



employment & labour

Department:
Employment and Labour
REPUBLIC OF SOUTH AFRICA

APPROVAL LETTER: DEPARTMENTAL BID ADJUDICATION COMMITTEE (DBAC)

ENQUIRIES: THEMBA MASEKO
TEL NO: 012 309 4826

24 MARCH 2025

DIRECTORATE: ICT
ATTENTION: FUMANI CHABALALA

APPROVAL GRANTED BY THE DEPARTMENTAL BID ADJUDICATION COMMITTEE FOR THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

Kindly be informed that the Departmental Bid Adjudication Committee approved the appointment of CSIR to conduct Forensic Investigation on Cyber Security breach which transpired through SITA VPNra. All work packages are costed and planned to take a period of one year at the proposed amount of R5 427 249.12 VAT inclusive, under authorization number **DBAC 40/03/2024-25**.

Please ensure that you immediately link the approved quotation on LOGIS (SCM) with the service provider; prior to capturing your request for an official order.

SECRETARIAT: DBAC

25/03/2025
DATE

CONTRACT MANAGEMENT

I hereby certify that an original copy of the contract was received by:

Initial & surname: _____

Date: _____

Signature: _____

THE DEPARTMENTAL BID ADJUDICATION COMMITTEE

HEAD OFFICE: PRETORIA

MEMORANDUM

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

AIM:

To request the Departmental Bid Adjudication Committee (DBAC) to approve the appointment of CSIR to conduct Forensic Investigation on Cyber Security breach which transpired through SITA VPNra.

MOTIVATION:

On 18 November 2024, the DEL ICT and MISS teams investigated a credential harvesting incident targeting the Active Directory (AD) domain controllers within the DEL environment. This led to a discovery of unauthorized access of the DEL ICT environment through the SITA VPNra system. The incident was escalated to involve SITA, DEL's third-party service provider, and the Microsoft Cybersecurity team. The breach resulted in unauthorized access to the AD database (ntds.dit), containing sensitive credentials and critical system information.

The attack leveraged a compromised service account that had previously held domain administrator privileges. Unauthorized access was achieved through a VPNra connection managed by SITA, revealing a potential security breach and gaps in account approval processes.

The impact of not upgrading the bandwidth is that as the utilization approaches 100% it negatively impacts on the end user performance across affected sites, in terms of slow response times and application timeouts. This creates frustration amongst users as it impacts on their productivity and service delivery.

From the technical investigation conducted by Microsoft, the following were identified:

- **Unauthorized Access:** An unauthorized VPNra admin account (padayachy.n@dbe.gov.za) was used to approve access of an unauthorized user account (Jonas.Mabetwa@dha.gov.za) on the 04th November 2024.
- This user account, Jonas.Mabetwa@dha.gov.za, approved the DEL user (Yousuf.Phalaso@labour.gov.za) on all VPNRa policies on the 14th November 2024.
- This user account, Jonas.Mabetwa@dha.gov.za, approved the DEL user (Dolly.Nkabinde@labour.gov.za) on all VPNRa policies on the 20th November 2024.

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

- **Sensitive Data Exfiltration:** The attacker used shadow copy commands to extract portions of the AD database (ntds.dit).
- **Compromised Accounts:** Three service accounts were compromised, namely (svc-exchange, svc-oititm and svc-dms). Domain admin privileges were revoked for the first two accounts, and all passwords were reset.
- **Affected Systems:** At least three domain controllers (ZADOLDCADC02, ZADOLDCADC03, ZADOLDCADC04) were accessed.

The incident exposed significant vulnerabilities in the account approval workflow of DEL's third-party service provider, SITA. These vulnerabilities facilitated unauthorized access, potential data exfiltration, and potential exposure of sensitive credentials. Further to these findings, there are weaknesses which have not been identified which require the knowledge and expertise of Forensic Investigation to get to the bottom of the incident and to be able to identify other mechanisms which are critical for the Department to deal and avert an incident of this magnitude.

The fact that SITA is a state institution, necessitated the engagement of CSIR due to the competences that it has as well as the fact that as an organ of state, it will be able to comprehend the complexity and the classification of the information that they need to navigated through as SITA deals with all government departments (the security of the state is at stake). Understanding and comprehending the technological gaps that will find within SITA environment require and institution and resources that are cleared do deal with such complexities within a short period of time given the assignment at hand. CSIR is in the position to promptly deal with the challenges at hand to assist the state in fortifying the weaknesses in place. Further to these investigations, there are other services which are offered by CSIR, which are critical for the further cyber security posture which included but not limited to the following:

Further to this investigations CSIR is required to assist the Department

- **Awareness Training for Employees**
 - Cybersecurity awareness training for Labour Centre Manager (Virtual Training)
 - Update existing cybersecurity awareness content based on the identified topics.
 - Deployment of EduCyber to Department of Labour
 - Train-the-trainer on how to use, support and maintain the EduCyber platform.
 - Conduct Instructor-Led Cybersecurity Awareness Training for a period of 12-months as and when required
- **Human Capital Development for Cybersecurity**
 - Facilitate skills development to empower identified Department of Labour IT employees.

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

- Expertise in Cybersecurity Training:
- Customized Training Solutions
- Career Development Guidance and advise
- **Contract and Project Management**
 - To provide project and technical management support and administration of the entire project as specified in work packages 1 to 4.

Request for deviation from Acting DG to appoint CSIR to conduct Forensic Investigation on Cyber Security breach is granted (see attached submission)

FINANCIAL IMPLICATIONS:

Find below a summary of pricing for all work packages defined on the proposal document. For detailed breakdown of each work package the costing is outlines hereunder and is inclusive of VAT:

Table 1: Cost Breakdown Per Work Package

	Description	Year 1 (Excl. VAT)	SUBTOTAL (Inc. VAT)
WP1	Digital Forensic Investigations	R742 125.01	R853 444.91
WP2	Security Controls Maturity Assessments	R1580 082.90	1817 095.34
WP3	Awareness Training for Employees	R1 369 405.18	R1 574 815. 96
WP4	Human Capital Development for Cyber Security	R598 694.30	R688 598.45
	Contract Project Management	R429 030.84	R493 385.47

All work packages is costed and planned to take a period of one year at the proposed amount of **R5 427 249.12 VAT inclusive.**

**REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE
THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA
VPNRA NETWORK BREACH.**

RECOMMENDATION/ DECISION:

That the Departmental Bid Adjudication Committee approve the appointment of CSIR to conduct Forensic Investigation on Cyber Security breach which transpired through SITA VPNra. All work packages is costed and planned to take a period of one year at the proposed amount of R5 427 249.12 VAT inclusive.

APPROVED/ NOT APPROVED

COMMENTS BY THE CHAIRPERSON:

We hereby declare that: -

It is certified that we did not purposefully favour or prejudice anyone in the recommendation process, as intended in Treasury Regulation 16A and the Code of Conduct for Bids.



DBAC DEPUTY-CHAIRPERSON

MS E TLOANE

20/03/2025

THE DEPARTMENT OF EMPLOYMENT AND LABOUR
PRETORIA
THE DEPARTMENTAL BID ADJUDICATION COMMITTEE

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

Date: 11 February 2025
Requested by: **Fumani Chabalala** **Extension:** 4967
Branch: Corporate Services
Chief Directorate: Office of the CIO
Directorate: Telecommunications & Information Security Management
Sub-Directorate: Telecommunications & Information Security Management

Aim:

To request the Departmental Bid Adjudication Committee (DBAC) to approve the appointment of CSIR to conduct Forensic Investigation on Cyber Security breach which transpired through SITA VPNra.

Motivation:

On 18 November 2024, the DEL ICT and MISS teams investigated a credential harvesting incident targeting the Active Directory (AD) domain controllers within the DEL environment. This led to a discovery of unauthorised access of the DEL ICT environment through the SITA VPNra system. The incident was escalated to involve SITA, DEL's third-party service provider, and the Microsoft Cybersecurity team. The breach resulted in unauthorized access to the AD database (ntds.dit), containing sensitive credentials and critical system information.

The attack leveraged a compromised service account that had previously held domain administrator privileges. Unauthorized access was achieved through a VPNra connection managed by SITA, revealing a potential security breach and gaps in account approval processes.

The impact of not upgrading the bandwidth is that as the utilisation approaches 100% it negatively impacts on the end user performance across affected sites, in terms of slow response times and application timeouts. This creates frustration amongst users as it impacts on their productivity and service delivery.

