RFP Number : AGSA/01/2025

Request for Proposal (RFP) for the appointment of a service provider for the provision and deployment of a Network Access Control (NAC) solution including configuration, maintenance and support for a period of forty (40) months

Auditing to build public confidence

AUDITOR-GENERAL SOUTH AFRICA

No.	Question/ Clarification	Type	Response
1	Provide a list of all technologies and/ or infrastructure that is currently deployed in the AGSA which is relevant to the NAC solution.	Technical	The following is a list of technologies and infrastructure currently deployed at AGSA that are relevant to the Network Access Control (NAC) solution: **1. Network Infrastructure:** > Switches & Routers: Cisco and Aruba > Wireless Access Points: Aruba (managed via Aruba Airwave) > Firewalls: Palo Alto Networks > Network Access Control (NAC) (Current State): No dedicated NAC solution in place, making this implementation a priority **2. Identity & Access Management:** > Active Directory (AD): Microsoft Active Directory (AD) for user authentication and policy enforcement > Identity Provider (IdP): Azure AD > Multi-Factor Authentication (MFA): Microsoft Authenticator **3. Endpoint & Security Infrastructure:** > Endpoint Protection: Microsoft Defender for Endpoint > Operating Systems: Windows 10/11 (for workstations) and Windows Server (various versions) > SIEM (Security Information and Event Management): Microsoft Sentinel > Vulnerability Management: Tenable Nessus **4. Virtualisation & Cloud Infrastructure:** > Hypervisor: VMware ESXi > Cloud Services: Microsoft Azure (various workloads) > IaaS and DRaaS: Migration in progress, currently a mix of on-premises and cloud workloads **5. Authentication & Access Control:** > 802.1X Authentication: Required for wired and wireless network access > RADIUS Server: Microsoft NPS (currently in use for authentication) > Certificate-Based Authentication: Internal PKI for secure device authentication **6. Integration & Monitoring:** > Network Monitoring: Site24/7 > Log Management: Microsoft Sentinel & Syslog servers This list provides a high-level overview of AGSA's relevant infrastructure that may require integration with the NAC solution.
2	"Appendix A, BRQ08, Integration with Existing and Planned Systems" – provide a response to elaborate what the expectation is for integration.	Technical	AGSA's existing infrastructure uses a combination of network, security, identity management, and monitoring solutions that require the following integration protocols: **Network Infrastructure Integration** > Cisco & Aruba Switches/Routers & Aruba Airwave (WAPs): Supports SNMP, RESTful APIs, and CLI-based integration. > Palo Alto Firewalls: REST API, XML API for configuration automation, and syslog for logging. **Identity & Access Management Integration** > Microsoft Active Directory (AD): Supports LDAP, LDAPS (for secure directory queries), and Kerberos authentication. > Azure AD & Microsoft Authenticator (MFA): Integrates via OAuth 2.0, OpenID Connect (OIDC), and SAML 2.0 for Single Sign-On (SSO) and authentication. > Microsoft NPS (RADIUS Server): Uses RADIUS protocol for authentication, with optional REST API support for enhanced integration. **Security & Endpoint Protection Integration** > Microsoft Defender for Endpoint: REST API for security event correlation and endpoint policy management. > Tenable Nessus (Vulnerability Management): JSON-based REST API for vulnerability scanning and risk assessment. **Virtualisation & Cloud Infrastructure Integration** > VMware ESXi (Hypervisor): Supports vSphere API (SOAP & REST) for virtual machine and network policy management. > Microsoft Azure (Cloud Services & IaaS/DRaaS Migration): Uses REST API, Graph API (for identity-related services), and Webhooks. **Authentication & Access Control Integration** > 802.1X Authentication: Requires RADIUS (Microsoft NPS) integration for wired and wireless access control. > Certificate-Based Authentication (Internal PKI): Uses TLS, OCSP, and CRL-based validation for secure authentication. **Monitoring & Log Management Integration** > Microsoft Sentinel (SIEM): REST API, syslog ingestion, and KQL queries for security event monitoring. > Site24x7 (Network Monitoring): Supports REST API and SNMP for real-time network visibility. The NAC solution must support RESTful APIs, SNMP, RADIUS, LDAP/SAML, syslog ingestion, and cloud-native authentication mechanisms (OAuth, OIDC) to ensure seamless integration across AGSA's infrastructure.
3	**5.2.4. Compliance with technical requirements for a NAC solution.** **(Refer to appendix A for detailed information)** Will the OEM data sheet suffice as a suitable cross reference and evidence?	Technical	Bidders are required to complete **appendix A** and indicate whether their proposed solution is compliant with the AGSA requirements or not. The written confirmation must be fully completed and signed off by the bidder's authorised signatory, i.e. an individual who signed-off the RFP documents. Bidders are also welcome to cross reference to their proposed solution functionalities or OEM data sheet as additional evidence where possible. This cross-referencing must be clearly indicated in the column provided in **appendix A**, **column E** which read Substantiating Details/ Comments (Bidder to provide page, section, and topic reference where their proposal supports each of the requirements stipulated below).
4	**5.2.5 Training and knowledge transfer to AGSA technical team members.** What type of training is required?	Technical	The bidder must provide a detailed plan and training material outlining how they will provide training to twenty (20) AGSA technical team/ staff members. The plan must include the transfer of knowledge and skills to the AGSA's staff to ensure that the AGSA personnel are fully capable of managing and maintaining the NAC solution post deployment. This includes comprehensive training to familiarise the relevant teams with the system's configuration, monitoring, and troubleshooting capabilities and the training will be throughout the contract period as and when the need arises.
5	**5.2.2 Skills and experience of resources that will be assigned to the project reflecting number of years' experience in the implementation and configuration of the NAC solution.** If engineers have one or more professional certifications of the examples provided, will this be acceptable?	Technical	Yes, the AGSA requires at least one engineer to possess at least one relevant OEM cetification. Therefore, as long as one engineer has one of the relevant OEM certificates, the bidders will be allocated 10, 8, 5 or 0 points in accordance with the criteria 2 scoring as stated in **appendix B**.