

- 7.1 Considering the above, it is recommended that the Departmental Bid Adjudication Committee approves the procurement of SITA services for Network connectivity and hosting of IJS Transversal Datacentres (Production and Distater Recovery) for a period of two(2) years.

DEPARTMENTAL BID ADJUDICATION COMMITTEE		
APPLICATION APPROVED <del>NOT APPROVED</del>		
NAME AND SURNAME	SIGNATURE	DATE
<del>Nicholas Mungu</del>	<del>[Signature]</del>	<del>27/08/2020</del>
Terence Rosendo	[Signature]	27/08/2020
Lufino Mumbisi	[Signature]	27/8/2020
ANDRÉ MALAN	[Signature]	27/8/2020
N Mthembu	[Signature]	27/8/2020

*Handwritten signature*



Proposal for Connectivity and Server  
Accommodation Facilities Services for  
Integrated Justice System, by the State  
Information Technology Agency SOC Ltd

Document No:	9492_INC19929038
Revision:	1.0
Author	Mmathapelo Rakgantsho
Effective Date:	On Date of Signature
Electronic File:	9492_INC19929038

## Notice

© 2020 SITA. All rights reserved.  
No part of this document may be reproduced or transmitted in any form or by any means  
without the express written permission of SITA SOC Ltd.

Document enquiries can be directed to: Customer Relationship Manager  
SITA SOC Ltd. P.O Box 26100, MONUMENT PARK, 0105, SOUTH AFRICA

Attention: nonhlanhla.duma@sita.co.za  
Telephone: +27 12482 3063

## Approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.



Michael Thage  
Acting Head of Department: Products, Services and Solutions  
State Information Technology Agency

22/01/2020

Date

On behalf of the Integrated Justice System and duly authorised thereto

Date

## Foreword

This document contains information regarding SITA's service offering to the Integrated Justice System. It does not form part of any other document, nor does it replace or supersede any other document.

The document is applicable to the management of the Integrated Justice System who shall be required to, should they elect for SITA to continue with the project, sign their approval of this document and place a formal order on SITA who shall be responsible for executing the project.

The document has been drafted according to the conventions as stipulated in the formal SITA document layout, writing and typing standard.

## References

1. SITA Network and Communication Security Policy available at: <http://www.NGN.gov.za/policy/SecPolJan2001.doc>
2. Minimum Information System Security Instructions
3. SITA Amendment Act (Act number 38 of 2002)
4. RIC Act

## Non-Disclosure

1. On receipt of a SITA proposal the client undertakes to:
  - a) keep confidential all information (written, including information contained in electronic format, or oral) concerning the business and affairs of SITA that it shall have obtained or received from SITA through the relevant document/agreement;
  - b) not disclose nor change the information in whole or in part to any other person save its employees involved in the implementation of this agreement, and who have a need to know the same without SITA's written consent; and
  - c) use this information solely in connection with the implementation of this agreement/document and not for its own benefit or that of any third party.
  
2. The provisions of paragraph 1 above shall not apply to the whole or any part information to the extent that it is:
  - a) already known to the recipient without obligation of confidence;
  - b) independently developed by the recipient;
  - c) publicly available without breach of this agreement;
  - d) rightfully received from a third party;
  - e) released for disclosure by the disclosing party with its written consent; or
  - f) required to be disclosed in response to a valid order of court or other governmental agency or if disclosure is otherwise required by law.

## CONTENTS

---

1.	Introduction .....	5
2.	Scope .....	5
3.	Service Components .....	5
4.	Service Exclusions .....	6
5.	Risks .....	6
6.	Benefits statements / Value Proposition .....	6
7.	Roles and Responsibilities .....	6
8.	High-Level Implementation Plan.....	8
9.	Service Governance .....	8
10.	General .....	9
	Annex A: Financial Implication.....	10
A1	Site List .....	10
A2	Once-Off Cost .....	10
A3	Monthly Recurring Cost.....	10
A4	Summarized Service Cost .....	11

## 1. Introduction

The Integrated Justice System (IJS) currently has a production datacentre hosted at Numerus, SITA building. The IJS Hub operated 24x7, 365 days a year and provides critical services for its member departments. For business continuity purposes the IJS need a failover Disaster Recovery (DR) site in case of a disaster.

The IJS has requested the State Information Technology Agency (SITA) to provide them with a solution proposal for Connectivity and Server Accommodation solution to ensure that the full requirement for the IJS is met.

SITA values the opportunity to provide the IJS with a proposal to accommodate their request.