From the technical investigation conducted by Microsoft, the following were identified:

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

- **Unauthorized Access:** An unauthorised VPNra admin account (padayachy.n@dbe.gov.za) was used to approve access of an unauthorised user account (Jonas.Mabetwa@dha.gov.za) on the 04th November 2024.
- This user account, Jonas.Mabetwa@dha.gov.za, approved the DEL user (Yousuf.Phalaso@labour.gov.za) on all VPNRa policies on the 14th November 2024.
- This user account, Jonas.Mabetwa@dha.gov.za, approved the DEL user (Dolly.Nkabinde@labour.gov.za) on all VPNRa policies on the 20th November 2024.
- **Sensitive Data Exfiltration:** The attacker used shadow copy commands to extract portions of the AD database (ntds.dit).
- **Compromised Accounts:** Three service accounts were compromised, namely (svc-exchange, svc-oititm and svc-dms). Domain admin privileges were revoked for the first two accounts, and all passwords were reset.
- **Affected Systems:** At least three domain controllers (ZADOLDCADC02, ZADOLDCADC03, ZADOLDCADC04) were accessed.

The incident exposed significant vulnerabilities in the account approval workflow of DEL's third-party service provider, SITA. These vulnerabilities facilitated unauthorized access, potential data exfiltration, and potential exposure of sensitive credentials. Further to these findings, there are weaknesses which have not been identified which require the knowledge and expertise of Forensic Investigation to get to the bottom of the incident and to be able to identify other mechanisms which are critical for the Department to deal and avert an incident of this magnitude. The fact that SITA is a state institution, necessitated the engagement of CSIR due to the competences that it has as well as the fact that as an organ of state, it will be able to comprehend the complexity and the classification of the information that they need to navigated through as SITA deals with all government departments (the security of the state is at stake). Understanding and comprehending the technological gaps that will fin find within SITA environment require and institution and resources that are cleared do deal with such complexities within a short period of time given the assignment at hand. CSIR is in the position to promptly deal with the challenges at hand to assist the state in fortifying the weaknesses in place. Further to these investigations, there are other services which are offered by CSIR, which are critical for the further cyber security posture which included but not limited to the following:

Further to this investigations CSIR is required to assist the Department

- **Awareness Training for Employees**
 - Cybersecurity awareness training for Labour Centre Manager (Virtual Training)

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

- Update existing cybersecurity awareness content based on the identified topics.
- Deployment of EduCyber to Department of Labour
- Train-the-trainer on how to use, support and maintain the EduCyber platform.
- Conduct Instructor-Led Cybersecurity Awareness Training for a period of 12-months as and when required
- **Human Capital Development for Cybersecurity**
 - Facilitate skills development to empower identified Department of Labour IT employees.
 - Expertise in Cybersecurity Training:
 - Customized Training Solutions
 - Career Development Guidance and advise
- **Contract and Project Management**
 - To provide project and technical management support and administration of the entire project as specified in work packages 1 to 4.

Request for deviation from Acting DG to appoint CSIR to conduct Forensic Investigation on Cyber Security breach is granted (see attached submission)

FINANCIAL IMPLICATION AND BUDGET CONFIRMATION

Find below a summary of pricing for all work packages defined on the proposal document.. For detailed breakdown of each work package the costing is outlines hereunder and is inclusive of VAT:

Table 1: Cost Breakdown Per Work Package

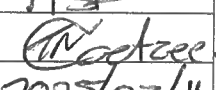
	Description	Year 1 (Excl. VAT)	SUBTOTAL (Inc. VAT)
WP1	Digital Forensic Investigations	R742 125.01	R853 444.91
WP2	Security Controls Maturity Assessments	R1580 082.90	1817 095.34
WP3	Awareness Training for Employees	R1 369 405.18	R1 574 815. 96
WP4	Human Capital Development for Cyber Security	R598 694.30	R688 598.45
	Contract Project Management	R429 030.84	R493 385.47

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

All work packages is costed and planned to take a period of one year at the proposed amount of R5 427 249.12 VAT inclusive.

Funds Available Under Allocation:

Funds: Voted Funds
Objective Office of the CIO
Project: No Project
Net Asset: Non-Asset Related
Regional Identifier: Nat Function: Whole Country D
Responsibility: (IT) Office of the CIO
Item: EXT COMP SER:SPEC COMPR SERV
Infrastructure: Non Infrastructure Stand-alone Cur

Finance Verification of Allocations & Budget	
Name & Surname:	T M Coetzee
Rank:	Asst
Signature:	
Date	2025/03/14
100%	
Amount	R5 427 249.12

Availability of Budget [Yes/ No]: Yes

Proof of Budget Availability [Yes/ No]: Yes

REQUEST FOR THE DEPARTMENTAL BID ADJUDICATION COMMITTEE TO APPROVE THE APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION ON SITA VPNRA NETWORK BREACH.

1. RECOMMENDATION

It is recommended that the Departmental Bid Adjudication Committee (DBAC) approve the procurement of the service from CSIR to conduct Forensic Investigations and three other related work packages to build Cyber Security resilience from the within the Department at the total cost outlined above which is available.

Compiled By:  SIGNATURE Director ICT RANK	24/02/2025 NAME IN PRINT Fumani Chebalala DATE
Approved By:  SIGNATURE Chief Director RANK	Makhura L.A NAME IN PRINT 13/03/2025 DATE

Rudzani Ndou (IT)

Subject: FW: CSIR ICSC Service Offering
Location: Microsoft Teams Meeting

Start: Mon 1/27/2025 2:00 PM
End: Mon 1/27/2025 3:00 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Muyowa Mutemwa

Good day;

These are the engagements I had with CSIR team after a directive was received from the Office of the DG to engage with Dr Jabu Mtsweni from CSIR after we incurred a VPNra Network breach.

Hope this assist in the process that we are pursuing.

Kind regards

Fumani Chabalala

-----Original Appointment-----

From: Fumani Chabalala **On Behalf Of** Muyowa Mutemwa

Sent: Monday, 27 January 2025 11:41

To: Fhatuwani Netsianda (ICT); Precious Malobane (IT Projects); Bertie Meyer (IT); Christine van den Heever (IT); Fhatuwani Netsianda (ICT); Fundiswa Mazibuko (IT); Makgabo Kgomo (CF - IT); Luthando Gqulu (IT); Muvhulawa Magoda (IT)

Subject: FW: CSIR ICSC Service Offering

When: Monday, 27 January 2025 14:00-15:00 (UTC+02:00) Harare, Pretoria.

Where: Microsoft Teams Meeting

Good morning Colleagues;

When your schedule allows , please join this meeting with CSIR.

Kind regards

Fumani Chabalala

-----Original Appointment-----

From: Muyowa Mutemwa <MMutemwa@csir.co.za>

Sent: Friday, 24 January 2025 16:19

To: Muyowa Mutemwa; Fumani Chabalala; Precious Maduma; Alex Ramantswana; Precious Malobane (IT Projects);

Fundiswa Mazibuko(IT)

Cc: Jabu Mtsweni

Subject: CSIR ICSC Service Offering

When: Monday, 27 January 2025 14:00-15:00 (UTC+02:00) Harare, Pretoria.

Where: Microsoft Teams Meeting

Good day all,

This session is to discuss the attached draft proposal.

Regards

Muyowa

Microsoft Teams [Need help?](#)

[Join the meeting now](#)

Meeting ID: 360 356 387 744

Passcode: y6dM7dg7

For organizers: [Meeting options](#)

From: Fumani Chabalala <Fumani.Chabalala@LABOUR.gov.za>

Sent: Friday, January 24, 2025 11:35 AM

To: Muyowa Mutemwa <MMutemwa@csir.co.za>

Cc: Precious Maduma <PNtuli1@csir.co.za>; Alex Ramantswana <ARamantswana@csir.co.za>; Jabu Mtsweni <jmtsweni@csir.co.za>; Precious Malobane (IT Projects) <Precious.Malobane@labour.gov.za>; Fundiswa Mazibuko(IT) <Fundiswa.Mazibuko@LABOUR.gov.za>

Subject: RE: CSIR ICSC Service Offering

Good morning Sir;

Can we have a meeting on Monday between 13:00 7 15:00pm. If we are unable to complete what we need to explore/discuss on the proposal, the workload available will assist us to determine if we further need to have an extended engagement before we work on the execution plan after our internal sourcing process have been finalised.

The proposed date is based on your availability and if there is any other input, am open to engagement. The engagement process is overdue and will appreciate to be afforded an opportunity for us to work on what was recommended/suggested going forward.

Thanking you in advance.

Regards

Fumani Chabalala

From: Muyowa Mutemwa <MMutemwa@csir.co.za >

Sent: Thursday, 16 January 2025 08:29

To: Fumani Chabalala <Fumani.Chabalala@LABOUR.gov.za >

Cc: Precious Maduma <PNtuli1@csir.co.za >; Alex Ramantswana <ARamantswana@csir.co.za >; Jabu Mtsweni <jmtsweni@csir.co.za >; Precious Mdlokovana (HQ) <Precious.Mdlokovana@labour.gov.za >

Subject: Re: CSIR ICSC Service Offering

Good day CIO,

Compliments of the new year.

