

TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY

**BUSINESS REQUIREMENTS**

TECHNICAL SECURITY REQUEST FOR INFORMATION  
ON SECURITY TECHNOLOGY

JUNE 2020

## TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY

**1. INTRODUCTION**

The South African Revenue Service (SARS) has administrative buildings, branch offices, ports of entry and other critical facilities country wide where business processes are conducted in order to collect revenue due to the fiscus in line with organisation's mandate.

To achieve the above the SARS Commissioner has mandated The National Security Management Unit (NSMU) to providing protection for SARS people, assets, facilities and ensure compliance to business processes in as far as it affects theft or sabotage of SARS assets. The NSMU aims to deliver a differentiated risk based security service, which is based on legislative requirements, business imperatives and flexible to be responsive to organisational changes.

SARS has deployed technical security in over one hundred and fifty (150) mobile and static sites. These sites are monitored at a site level, regional level, and national level. SARS requires modernised security technology that will enable seamless monitoring at all levels and sharing of information or integration with other organisational functions.

**2. SCOPE OF INFORMATION REQUIRED**

The primary objective of the RFI is for SARS to investigate available modern security technology that is aimed at facilitating a safe and secure working environment. The technological security solution is based on the technical security systems model, **See Annexure A.**

**3. TECHNOLOGY APPLICATION**

The below table is a guide of possible technology that is required but should not limit the responder.

## TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY

<b>Barriers Deterrent Security Systems</b>	<b>Access Control Security Systems</b>	<b>Detection and Assessment Systems</b>	<b>Emergency Security System</b>
<ul style="list-style-type: none"> <li>• Perimeter fence</li> <li>• Energised coil</li> <li>• Boom gates</li> <li>• Turn stiles</li> <li>• Security windows</li> <li>• Hardened doors</li> <li>• Window screens</li> <li>• Electric fence</li> <li>• Tyre Spikes</li> </ul>	<p><b>Access control that include but not limited to the following:</b></p> <ul style="list-style-type: none"> <li>• Visitor management</li> <li>• Key control management</li> <li>• Time management and attendance</li> <li>• Parking Management System</li> <li>• Automatic Licence Plate Recognition</li> <li>• Protect sensitive data from tampering, malware</li> <li>• Fully customizable capabilities</li> <li>• Support automated fault reporting on software and hardware</li> <li>• Support HID reader hardware, smart card readers and biometric</li> <li>• Support remote management and a centralised SQL and or DB2 Enterprise</li> </ul>	<p><b>Alarm system</b></p> <ul style="list-style-type: none"> <li>• alarm response should trigger audio and/or visual messages</li> <li>• system should be able to make email or text message notifications</li> <li>• centralized alarm handling and reporting</li> <li>• Have the ability to integrate into a 3rd party centralised access control solution</li> <li>• Support automated fault reporting on software and hardware</li> <li>• System should support Dual connections e.g. GSM and TCP/IP</li> <li>• Support remote equipment diagnostics</li> <li>• Protect sensitive data from tampering, malware</li> <li>• Fully customizable capabilities</li> </ul> <p><b>Close Circuit Television</b></p>	<p><b>Emergency Panic Solution and Evacuation Management systems</b></p> <ul style="list-style-type: none"> <li>• Have the ability to integrate into a 3rd party centralised access control solution</li> <li>• Send a distress SMS detailing the user's location to emergency contacts</li> <li>• Have the ability to track a cell phone anywhere in South Africa</li> <li>• Available 24hours a day</li> <li>• Have a centralized monitoring software</li> <li>• Electronic Occurrence Book which includes an Incident management system, a risk management system with an ability to</li> </ul>

## TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY

	<ul style="list-style-type: none"> <li>• Support MS Active Directory</li> <li>• Logical Access integration</li> </ul>	<ul style="list-style-type: none"> <li>• Have the ability to integrate into a 3<sup>rd</sup> party centralised access control solution</li> <li>• Support remote management and a centralised SQL, SQLand or DB2 Enterprise</li> <li>• Support automated fault reporting on software and hardware</li> <li>• Must provide for Audit trails on access logs, Remote diagnostics and single point access</li> <li>• adherence to SARS Enterprise IT architecture software standards(Benny to Confirm)</li> <li>• Support network storage</li> <li>• Allow for video walls, multi viewers and matrix switchers</li> <li>• Protect sensitive data from tampering, malware</li> <li>• Fully customizable capabilities</li> <li>• Must allow multiple operators to view the same video and graphic feeds at exactly the same moment, with no encoding delay or variation.</li> </ul>	<p>generate operational and strategic reports and dashboards.</p>
--	---	---	---

## TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY

		<p><b>Asset Tracking</b></p> <ul style="list-style-type: none"> <li>• Track the movement of assets in and out of premises</li> <li>• Have the ability to integrate into a 3rd party centralised access control solution</li> <li>• Support remote management and a centralised SQL, SQLand or DB2 Enterprise Support automated fault reporting on software and hardware</li> <li>• Must provide for Audit trails on access logs, Remote diagnostics and single point access</li> <li>• adherence to SARS Enterprise IT architecture software standards</li> <li>• Protect sensitive data from tampering, malware</li> <li>• Fully customizable capabilities</li> <li>• Guard Patrol devices <ul style="list-style-type: none"> <li>• Walk- through Metal as well as hand held detectors</li> </ul> </li> <li>• <b>Bag Scanners</b></li> </ul>	
--	--	---	--

## TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY

**4. INTEGRATION**

The Integrating system must adhere to the SARS Enterprise IT architecture software standards. It will be the main platform and must interface between various security systems.

**All required licencing must be clearly stipulated in the proposal, providing option enterprise, client or group licences.** The identified system should be scalable with the following features:

- Ability to integrate with the following 3<sup>rd</sup> party security systems; CCTV, alarms, perimeter fencing, asset tracking, Number Plate Recognition software, Metal Detectors, Turnstiles; Access Control;
- Integrate with SAP HR, Vetting systems;
- Must provide for Audit trails on access logs, Remote diagnostics and single point access
- The integrating system must provide an ability for an operator to view all subsystems on one monitor for quick response.

The technological security solution should include CCTV, Alarm and Access control systems that will be deployed at SARS facilities, high risk areas, mobile vehicles and can be utilised on mobile devices. It must further be able to integrate parking, key management, BMS, fire alarms, HR management, time management, visitor management and emergency alarms systems.

**5. SPECIAL REQUIREMENTS**

SARS requires a proposal that will detail a refresh and a hybrid acquisition model. The hybrid model includes SARS ownership of technical security systems deployed at high-risk facilities and the acquisition of technical security systems for medium and low-level risk facilities through lease agreements.

**6. TRAINING**

The Responder must include all details on the training availability on all proposed systems and equipment.

TECHNICAL SECURITY REQUEST FOR INFORMATION ON SECURITY TECHNOLOGY