## 2. Scope

SITA will provide the IJS with a Server Accommodation and Connectivity solution at the Midrand Data Centres. This will ensure that:

The following requirements will be executed accordingly:

- a) Server Accommodation
  - i. The Integrated Justice System (IJS) needs a basic hosting solution, at a level of at least Tier III (preferably Tier IV) to house physical IT infrastructure consisting of seven (7) cabinets which includes power, cooling and floor space.
- b) Virtual Private Network (VPN) Network Connectivity

## 3. Service Components

- a) The service consists of the following features:
  - i. Floor space
  - ii. Physical Security
  - iii. Biometric access (only at Midrand data centre)
  - iv. Access & Climate control
  - v. Power & Emergency power
  - vi. Fire & Surge protection
- b) Facilities at permanent core SITA Switching Centres
- c) SLA Reporting (individual client reports)
- d) 24/7 service
- e) Monitoring and Reporting
  - i. 24/7 Monitoring
  - ii. Reporting on service levels and usage
- f) Cage Infrastructure
- g) Server Accommodation
  - i. 7 Cabinets
- h) Connectivity
  - i. Final pricing will be provided on completion of the formal SITA RFQ process and quoted separately to IJS from this proposal.
    - 1. SALU Building, 316 Thabo Sehume Street, Pretoria CBD (50Mbps)
    - 2. Numerus Building, 99 Hamilton Street, Pretoria (50Mbps)
    - 3. CLOUD (NDC2) Centurion, (50Mbps)
    - 4. CLOUD (NDC2) Numerus, replication link traffic (100 Mbps)
  - ii. Three (3) category B routers

## 4. Service Exclusions

The following are excluded from the service offering:

- a) Establishment of core switch infrastructure (this requirement is dealt with in a sub project and will be quote separately of this proposal);
- b) Professional Service (this requirement is dealt with in a sub project and will be quote separately of this proposal);
- c) Move, installation, connection and configuration of servers;
- d) Server Support and Maintenance will be the responsibility of the Department;
- e) The daily management of any hardware and software;
- f) Management, technical support, administration and maintenance of the application and the integrity of data, will be the responsibility of the Department;
- g) The provisioning of all hardware and software assets;
- h) Application Enhancements;
- i) The licensing of any database, application software, integration toolsets or any other software not covered within this service offering as part of the proposed solution;
- j) Migration of applications is not covered within this service offering as part of the proposed solution;
- k) Third Party Support; and
- l) Backup of the current environment.

## 5. Risks

SITA will not provide internet connectivity for the IJS. The Current IJS internet breakout will stay at Numerus building and will migrate to SITA as phase 2 of the project.

## 6. Benefits statements / Value Proposition

	Business challenge	Value statement	
		Area	Statement
1	High cost of: <ul style="list-style-type: none"> <li>• Building and maintaining your own server room/ data centre.</li> <li>• Implementing and maintaining server room standards.</li> </ul>	Cost savings	<ul style="list-style-type: none"> <li>• Data Centre Facility services removes the burden from Government departments to maintain facilities, security and uptime.</li> <li>• Shared capability for multiple customers housing servers in the shared facilities, result in lower unit cost based on shared infrastructure and bulk discounts.</li> </ul>
2	Safeguarding of Government ICT against unauthorised access, power outages and environmental factors.	Security and Reliability	<ul style="list-style-type: none"> <li>• The Department's ICT infrastructure will be securely housed in a Tier IV data centre with redundant power, fire suppression, biometric access, CCTV video surveillance and physical security.</li> <li>• Secure access control to approved individuals, based on client policy, limits unauthorised access.</li> <li>• Colocation allows Government to bring its own hardware to a secure facility shared only by Government.</li> </ul>

## 7. Roles and Responsibilities

### 7.1 Server Accommodation Facilities

Service Component	SITA Responsibilities	Customer Responsibilities
Server Accommodation (Tier IV Data Centre)	<ol style="list-style-type: none"> <li>1. SITA will provide access to the servers when required by the Client through the SITA toll-free number (0800 11 55 75), 24/7.</li> <li>2. Ensure that the SITA Incident, Request and Change Management processes are followed (as may be communicated by SITA to the Client from time to time) under the auspices of SITA.</li> <li>3. SITA reserves the right to physically disconnect the server from the WAN Network during any virus infestations.</li> </ol>	<ol style="list-style-type: none"> <li>1. Report all identified Server Accommodation related incidents via the SITA Toll free number (0800 11 55 75) including request for access to servers.</li> <li>2. Ensure that the SITA and Client Incident, Request and Change Management processes are followed for service provisioning, upgrades and/or service de-provisioning.</li> <li>3. Change requests to be provided to SITA in writing.</li> <li>4. Adhere to SITA's access approval processes for access rights into SITA's Data Centre facilities.</li> <li>5. Adhere to SITA's facility access control policies.</li> </ol>