I wanted to know if you are available to discuss the attached draft proposal.

regards
Muyowa

From: Muyowa Mutemwa <MMutemwa@csir.co.za >

Sent: Tuesday, 17 December 2024 10:05

To: Fumani Chabalala <Fumani.Chabalala@LABOUR.gov.za >

Cc: Precious Maduma <PNtuli1@csir.co.za >; Alex Ramantswana <ARamantswana@csir.co.za >; Jabu Mtsweni <jmtsweni@csir.co.za >; Precious Mdlokovana (HQ) <Precious.Mdlokovana@labour.gov.za >

Subject: Re: CSIR ICSC Service Offering

Good day CIO,

I trust you are well.

Please find attached the unsigned draft proposal.

I would like to discuss it with you. I suggest we can meet at your earlier convenience.

regards
Muyowa

From: Fumani Chabalala <Fumani.Chabalala@LABOUR.gov.za >

Sent: Wednesday, 27 November 2024 10:39

To: Muyowa Mutemwa <MMutemwa@csir.co.za >

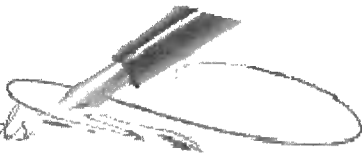
Cc: Precious Maduma <PNtuli1@csir.co.za >; Alex Ramantswana <ARamantswana@csir.co.za >; Jabu Mtsweni <jmtsweni@csir.co.za >; Precious Mdlokovana (HQ) <Precious.Mdlokovana@labour.gov.za >

Subject: RE: CSIR ICSC Service Offering

Good morning;

I have gone through the attachment and like you indicated, we need further engagement so that we can establish more of what we need over and above post incident recovery. Will engage internally to finalise and agree on a date in which we can engage further.

Thank you again for your prompt response at a short notice and pass further my appreciation to Dr Mtsweni for leadership and flexibility in times of need.

Regards 

Fumani Chabalala

Acting Chief Information Officer: DEL

Tel: 012 309 4967

Cell: 072 980 7470

Laboria House 215 Francis Beard Street PRETORIA



employment & labour

Department:
Employment and Labour
REPUBLIC OF SOUTH AFRICA

From: Muyowa Mutemwa <MMutemwa@csir.co.za>

Sent: Tuesday, 26 November 2024 14:50

To: Fumani Chabalala <Fumani.Chabalala@LABOUR.gov.za>

Cc: Precious Maduma <PNtuli1@csir.co.za>; Alex Ramantswana <ARamantswana@csir.co.za>; Jabu Mtsweni <jmtsweni@csir.co.za>

Subject: CSIR ICSC Service Offering

Good day CIO,

Thank you for meeting with us this morning.

Please find attached information related to services that the CSIR's ICSC can provide. Should you have questions, I can present you our capabilities.

The next steps, we will await:

1. a session to review in detail the firewall activities.
1. a session to speak to your Security Operations Centre team about additional incidents observed in your environment.

regards

Muyowa



Muyowa Mutemwa

Senior Cybersecurity Specialist

Research Group Leader: Data Security & Analytics

CompTIA CASP+ | EC Council CEH | (ICS)2 CISSP

Information and Cyber Security Centre

Defense and Security



Email: mmutemwa@csir.co.za

Mobile: 072 781 1964

[LINKSHIELD PROTECTED] [LINKSHIELD PROTECTED] [LINKSHIELD PROTECTED] https://smex-ctp.trendmicro.com:443/wis/clicktime41c2-8b74-086c08e13979&auth=e5e15f8bef622a11105797be1b06103c1898dd0-91180c008fa374a60d1063d60c2c1b1243336090_origi%3Ftext%3DW0xJTktTSElFTEQgUFJPVEVDVEVEXSB3d3cuY3Npci5jbY56YTxcGFuIHNOeWxlPSJmb250LXNpemU6MS4wcHQiPiBvcmlnaW5hbC1l



employment & labour

Department:
Employment and Labour
REPUBLIC OF SOUTH AFRICA

SUBMISSION

DMS: 00810/2025/1

Acting Director-General: Employment and Labour

PRETORIA

SUBJECT: REQUEST THE ACTING DIRECTOR GENERAL TO APPROVE DEVIATION FROM PROCUREMENT PROCESS BY APPOINTING CSIR TO CONDUCT NETWORK BREACH FROM SITA VPNRA DEL ACCOUNT

1. PURPOSE OF THE SUBMISSION:

- 1.1 Appoint CSIR to conduct Cyber Security Forensic Investigation on SITA VPNra Network Breach

2. BACKGROUND:

- 2.1 VPNra access and credential harvesting Incident in DEL ICT Environment
- 2.2 A SITA VPNra incident occurred on the 18th of November 2024 where the Active Directory domain controller of the Department was targeted. This led to a discovery of unauthorised access of the DEL ICT environment through the SITA VPNra system. The incident was escalated to involve SITA, DEL's third-party service provider, and the Microsoft Cybersecurity team. The breach resulted in unauthorized access to the AD database (ntds.dit), containing sensitive credentials and critical system information.
- 2.3 The attack leveraged a compromised service account that had previously held domain administrator privileges. Unauthorized access was achieved through a VPNra connection managed by SITA, revealing a potential security breach and gaps in account approval processes.
- 2.4 Departmental ICT resources and Microsoft DART team were brought on board to investigate the incident and arrived at the following key findings:
- 2.5 1. **Unauthorized Access:** An unauthorised VPNra admin account (padayachy.n@dbe.gov.za) was used to approve access of an unauthorised user account (Jonas.Mabetwa@dha.gov.za) on the 04th of November 2024.
- 2.6 2. **This user account, Jonas.Mabetwa@dha.gov.za,** approved the DEL user (Yousuf.Phalaso@labour.gov.za) on all VPNRa policies on the 14th of November 2024.

Kommunikasie-en-inligtingsteiël • Dithaeletsano tsa Puso • Tekuchumana taHulumende • EzokuXhumana koMbuso • Dikgokahano tsa Mmuso
Vhudevhidzani ha Muvhuso • Dikgokagano tsa Mmuso • IiNkonzo zoNxibelelwano lukaRhulumente • Vuhlanganisi bya Mfumo • UkuThintanisa koMbuso

Batho Pele - putting people first

- 2.7 3. **This user account**, Jonas.Mabetwa@dha.gov.za, approved the DEL user (Dolly.Nkabinde@labour.gov.za) on all VPNRa policies on the 20th of November 2024.
- 2.8 4. **Sensitive Data Exfiltration**: The attacker used shadow copy commands to extract portions of the AD database (ntds.dit).
- 2.9 5. **Compromised Accounts**: Three service accounts were compromised, namely (svc-exchange, svc-oititm and svc-dms). Domain admin privileges were revoked for the first two accounts, and all passwords were reset.
- 2.10 6. **Affected Systems**: At least three domain controllers (ZADOLDCADC02, ZADOLDCADC03, ZADOLDCADC04) were accessed.
- 2.11 There was immediate action that were taken by the Department immediately after the occurrence of the incident which include the following steps.
- 2.12 1. Compromised accounts were secured, and their VPNra access was revoked.
- 2.13 2. The suspicious endpoint (MUMDUT2024) was blacklisted on the MISS SOC and Insider Threat Management (ITM) system.
- 2.14 3. Logs from the MISS SOC were analyzed to trace unauthorized actions.
- 2.15 4. Microsoft Entra ID was reviewed by Microsoft cybersecurity team to identify any cloud-based impacts, and none were found.
- 2.16 5. Passwords for all affected accounts were reset, and domain admin privileges were revoked where necessary.
- 2.17 6. All AD accounts were set to "Reset password on next logon".
- 2.18 7. Commands recommended by Microsoft, including klist purge and repadmin /syncall, were executed on accessible domain controllers to restore integrity

3. DISCUSSIONS:

- 3.1 Section 217 of the constitution of the Republic of South Africa requires that when an organ of state in the national, provincial or local spheres contracts for goods and services, it must do so in accordance with a system which fair, equitable, transparent, competitive and cost effective. However, 16A6.4 requires that If in a specific case it is impractical to invite competitive bids, the accounting officer or accounting authority may procure the required goods or services by other means, provided that the reasons for deviating from inviting competitive bids must be recorded

4.1 State Security Agency, South African Police Service, State Information Security Agency and other related authorities of government directly or indirectly impacted by Network breach will be informed about the steps undertaken to deal with Cyber Security weaknesses identified. See attached letters of notification about the Network VPNra breach communicated to SITA, SSA and the report for the attention of ADG.

