SITA RESPONSE TO THE MEDIA ENQUIRY FROM GROUNDUP NEWS

1. Does SITA acknowledge that all hosts that fall under the SITA ASN, AS37130, are SITA-managed or SITA-associated infrastructure?

Not all hosts that fall under SITA ASN are managed by SITA.

2. What percentage of hosts under the ASN are directly managed by SITA, and how many are managed by other government departments, municipalities, and third-party service providers?

It is estimated that 37% across the end-to-end value chain of services at National and Provincial level are provided and secured by SITA. This is because SITA does not provide all services in the value chain, with the remaining estimated 63%, being the responsibility of respective government departments.

3. Does SITA maintain a complete, current inventory of all internet-facing systems in its ASN?

Yes.

4. How often does SITA perform external attack-surface monitoring of its ASN?

There is a monthly vulnerability scanning process for all the SITA hosted websites.

5. Are all public facing systems in the ASN required to have a named technical owner/business owner that can be held accountable for any issues?

Yes.

6. What process exists for removing or decommissioning forgotten, unused, or legacy internet-facing services?

As part of a risk management process forgotten, unused, or legacy internet-

facing services are removed following approval from owner departments / entities.

7. What is SITA's required patch timeline for internet-facing systems with critical or high-severity vulnerabilities?
The vulnerability remediation process in place that is executed, following approval from owner departments / entities before the systems or vulnerabilities are patched.

8. What enforcement mechanism exists if a department or vendor fails to remediate a serious vulnerability?

There is continuous robust engagement with owner departments / entities as part of a risk management process to ensure the vulnerabilities are treated and mitigated.

9. Does SITA have a central vulnerability management programme covering all public-facing systems in its ASN?
The vulnerability management process in in place covering all websites managed by SITA.

10. Does SITA have authority to force remediation when a department-owned service creates risk inside SITA-hosted infrastructure?
No SITA does not have that authority.

11. What cybersecurity standards must departments meet to host systems on SITA infrastructure?

SITA has invested in building a government private cloud and all the systems hosted in the Cloud must follow the internal standard ensuring that only compliant technologies are used.

12. Has SITA performed a recent audit of exposed public-sector services in its ASN?

There is continues vulnerability scanning for all the SITA hosted systems and some have pen testing Service Level Agreements with SITA to ensure continuous risks assessment and mitigation actions.