Service Component	SITA Responsibilities	Customer Responsibilities
	<ol style="list-style-type: none"> <li>4. SITA further reserves the right to audit the server to determine if the latest operating system service packs and security patch levels are installed.</li> <li>5. Establish and maintain processes for incident (fault/problem) and change management.</li> <li>6. Provide tools to support the service management processes.</li> <li>7. Service reporting reflecting Server Accommodation Facilities availability.</li> </ol>	<ol style="list-style-type: none"> <li>6. Ensure that a suitable Anti-virus solution is installed on the server and configured to update itself from a reputable source.</li> <li>7. Server Support and Maintenance remains the responsibility of the Client.</li> <li>8. Inform SITA in writing of any Client initiated change controls that will affect the Server Accommodation service.</li> <li>9. Provide the specifications of the equipment to be hosted by SITA for approval by SITA prior to deployment.</li> <li>10. Provide reasonable advance notice to SITA should the Client elect to audit the environment in which its equipment is hosted, and to agree to the reimbursement of SITA's reasonable expenses in taking part in such an audit.</li> <li>11. Maintain any hosted equipment in accordance with the OEM specifications for such equipment.</li> <li>12. Provide SITA with ongoing server accommodation capacity requirements.</li> <li>13. Provide SITA with a formal change request should there be a requirement to deviate from the rack or floor space requirements.</li> </ol>

## 7.2 VPN Service

Service Component	SITA Responsibilities	Customer Responsibilities
VPN	<ol style="list-style-type: none"> <li>1. Establish, operate, monitor and manage VPN services.</li> <li>2. Operate, monitor and maintain Core infrastructure.</li> <li>3. Ensure sufficient core bandwidth capacity to cater for VPN Customers.</li> <li>4. Inform the Customer of any change requests on the WAN infrastructure (downtime or disruptive changes) at least 5 working days in advance of such change. No penalties will apply during this downtime period.</li> <li>5. Execute and resolve Service Request Applications.</li> <li>6. Present quotations to Customer on receipt of an official URS.</li> <li>7. Process orders for procurement and installation of access link infrastructure on receipt of an official Government Order.</li> <li>8. Manage application process for data lines to TelCo.</li> <li>9. Provide the necessary access connectivity from Customer sites to SITA NGN.</li> <li>10. Acquisition, supply, installation, configuration and management of Customer edge hardware and software requirements (including power management) in compliance with SITA's recommended standards.</li> <li>11. Hardware maintenance and support on SITA-owned site equipment.</li> <li>12. Establish and maintain processes for VPN fault, incident and change management.</li> <li>13. Service reporting reflecting end-to-end operational performance statistics.</li> </ol>	<ol style="list-style-type: none"> <li>1. Inform SITA of any Customer initiated change controls that will affect the SITA Wide Area Network (WAN) service.</li> <li>2. Provide approved Security Policy that will govern the VPN, inclusive of the Rules of Access required for configuring the Internet Gateway.</li> <li>3. Submit completed and signed Service Request Applications to SITA.</li> <li>4. Issue SITA with an official government order on acceptance of a SITA proposal or quotation for Ad Hoc access link services.</li> <li>5. Advising SITA of significant changes in usage forecasts, planned implementation of future changes or new service requirements where SITA will be impacted.</li> <li>6. Downtime experienced due to power related issues on the Customer sites will not be added to any SLA downtime measurements.</li> <li>7. Report all identified VPN relation calls via the SITA Toll free number (0800 11 55 75).</li> </ol>

## 8. High-Level Implementation Plan

The solution, including the planning, migration and support of the network, is managed using experienced Project Managers with detailed project plans for the VPN migration activities to ensure a smooth migration, with limited impact to the Customer. Downtime to users is minimised and Change Management principles and procedures form a huge part of the migration, ensuring that the Customer is aware of all planned changes and roll-back plans associated with the specific changes.

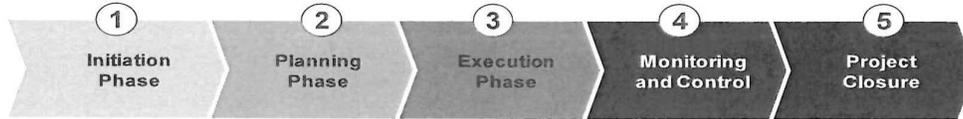


Figure 1: High-level implementation process

### 1) Initiation Phase

The Initiation Phase begins when the proposal has been signed and a Government order has been submitted to SITA by the department. In this phase the project charter will be developed and approved by the department and SITA. The project team for the implementation will also be appointed.