5.1 CSIR was engaged to provide a proposal for the requested services. The total cost of the four services including Contract and Project Management amounts to R5, 427, 240.12 VAT inclusive

REQUEST THE ACTING DIRECTOR GENERAL TO APPROVE DEVIATION FROM
PROCUREMENT PROCESS BY APPOINTING CSIR TO CONDUCT NETWORK BREACH FROM

ITEM:

CNS:BUS&ADV FUND: VOTED FUNDS

SER:RESEARCH&ADVISOR

OBJ: OFFICE OF THE CIO

RESP: (IT) OFFICE OF THE CIO

INFR: NON INFRA/ST ALONE:CURRENT

ASS: NON-ASSETS RELATED

PROJ: NO PROJECTS

REG: NAT FUNCTION:WHOLE COUNTRY
DOM

AMOUNT: R5,427,240.12



CHIEF FINANCIAL OFFICER: BE MADUNA

DATE: 06/02/2025

6. LEGAL IMPLICATIONS:

No legal implication identified

7. RECOMMENDATIONS:

It's recommended that the Director-General: Approve to deviate from normal procurement process by appointing CSIR to conduct services recommended below

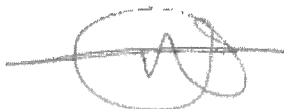
- 7.1 It is recommended that the Acting Director General approve the request to deviate from normal procurement process and appoint CSIR to conduct the following key activities in order to improve the Departmental Cyber Security posture and also to implement the findings that will arise from the investigation: 1: digital forensics investigations, 2: cybersecurity controls maturity assessment, 3: awareness training for employees (optional), 4: human capital development (optional).

8. ATTACHMENTS:

1. Department of Labour Incident Response Services Technical and Pricing Proposal unsigned (009).pdf
2. VPNra access and credential harvesting Incident November 2024.pdf
3. Public Service ICT Security Incident Management Guidelines (004).pdf
4. SITA Letter - VPnRA Incident 02 12 2024.pdf
5. SSA Letter - VPnRA Incident 02 12 2024.pdf

The recommendation in Par 7.1

Recommended



DEPUTY DIRECTOR GENERAL: CORPORATE SERVICES: MRS BB MATEBESI

DATE: 05/02/2025

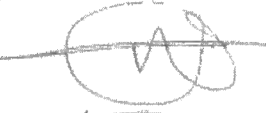
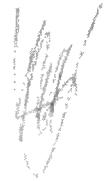
9. DIRECTOR-GENERAL: EMPLOYMENT AND LABOUR

The recommendation in Par 7.1

Approved



ACTING DIRECTOR-GENERAL: EMPLOYMENT AND LABOUR: MR LLV MLENZANA
DATE: 16/02/2025

DATE	SIGNATURE	NAME OF SIGNATORY	DATE	SIGNATURE
		LA MAHOLELA	30/01/2025	
		KG MAHOLWANA	03/02/2025	
		NG MDITSHWA	05/02/2025	
		BB MATEBESI	05/02/2025	
		BE MADUNA	06/02/2025	
		LLV MLENZANA	16/02/2025	

Department of Labour
Financial Year 2025/26
OFFICE OF THE CIO BUDGET

DESCRIPTION	ORIGINAL BUDGET 2025/26	SHIFTS	VARIANCE
Salaries and Wages	25,226		25,226
S&W:Basic Salary (Res)	20,000		20,000
S&W:Performance Bonus (Res)	1,426		1,426
S&W:Perfm Award other (Res)			-
S&W:Serv Based other (Res)	50		50
S&W:Leave Discounting (Res)	100		100
S&W:Overtime (Res)	150		150
S&W:Compens/Circum other (Res)	100		100
S&W:Capital Remuneration (Res)			-
S&W:Home Owners Allowance (Res)	400		400
S&W:Non Pensionable All Oth (Res)	2,000		2,000
S&W:Service Bonus	1,000		1,000
Social contributions	2,418		2,418
Empl Contr: Bargain Council (Res)	5		5
Empl Contr: Insurance (Res)			-
Empl Contr: Medical (Res)	713		713
Empl Contr: Off Union & Ass (Res)			-
Empl Contr: Pension (Res)	1,700		1,700
COMPENSATION OF EMPLOYEES	27,644		27,644
ADMINISTRATIVE FEES	58	-48	10
Registration Fees			-
Bank Charg&Card Fees Comm Bank			-
Management / Handling Fees			-
Travel Agency Fees	58	-48	10
ADVERTISING			
Advert: Marketing			-
Advert:Tenders			-
Advert:Promotional Items			-
Advert:Recruitment			-
ASSETS<R5000	699		699
Eqp<R5000: Audio Visual Equipment			-
Eqp<R5000: Bags			-
Eqp<R5000:Domestic Equipment	50		50
Eqp<R5000:Kitchen appliances	30		30
C/EQP<R5000:COM SYS - Desktop	200		200
C/EQP<R5000:COM Peripherals	200		200
F&O/Eqp<R5000:Office Equip	100		100
F&O/Eqp<R5000:Office Furn	100		100
F&O/Eqp<R5000:Paint/Sculp&Or			-
EQP<R5000:LEA/TRA/SUP/LIB/MA			-
PHO EQP<R5000:Photographc EQ			-
Eqp<R5000:Telec Equipment	19		19
Eqp<R5000:Tents,Flags&Access			-
Eqp<R5000:Workshop EQ&Tools			-
Audit Fees:Ext Current Year			
Bursaries (Employees)			
Catering: Departml Activities	76		76
COMMUNICATION	14,993		14,993
Com:Cell Contract (Subs&Calls)	5,000		5,000
Com:Post/Stamp/Frank Mach			-
Com:Radio&TV Transmission			-
Com:Rent Priv Bag&Post Box			-
Com: Satellite Signals			-
Com:Tel/Fax/Telegrap&Telex	9,993		9,993
Com:Telephone Installation			-
COMPUTER SERVICES	104,587		104,587
SITA ELECTRON DOC DEL SYS (EDD)	20		
SITA DATA LINES	14,000		14,000
SITA HELP DESK	250		250
SITA INTERNET SERV CHRGS	1,000		1,000
PERSAL MAINFRAME TIME	300		300
BAS MAINFRAME TIME	2,700		2,700

Department of Labour
Financial Year 2025/26
OFFICE OF THE CIO BUDGET

DESCRIPTION	ORIGINAL BUDGET 2025/26	SHIFTS	VARIANCE
LOGIS MAINFRAME TIME	400		400
SITA PRINTING WORKS	25		25
SITA SOFT LIC:OPER SYS SOFT	50		50
SITA SOFT LIC:OFF SUITE SOFT	-		-
SITA SOFT LIC:UTILITY SOFT	-		-
SITA SOFT LIC:DEVELOPM SOFT	-		-
SITA SOFT LIC:SECURITY SOFT	-		-
SITA SPECIALISE COMPT SER	11,000		11,000
EXT COMP SER:DATA LINES	100		100
EXT COMP SER:INFOR SERVICES	-		-
EXT COMP SER:SFT LCN:OP SY S	15,000		15,000
EXT COMP SER:SFT LCN:OF ST S	17,000		17,000
EXT COMP SER:SFT LCN:DEV SOF	-		-
EXT COMP SER:SPEC COMPR SERV	23,000		23,000
EXT C/S:SYS :MAINT. SYSTEM	14,000		14,000
EXT C/S:SYS :OPERAT SUPPRT	5,742		5,742
CONS/PROF:BUSINESS&ADVISORY SERV	784	-584	200
C/P:Bus&Adv Ser:Accont&Auditr	-		-
C/P:Bus&Adv Ser:Board Member	684	-584	100
C/P:Bus&Adv Ser:Communicatn	-		-
C/P:Bus&Adv Ser:Human Resou	-		-
C/P:Bus&Adv Ser:Occu Safe& Hea	-		-
C/P:Bus&Adv Ser:Rese&Advisor	100		100
C/P:Bus&Adv Ser:Valuer	-		-
C/P:Bus&Adv Ser:Qualif Verif	-		-
C/P:Bus&Adv Ser:Trns&Trnsc	-		-
Cons/Prof:Infrastructure&Planning	-		-
Cons/Prof:Laboratory Services	-		-
Cons/Prof:Legal Cost	-		-
C/P:L/PVT Firm:LegalAdvice	-		-
C/P:L/PVT Firm:Mesr of Cour	-		-
C/P:L/State Attny:Legal Adv	-		-
CONTRACTORS	226	-123	103
Contrctrs:Artists& Performers	-		-
Contrctrs:Audio- Visual Serv	-		-
Contrctrs:Casual Labourers	-		-
Contrctrs:Interior Decorator	-		-
Contrctrs:Plant Flow&oth Dec	3		3
Contrctrs:Stage & Crew	-		-
Contrctrs:Tracing Agnts&Debt Coll	-		-
Contrctrs:Trnsprt/Relctn Contr	-		-
Outs:Contrctrs:Mnt & Rep N-Inf Ass	223	-123	100
AGENCY&SUPRT/OUTSOURCED SERVICES	-		-
A&S/O/S:Professional Staff	-		-
A&S/O/S:Security Services	-		-
Entertainment Management	-		8
Fleet Services (including government motor transport)	10	-10	-
F/Ser:Tracking (PHYS CS)	10	-10	-
F/Ser:Kilometers	-		-
F/Ser:Batteries	-		-
F/Ser:Licence Plates	-		-
F/Ser:Fuel,Oil& Grease	-		-
F/Ser:Spares&Accessorie	-		-
F/Ser:Towing	-		-
F/Ser:Transaction Costs	-		-
F/Ser:Tyres& Tubes	-		-
F/Ser:Vehicle Repairs	-		-
F/Ser:Toll Fees	-		-
F/Ser:Car Valet & Washing Serv	-		-
Inventory:Fuel, Oil & Gas	-		-
Inv F&G: Fuel, Oil & Lubricants	-		-
Inventory:Materials & Supplies	-		-
Inv Mat&Sup:Electrical Supplies	-		-
Inv Mat&Sup:Notice Boards&Signs	-		-

