerning Section 4.4, which outlines requirements for Advanced Email Threat Protection. In response to your questions: Clarification on Email Security Scope SASSA does currently operate an enterprise email security solution as part of its broader cybersecurity infrastructure, specifically e-Purifier and Microsoft O365. The inclusion of Section 4.4 in the TOR is intended to ensure that the proposed awareness and training solution can interface effectively with existing email security systems. Specifically, we are seeking a solution that can:

		security solution. Are you looking for an e-mail security solution as described in 4.4 , or merely for the user awareness training and simulation solution to be able to integrate with your existing e-mail security solution so that your existing e-mail security solution can take the blocking actions? Question 2: What is your existing e-mail gateway security solution?	• Leverage threat intelligence and simulation capabilities to enhance user awareness. • Integrate with existing email gateways to support safe simulations and reporting workflows. Enhance user awareness through realistic simulations and reporting workflows. • Integrate with current email gateways to support safe simulations and threat visibility. • Provide visibility into user behaviour and support escalation mechanisms for risky actions. Integrate with current email gateways to support safe simulations and threat visibility. 2. Existing Email Gateway Security Solution As noted above, SASSA utilizes e-Purifier and Microsoft O365 as part of its email security environment. Any proposed solution should be compatible with these platforms and capable of supporting awareness and simulation features that align with our cybersecurity objectives. Therefore, the requirement is not for a full standalone email security platform, but rather for a solution that can complement and integrate with our current environment. We trust this clarifies the intent behind Section 4.4 and encourages your continued engagement in the tender process.
--	--	---	--