### 2) Planning Phase

The Planning Phase begins when the Project Charter has been formally approved by the department. The charter contains the project work break down structure which defines specific tasks and sub-tasks, including the identification of project deliverables and assignment of allocated resources to each task. Milestones are established together with specific plans for management and governance of the project to guide ongoing project execution and control.

### 3) Execution Phase

The Execution Phase involves implementing the Project Charter and includes reviewing the deliverable quality and measuring each deliverable produced against the acceptance criteria. As deliverables have been implemented and accepted by the department, the performance against the applicable service components implemented will then be managed through a service level agreement. When all deliverables are completed, the project will be ready for closure.

### 4) Monitoring and Control

The Monitoring and Control involves the management of project performance through formal processes by:

- a) Coordinating changes throughout the project;
- b) Controlling changes to project scope;
- c) Controlling changes to project schedules;
- d) Providing performance information which includes, status reports, progress measurement and forecasting;
- e) Establishing a risk register to track and report on changes in risk over the course of the project.

### 5) Project Closure

The Project Closure involves a final project review and documentation of the Project Closure Report. The “Lessons Learned” from the project will also be included in the project closure report. This phase further involves a formal completion or de-commissioning step involving a meeting with the department. The purpose of the meeting will be to review the final acceptance document(s) and obtain final approval that the project is complete and objectives have been met.

**NOTE:** The above implementation/take-on approach would be detailed in a Project Charter to be drafted within agreed timelines on acceptance of the proposal.

## 9. Service Governance

The service will be governed by the SITA / Department of Justice and Constitutional Development business agreement. The service will be governed by a Service Level Agreement (SLA), which is subsidiary to the business agreement.

Service monitoring, measuring and reporting will be aligned to Information Technology Infrastructure Library (ITIL) service processes and service review meetings will be held monthly.

## **10. General**

### **10.1 Document Validity and Acceptance of Proposal**

On acceptance of the proposal for Connectivity and Server Accommodation Facilities Services, a Government Order should be provided to SITA via the relevant Customer Relationship Manager, before the project implementation can commence.

The information contained in this document is valid for sixty (60) days.

### **10.2 Service Level Agreement**

A 2 year SLA will be entered into between SITA SOC Ltd. and Integrated Justice System. The SLA will be re-negotiated if the client decides to move on to the SITA cloud services.

### **10.3 Human Resources and Hours of Service**

All human resources shall be supplied by, and shall be under the jurisdiction of the applicable SITA Manager. In order to achieve the required results relevant to the request as contained herein, SITA SOC Ltd. reserves the right to outsource or in-source any or all of the tasks and functions of this project to industry and utilise those contractors as part of their own members of staff.

This service is concerned with the hours 07h45 – 16h30 for five (5) working days per week, excluding public holidays. Any additional time required after normal working hours shall be calculated as per the SITA SOC Ltd. approved tariff.

## Annex A: Financial Implication

### A1 Site List

SITE NAME	BANDWIDTH
SALU Building, 316 Thabo Sehume Street, Pretoria CBD	50MBPS
Numerus Building, 99 Hamilton Street, Pretoria	50MBPS
CLOUD (NDC2) Centurion	50MBPS
CLOUD (NDC2) – NUMERUS (Replication Link)	100MBPS

**Note:**

- a) SITA will follow the RFQ process to procure the router and access links required for the solution.
- b) Integrated Justice System to follow SITA RFQ process to add new sites to the VPN service.

### A2 Once-Off Cost

ONCE-OFF INSTALLATION COST	
Description	Total
Procurement of Hardware, Installation, Setup of Hardware, Software, and SITA support	R 682 182.57
<b>Total Excluding VAT</b>	<b>R 682 182.57</b>
PLUS: 15%VAT	R 102 327.39
<b>Total including VAT</b>	<b>R 784 509.96</b>

**Note:**

- a) The above mentioned support services include:
  - a. Project Management Services
  - b. Network Architecture Service
  - c. Network Support Services
  - d. Hosting Support Services