Department of Labour
Financial Year 2025/26
OFFICE OF THE CIO BUDGET

DESCRIPTION	ORIGINAL BUDGET 2025/26	SHIFTS	VARIANCE
Inventory:Other Consumables			
Inv Mat&Sup:Household Supplies			
CONS SUPPLIES	140		140
Cons Supp:Gifts and Awards			-
Cons Supp:Uniform & Clothing	25		25
Cons Hous Sup:Broom & Brsh			-
Cons Hous Sup: Crockery&Cutlery	5		5
Cons Hous Sup:Disp Paper/Plastic			-
Cons Hous Sup:Packing Material	5		5
Cons Hous Sup:Toiletries			-
Cons Hous Sup:Tblght&Lght Bulb			-
Cons Hous Sup :Wash/Cean Dete			-
Cons Hous Sup :Water			-
Cons Hous Sup :Workplace Decor			-
Cons Hous Sup:Fuel Supplies			-
Cons: Materials & Supplies	5		5
Conss: First Aid Kit			-
Conss: Security Access Conss			-
Cons: IT Conssmbles	100		100
Cons: Bags and Accessories			-
Cons: Photographic Conss			-
CONS STA PRINT&OFF SUP	148	-100	48
Cons: SP&OS: Audio Visual			-
Cons: SP&OS: Gov Prin	102	-100	2
Cons: SP&OS: Mag/News/Jnrls			-
Cons: SP&OS: Stationery	15		15
Cons:SP&OS:Art & Draw			-
Cons: SP&OS: Media Collections			-
Cons: SP&OS: Print Cartridge	10		10
Cons: SP&OS: Printing Paper	21		21
LEASE PAYMENTS	3,256		3,256
Operating Leases:Infstrctr			-
Operating Leases:Non-Infstrctr	3,256		3,256
RENTAL & HIRING			-
PROPERTY PAYMENTS	56	-56	-
P/P:Gardening Services	56	-56	-
P/P:Cleaning Services			-
P/P:Fire Protection			-
P/P:Laundry Services			-
P/P:Management fee			-
P/P:Pest Cntrl/Fumigation Ser			-
P/P:Safeguard& Security			-
OUTS P/P:Contractd Maint			-
P/P:Water			-
P/P:Electricity			-
P/P:Sewerage			-
P/P:Waste/Refuse Removal			-
Transport Provided Dept Activity	-	-	-
Tranport for Public Events			-
TRAVEL AND SUBSISTENCE	901	-	901
T&S Dom:Accomodation	400		400
T&S Dom: Special Daily Allow	100		100
T&S Dom:Food & Bever	50		50
T&S Dom:Incidental Cost	50		50
T&S Dom :Car Rent	40		40
T&S Dom :Km Alll (Own Transport)	106		106
T&S Dom:Km Allowance sms	-		-
T&S Dom :Air Transport	60		60
T&S Dom:Railway Transport	20		20
T&S Dom :Road Transport	40		40
T&S Forgn:Accomodation			-
T&SForgn: Special Daily Allow			-

Department of Labour
Financial Year 2025/26
OFFICE OF THE CIO BUDGET

DESCRIPTION	ORIGINAL BUDGET 2025/26	SHIFTS	VARIANCE
T&S Forgn:Food & Bever			-
T&S Forgn:Incidental Cost			-
T&S Forgn :Car Rent			-
T&S Forgn :Air Transport			-
T&S Forgn :Road Transport			-
T&S Dom Non Empl: Accommodation	10		10
T&S Dom Non Empl: Food & Bever	10		10
T&S Dom Non Empl: Incidental Cost	5		5
T&S Dom Non Empl: Transport	10		10
Train&Staff Dev Employees	973		973
OPERATING PAYMENTS	166	921	1,087
O/P:Cach Discount:Temp			-
O/P:Laundry Services			-
O/P:Courier&Delivery Servs	100		100
O/P:Competency Cert/Licenses			-
O/P:SUBSCRIPT,PRINT&PUBLIC SERV	66	921	987
O/P: N-life Ins PRM-TRY12.1.2			-
O/P: Printing & Publicat Serv			-
O/P: Prof Bod,Memb&Subcr Fees			-
O/P:Resettlement Cost			-
O/P:Roadworthy Tests			-
O/P:Storage of Assets			-
O/P:Storage of Files			-
Venues and Facilities	38		38
Interest & Rent on Land			-
TOTAL GOODS & SERVICES	127,119		127,119
Thefts & Losses			-
PAYMENTS FOR FINANCIAL ASSET CUR			-
Provincial and Local Governments			-
MUN B/ ACC: Vehicle Licences Mun			-
HOUSEHOLDS (HH)			-
H/H Empl S/Ben: Leave Gratuity			-
H/H: Claims Against State (CASH)			-
TRANSFERS & SUBSIDIES			-
Buildings & Other Fix Structures			-
Outs Contrctr:New Buil & Ot Fix St			-
Transport Equipment			-
Buses			-
Mobile Offices			-
Motor Vehicles			-
Finance Leases Trnsp EQP			-
Machinery & Equipment	18,519	0	18,519
Audio Visual Equipment	1,000		1,000
Domestic Equipment	50		50
Kitchen Appliances	50		50
Photographic Equipment			-
Secure Equipm,Sys,Materi:Fix			-
Telecom Equipm-Equipment	100		100
Domestic Furniture	100		100
Office Equipment	100		100
Office Furniture	200		200
Comp Hard & Sys -Desktop	1,000		1,000
Comp Hard & Sys -Laptop	5,000		5,000
Comp Hard & Sys -Server/Main	10,000		10,000
Desktop Printing Equipment	919		919
Finance Leases oth mach			-
PAYMENTS FOR CAPITAL ASSETS	18,519		18,519
EXPENDITURE: VOTED	173,282		173,282



CSIR

Touching lives through innovation

Document No : CSIR/DS/ICSC/DSA/DOL/PROP/2024/0001/B

DEPARTMENT OF LABOUR INCIDENT RESPONSE SERVICES

TECHNICAL & PRICING

PROPOSAL

CSIR

December 2024

© CSIR 2024. All rights to the intellectual property and/or contents of this document remain vested in the CSIR. This document is issued for the sole purpose for which it is supplied. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by means electronic, mechanical, photocopying, recording or otherwise without the express written permission of the CSIR. It may also not be lent, resold, hired out or otherwise disposed of by way of trade in any form of binding or cover than that in which it is published.

Laboria House,
215 Francis Baard Street,
Pretoria,
0001

Attention: Acting CIO, Mr Fumani Chabalala

13 December 2024

Reference: CSIR/DS/ICSC/DSA/DOL/PROP/2024/0001/B

**DEPARTMENT OF LABOUR INCIDENT RESPONSE SERVICES
(TECHNICAL & PRICING PROPOSAL)**

Dear Sir/Madam,

Please find attached the CSIR proposal to the Department of Labour to provide Incident Response through digital forensic investigations, cybersecurity controls maturity assessment, awareness training for employees, and human capital development for a period of twelve (12) months.

To support the Department with cybersecurity investigations and incident response, the CSIR herein proposes four work packages.

- Work package 1: digital forensics investigations,
- Work package 2: cybersecurity controls maturity assessment,
- Work package 3: awareness training for employees (optional),
- and work package 4: human capital development (optional).

This proposal is valid for 90 (ninety) days from the date of submission to the department.

For any queries, kindly do contact me on the details provided below.

Dr Jabu Mtsweni,
Head: Information and Cyber Security Centre
Email: jmtsweni@csir.co.za
Contact Number: +2772 407 4757

PREPARED FOR

DEPARTMENT OF LABOUR

Document No: CSIR/DS/ICSC/DSA/DOL/PROP/2024/0001/B

**DEPARTMENT OF LABOUR INCIDENT RESPONSE SERVICES
(TECHNICAL & PRICING PROPOSAL)**

Approved By

Mr. Sipho Mbhokota
Executive Cluster Manager: Defence & Security

Date

[illegible]

CONTENTS

Tables	5
Figures	6
Abbreviations	7
1 Executive Summary	8
1.1 About Us	8
1.2 Designed Signatory	8
1.3 Company Experience	8
2 Scope of Work	9
2.1 Work Package 1: Digital Forensics Investigations	10
2.2 Work Package 2: Cybersecurity Controls Maturity Assessments	11
2.3 Work Package 3: Awareness Training for Employees	12
2.4 Work Package 4: Human Capital Development for Cybersecurity	13
2.5 Contract and Project Management	14
3 Pricing Schedule	15
4 General Contracting Information	17
4.1 Management	17
4.2 Contract Conditions	17
4.3 International Financial Reporting Standard 15 Applicability	17
4.4 Sub-Contracting	17
4.5 Subsistence and Travel	18
4.6 Intellectual Property	18
4.7 Protection of Personal Information	18
4.8 Cost Recovery	18
4.9 Security Clearances	18
4.10 Validity	18
4.11 Notes	18
5 Profile of the Project Team (Professional Qualification and Experience)	19
6 SIMILAR ASSIGNMENTS AND REFERENCES	23
7 Additional Previous Project Experience	24
7.1 Military Environment	24
7.2 Public Sector	24
7.3 Private Sector	24
8 CSIR Institution Profile	26
9 CSIR General Contract Conditions	27

TABLES

Table 1:	Cost Breakdown Per Work Package	15
Table 2:	Estimated Cost Summary	15
Table 3:	Payment Milestones	16

FIGURES

Figure 1:	Scope of Work	9
Figure 2:	Digital Forensics Approach	10
Figure 3:	Cyber Security HCD Roadmap	13

ABBREVIATIONS

CIO	Chief Information Officer
CSIR	Council for Scientific and Industrial Research
D&S	Defence and Security
GDPR	General Data Protection Regulation
ICSC	Information and Cyber Security Centre
ICT	Information and Communication Technologies
POPIA	Protection of Personal Information Act
R&D	Research and Development
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
SQL	Structured Query Language
VPN	Virtual Private Network

1 Executive Summary

This executive summary to the Department of Labour covers firstly the background of the CSIR, secondly the CSIR's experience, thirdly how the CSIR understands what Department of Labour is looking for from Department of Labour Incident Response Services call, and lastly the summary of the CSIR's proposed solution.

1.1 About Us

The CSIR is a statutory body established in 1945 with continued existence under the Scientific Research Council Act (Act No. 46 of 1988), as amended, operating through the Information and Cyber Security Centre in the Defence and Security Cluster ("CSIR"), 1 Meiring Naude Rd Pretoria 0184.

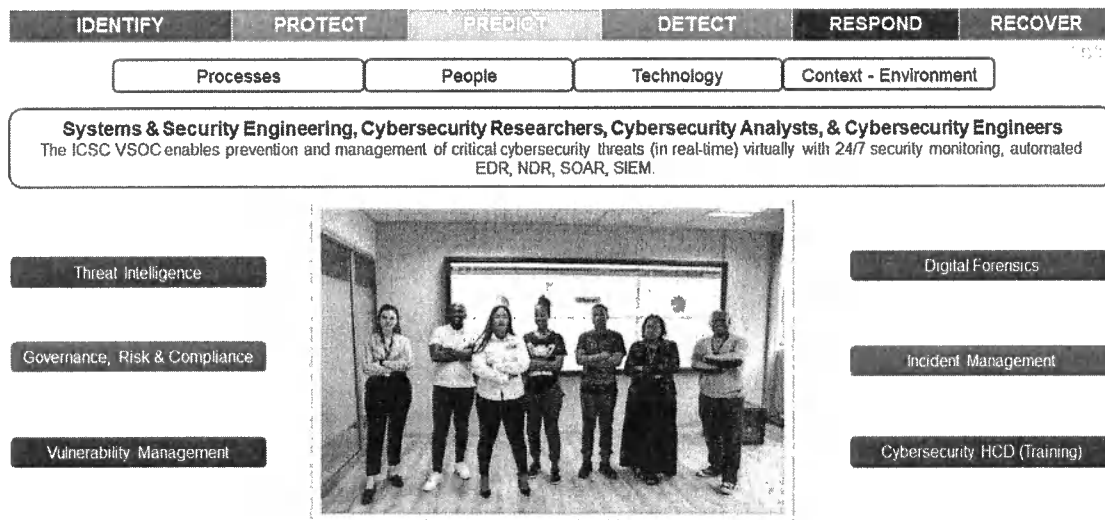
1.2 Designed Signatory

Dr Jabu Mtsweni in his capacity as the Impact Area Manager of the Information & Cyber Security Centre is authorised to act on behalf of the company in negotiating and signing all documents which shall be deemed to include the "Department of Labour Incident Response Services" proposal.

1.3 Company Experience

CSIR is a trusted state-owned entity (SOE) and has an impressive list of satisfied clients in the African marketplace, including, City of Johannesburg (South Africa), Eswatini Electricity Company (Eswatini), RAND Water Utility (South Africa), Senegal National Electricity Agency (Senelec SA)(Dakar, Senegal), The Presidency (South Africa), Gauteng Department of e-Government (South Africa) amongst others.

CSIR Virtual Security Operations Centre (VSOC)



2 Scope of Work

The services required by the Department of Labour includes the digital forensic investigations, cybersecurity controls maturity assessments, awareness training for employees, and human capital development related to cybersecurity. Contract & Project Management is a key process to ensure that all activities proposed are well planned, organized, and executed to deliver the security services required by the department of labour. Figure 1 presents the work packages required to provide the department of labour with incident response services.

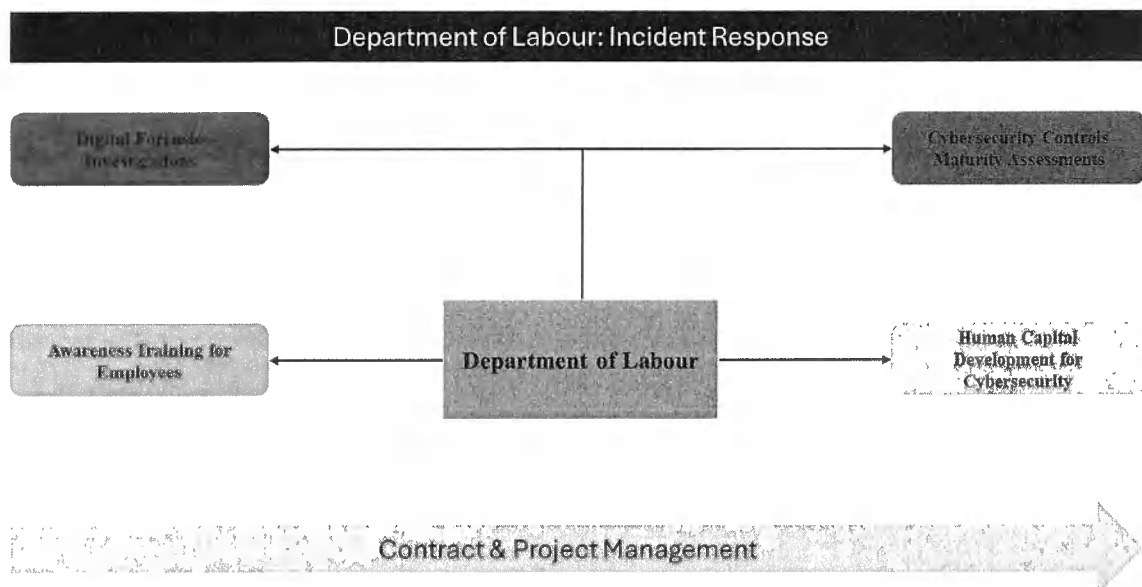


Figure 1: Scope of Work

The CSIR shall deliver on the following requirements:

- digital forensic investigations,
- cybersecurity controls maturity assessments,
- awareness training for employees (this is optional for the department),
- and human capital development related to cybersecurity (this is optional for the department)

2.1 Work Package 1: Digital Forensics Investigations

The Digital Forensics services work package is tailored to furnish the Department of Labour with proficient analysis (and investigation) of cybersecurity incidents across VPN logs, computer systems, emails, citrix and storefront logs, Microsoft Active Directory (AD) logs, Trend Micro anti-virus logs, SQL servers, and so on. This work package will seek to ascertain the cause, scope and impact of the reported unauthorized access to the Department's IT environment.