### A3 Monthly Recurring Cost

#### A3.1 Server Accommodation Facilities Services (Midrand)

SERVER ACCOMMODATION FACILITIES (MIDRAND)				
Description	Unit	Rate per SQM	Qty	Total
Server Accommodation Facility Services (With rack)	ZAR per sqm	R5 577.68	16.8	R 93 705.02
<b>Total Excluding VAT</b>				<b>R 93 705.02</b>
PLUS: 15%VAT				R 14 055.75
<b>Total per month Including VAT</b>				<b>R 107 760.78</b>
<b>Total per annum Including VAT</b>				<b>R 1 293 129.28</b>

#### A3.2 Data Centre Connectivity

DATA CENTRE CONNECTIVITY				
Description	Bandwidth	Data Line	Port Cost	Total
Salu Data Centre Connectivity	50Mbps	R 43 021.00	R 103 063.00	R146 084.00
Numerus Data Centre Connectivity	50Mbps	R 43 021.00	R 103 063.00	R146 084.00
Centurion Data Centre Connectivity	50Mbps	R 43 021.00	R 103 063.00	R146 084.00
Numerus & Midrand Data Centre Connectivity (Replication Link)	100Mbps	R 47 538.68	R 4 753.87	R 52 292.55
<b>Total Excluding VAT</b>				<b>R 490 544.55</b>
PLUS: 15%VAT				R 73 581.68
<b>Total per month Including VAT</b>				<b>R 564 126.23</b>
<b>Total per annum Including VAT</b>				<b>R 6 769 514.76</b>

**Note:**

- a) Pricing is based on cost estimates and will review on the completion of the formal RFQ process.
- b) Any network connectivity services that will be commissioned, decommissioned, upgraded or downgraded will be dealt with via the normal network application process; and
- c) The current WAN billing information will be updated with the new pricing.

#### A4 Summarized Service Cost

Service	Monthly
Server Accommodation Facility Services (Midrand)	R 93 705.02
Data Centre Connectivity	R 490 544.55
<b>Total Excluding VAT</b>	<b>R 584 249.57</b>
PLUS: 15%VAT	R 87 637.44
<b>Total Including VAT</b>	<b>R 671 887.01</b>
<b>Total for Year 1</b>	<b>R 8 062 644.09</b>
<b>Total for Year 2</b>	<b>R 8 586 715.96</b>
<b>Total ESTIMATED pricing for 2 year SLA Including VAT</b>	<b>R 16 649 360.05</b>

**Notes:**

- a) Annual price escalations will be based on CPI price adjustment;
- b) Pricing will be subject to price variation as a result of approved rates and tariffs; and
- c) Pricing for services will be reflected on the monthly invoices, to be settled within 30 days.

RESTRICTED



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: IJS\_letter\_02  
Enquiries: N. Duma  
Tel: +27 82 307 3295  
Date: 4 November 2020

The Acting IJS Head

INTEGRATED JUSTICE SYSTEM (IJS)

25th Floor,

DOJ&CD, SALU Building,

316 Thabo Sehume Street

Pretoria CBD

Dear Mr. Nicholas Munyai

## LETTER OF INTENT: CONNECTIVITY AND SERVER ACCOMMODATION FACILITIES FOR INTEGRATED JUSTICE SYSTEM

SITA accepted Service Level Agreements (SLA) and Purchase Order issued herein refers.

DOJ&CD issued a Letter of Award and a Purchase Order to SITA to the value of R 8 347 620.15 (VAT Inclusive) for the "Appointment of SITA as Service Provider for Network Connectivity and Hosting of IJS Transversal Datacentres (Production and Disaster Recovery)" procurement.

This purchase order covers for the Service Level Agreement (SLA), recurring monthly costs and excludes the once off payment of R 784,509.96 (VAT Inclusive). The once off payment of R 784,509.96 was erroneously missed from the overall proposal and the quote when SITA submitted the documents to the department. The once off payment is required at the initial stage of the project to procure the following:

- a) Client Edge Routers, Class B routers 4321
- b) Data lines and ports charges
- c) White Space setup.
- d) Support services are inclusive of the once off payment, which caters for (Project Management Services, Network Architecture Service and Network Support Services).

The proposal document explaining the once off cost is attached with this letter.

---

Mr O. Shelembe: **Acting Chairman**; Mr L. Keyise: **Executive Caretaker**; Mr A. Pretorius: **Acting Chief Financial Officer**  
Ms. V. Xaxa: **Company Secretary**

RESTRICTED

1

RESTRICTED

SITA is committed to the success of the project and apologise for the delay and any inconvenience caused.

Yours sincerely,



.....

Lwazi Sam

Head of Department: National and DOD Networks

04/11/2020  
.....

Date

RESTRICTED