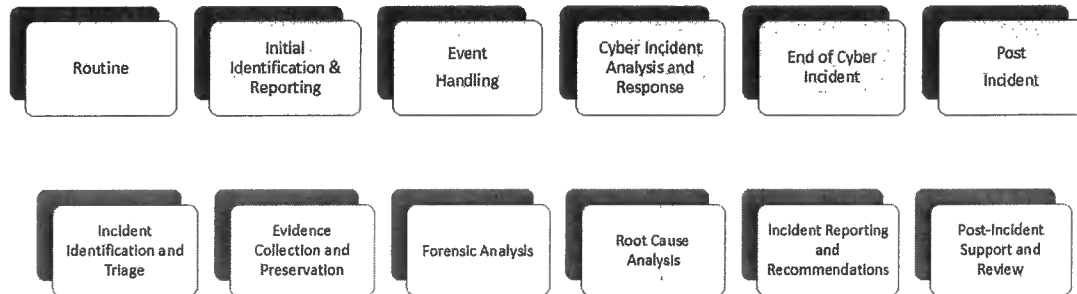


Figure 2: Digital Forensics Approach

The CSIR's approach to Digital Forensics is a tailored version of the National Institute of Standards and Technology (NIST) framework that will be adapted for the Department of Labour's IT environment. This approach is illustrated in Figure 2. This starts by identifying and triaging cybersecurity incidents. After identifying the incident, the team analyses the incident to understand the incident's impact and severity. In this case, response prioritization is based on the incident's impact and severity.

The next step involves evidence collection and preservation to secure digital evidence from affected systems. The analysis phase is for conducting a forensic analysis of evidence in search of details to identify attack vectors, systems compromised, and malicious payloads. The root cause of the incident must be identified whether it is a security gap or a vulnerability that may have been exploited by the attacker.

The reporting stage prepares and provides a detailed incident report that documents the sequence of events, extent of the breach including findings. Recommended remediation actions include post-incident activity and support to return operations to normal, which includes system recovery and restoration of data.

Deliverable(s):

- Comprehensive Incident Forensics & Remediation Report covering the following:
 - Incident Triage
 - Evidence
 - Forensic Analysis
 - Root Cause Analysis
 - Incident Response & Remediation Recommendations
- Post-Incident Review & Lessons Learned

2.2 Work Package 2: Cybersecurity Controls Maturity Assessments

This work package aims to conduct an assessment of the Department of Labour's security controls maturity across its diverse IT infrastructure, for both cloud and on-premises data centres environments for a period of 12 months. The assessment will evaluate the effectiveness of existing security controls against industry best practices and regulatory requirements, identifying gaps and weaknesses, and provide actionable recommendations for improvement.

This work package deliverables are:

- **Assessment Plan:**
 - Provide detailed project plan outlining the scope, methodology, timeline and resource allocation.
 - Conduct a risk assessment plan for identifying potential risks and mitigation strategies.
 - Communication plan outlining stakeholder engagement and reporting mechanisms.
- **Security Controls Inventory:**
 - Conduct a comprehensive inventory of existing security controls across all IT environments.
 - Mapping of controls to relevant industry standards and frameworks (e.g., NIST cybersecurity Framework, Critical Security Controls).
- **Gap Analysis:**
 - Identify gaps between current security posture and industry best practices.
 - Prioritize critical gaps based on risk assessment.
 - Detailed analysis of control effectiveness and efficiency.
- **Maturity Assessment Report:**
 - Detailed assessment reports for each assessed domain including access control, incident response and data protection.
 - Provide overall maturity assessment report summarising the Department of Labour cybersecurity maturity level.
- **Recommendations Report:**
 - Provide actionable recommendations to address identified gaps and improve overall cybersecurity posture.
 - Prioritized recommendations based on risk and impact.
 - Cost-benefit analysis for proposed recommendations.
- **Remediation Plan:**
 - Provide a detailed remediation plan outlining the steps required to implement recommended improvements.
 - Provide a timeline for remediation activities and budget requirements.
- **Final Report:**
 - Provide executive summary highlighting key findings and recommendations.
 - Provide detailed assessment results and analysis.
 - Provide recommendations for ongoing monitoring and improvements.

2.3 Work Package 3: Awareness Training for Employees

This work-package aims to conduct cybersecurity awareness training to Department of Labour Centre Managers, deployment of Cybersecurity awareness training platform (Edu-Cyber). The training will occur on Microsoft Teams and where possible the training will be done in-person across the country. The following activities will be conducted:

Cybersecurity awareness training for Labour Centre Manager (Virtual Training)

- Update existing cybersecurity awareness content based on the identified topics.
- Conduct pre-assessment for the Labour Centre Managers.
- Conduct cybersecurity awareness training for Labour Centre Managers via Microsoft Teams. Where possible these training could be held in-person across the country.
- Conduct post-assessment.
- Analyse results of pre and post assessments to determine impact of the training.
- Develop report highlighting the impact of the training with recommendations.

Deployment of EduCyber to Department of Labour

- Determine EduCyber installation and hosting requirements at Department of Labour
- Determine key cybersecurity awareness themes and topics for various end-user groups.
- Develop/update existing cybersecurity awareness content based on the identified themes and topics.
- Develop question banks in-line with the awareness content including pre and post assessment questions.
- Convert the developed awareness content into SCOM packages and upload into EduCyber.
- Set-up configuration and deployment of EduCyber to Department of Labour operational environment.
- Train-the-trainer on how to use, support and maintain the EduCyber platform.

Conduct Instructor-Led Cybersecurity Awareness Training for a period of 12-months as and when required

In this activity, CSIR will conduct Cybersecurity awareness training to Department of Labour staff as and when required for a period 12 months. Each training can take several formats depending on the current needs of Department of Labour, but not limited to the following:

- One-hour brown bag session where Department of Labour employees gets to ask cyber-awareness questions to CSIR experts.
- Conducting instructor-led cybersecurity awareness training to a selected group of end-users (e.g., Senior Management, Legal, HR, Finance, etc). 4-hours training per group.
- Providing support during October cybersecurity awareness month.
- A pre and post assessment will be conducted for each of the sessions, and a report will be developed to measure the impact of the training.

2.4 Work Package 4: Human Capital Development for Cybersecurity

The main objective of this work package is to facilitate skills development to empower identified Department of Labour IT employees. This task includes the development of the identified personnel, to empower them to take over some of the responsibilities related to cybersecurity security operations monitoring and response.

As part of the Department of Labour's continuous improvement in cyber security, a key focus will be on enhancing the skills and expertise of its ICT team. To support this objective, the CSIR proposes a 12-month Human Capital Development Plan as depicted in Figure 3 for IT Training and Certification. This plan will be designed to the Department of Labour's ICT professionals with advanced knowledge and skills in cybersecurity, ensuring the team is well-prepared to address emerging threats and challenges.

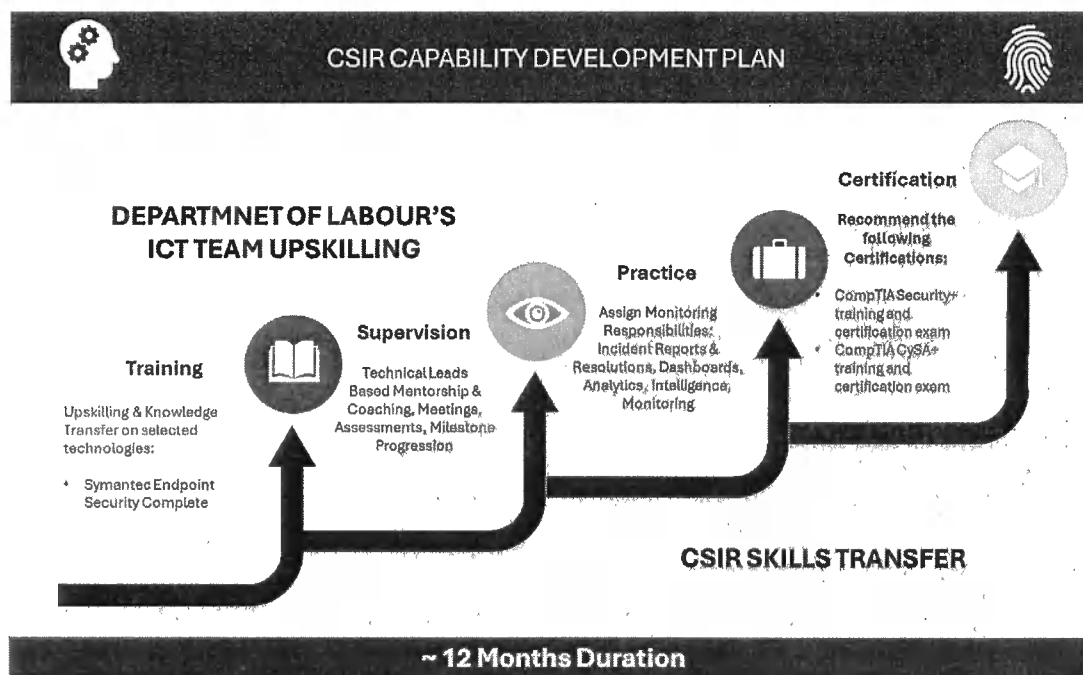


Figure 3: Cyber Security HCD Roadmap

As a partner, the CSIR shall offer the following:

- **Expertise in Cybersecurity Training:** CSIR has a proven track record in delivering comprehensive cybersecurity mentorship & coaching programmes. The CSIR staff are certified professionals with extensive industry experience, ensuring that the training content is both relevant and practical.
- **Customized Training Solutions:** Understanding that the Department of Labour may have unique needs, the CSIR shall tailor its capability development programme to align with Department's specific environment. This will ensure that the ICT team receives training that is directly applicable to their roles and responsibilities.
- **Career Development Guidance:** Beyond technical training, the CSIR offers career development advice and guidance. The experts will work closely with the Department's ICT

team to assist in achieving globally recognized certifications such as CompTIA Security+, CompTIA Cybersecurity Analyst+ (CySA+) and amongst others. This training comes with certification voucher exams.

Deliverables:

At the end of this 12-month Human Capital Development Plan, the Department of Labour can expect the following outputs:

- **Trained Professionals:** A significant portion of the ICT team will have completed the training courses listed above.
- **Enhanced Skills and Knowledge:** The ICT team will possess advanced skills in cybersecurity, enabling them to effectively manage and mitigate cyber threats.
- **Career Development Plans:** Individual career development plans for ICT team members, including pathways to achieve further certifications such as CompTIA Security+, CompTIA CySA+, and so on.
- **Documentation and Reports:** Comprehensive documentation and progress reports detailing the training activities, outcomes, and recommendations for future development.

2.5 Contract and Project Management

The main objective of this work package is to provide project and technical management support and administration of the entire project as specified in work packages 1 to 4. The following deliverables are envisioned:

- Support project and contract management including project administration.
- Create an annual high level project schedule for all required activities and services.
- Conduct progress meetings as agreed with the client.
- Compile and deliver progress, monthly and annual reports.
- Preparations and presentation of service definition deliverables
- Perform resource levelling in the project as per the demands and needs of the client from service requirements in this contract.
- Provide project financial and technical progress feedback during project management and project steering committee meetings.
- Monitor of project activities and progress to ensure alignment with contract requirements, stipulations, and work authorisations (WAs)
- Coordinate subcontracting activities as agreed following CSIR procurement processes.
- Conduct project risk assessment and develop mitigations plans/actions.
- Manage ICT security related assets (software and hardware) during the procurement phase and until complete asset transfer to the client.
- Configuration Management
- Quality Control Management

3 Pricing Schedule

The schedules and costs are as follows and include VAT at 15%.

Cost	R	4 719 339.23
VAT	R	707 900.89
Total	R	5 427 240.12

A detailed twelve (12) months costs breakdown per work package is shown in **Table 1**. Invoicing by the CSIR will be done monthly. WP3 and WP4 are optional. The CSIR will only invoice for work done.

Table 1: Cost Breakdown Per Work Package

	Description	Year 1 (Excl. VAT)	SUBTOTAL (Incl. VAT)
WP1	Digital Forensics Investigations	R742 126.01	R853 444.91
WP2	Security Controls Maturity Assessments	R1 580 082.90	R1 817 095.34
WP3	Awareness Training for Employees (optional)	R1 369 405.18	R1 574 815.96
WP4	Human Capital Development for Cybersecurity (optional)	R598 694.30	R688 498.45
	Contract and Project Management	R429 030.84	R493 385.47

Table 2 shows the estimated cost summary over the twelve (12) months of the contract.

Table 2: Estimated Cost Summary

Agreement Year	Cost	VAT	Total Cost VAT Incl.
Year-1 (2024/25)	R4 719 339.23	R707 900.89	R5 427 240.12
Sub Total	R4 719 339.23	R707 900.89	R5 427 240.12

Payment Milestones

The provisional payment milestones indicated in the table below are based on a linear scheduling of the total costs proposed per agreement year. Note: Milestones will be derived from the work packages and roadmap and may be scoped per month by the project team in liaison with NHFC. In addition, should the VAT percentage rate by the South African government change during the period of the contract, the values in **Table 3** will also change accordingly.

Table 3: Payment Milestones

Achievement Plan				
CSIR Project Plan	Department of Labour			
CSIR Project Manager	Mr Muyowa Mutemwa			
Total Contract Value (Excl. Vat)	R4 719 339.23			
Customer Contract Person	acting CIO, Mr Fumani Chabalala			
Contractual Completion Date	*ARO+ 12 months			
Contractual Condition to be Compiled With	Contractual Dates	Indicative Costs Customer To Pay		
		Cost VAT EXCL	VAT 15%	Total VAT INCL
Year 1: Training/Certification		R79 200.00	R11 880.00	R91 080.00
Year 1 Quarter 1 Activities and Progress Report		R1 160 034.81	R174 005.22	R1 334 040.03
Year 1 Quarter 2 Activities and Progress Report		R1 160 034.81	R174 005.22	R1 334 040.03
Year 1 Quarter 3 Activities and Progress Report		R1 160 034.81	R174 005.22	R1 334 040.03
Year 1 Quarter 4 Activities and Progress Report		R1 160 034.81	R174 005.22	R1 334 040.03
TOTAL		R4 719 339.23	R707 900.89	R5 427 240.12

4 General Contracting Information

4.1 Management

Your contact persons at CSIR, D&S are:

Name	Telephone Number/Email	Job Description
Dr Jabu Mtsweni	+27 12 841 4319 (jmtsweni@csir.co.za)	Centre Manager: Information and Cybersecurity Centre (ICSC)
Mr Muyowa Mutemwa	+27 12 841 7326 (mmutemwa@csir.co.za)	Research Group Leader: Data Security and Analytics

4.2 Contract Conditions

The CSIR general contract conditions apply to this contract. A copy is attached for your reference. Depending on your exact requirements some of these clauses can be re-negotiated.

Should the contract be terminated at any point in time due to no fault of the CSIR, the CSIR will be entitled to payment for work performed to date plus commitments incurred.

Should the client require that the terms covered in the Request for Quotation, then the CSIR reserves its rights to negotiate such terms. To that extent, the CSIR further requests the following deviation from such terms:

- where delivery dates are missed, the CSIR requests the right to remedy such delay, prior to Client terminating the order.
- the CSIR requests the opportunity to remedy the non-compliance, and only upon failure to so remedy, shall the Client be entitled to terminate.
- the CSIR requests that the penalty framework be negotiated and agreed upon by the parties, specifically on the computation of such penalties and the application thereof.

4.3 International Financial Reporting Standard 15 Applicability

The International Financial Reporting Standard 15 (IFRS 15) is applicable to this contract. Work performed for the client is confidential and will not be distributed to another party. Should the contract be terminated at any point in time due to no fault of the CSIR, the CSIR will be entitled to payment for work performed to date plus commitments incurred.

4.4 Sub-Contracting

Where materials and/or services have to be procured by the CSIR as part of its execution of the tasks described in this proposal, it will be done according to CSIR policies, regulations and guidelines as governed by the Public Finance Management Act (No.1 of 1999 as amended by Act 29 of 1999) and Preferential Procurement Policy Framework Act (No. 5 of 2000) (PPFA), together with its regulations. Should it not be possible for the CSIR to register a supplier on its procurement framework system, for any reason, it will not be possible to procure materials and/or services from such a supplier.

4.5 Subsistence and Travel

All Subsistence and Travel (S&T) costs will be at CSIR approved rates, in compliance with the National Treasury Instruction on Cost Containment Measures and additional issued instructions, with the latest being Instruction 03 of 2016/17, effective 1 November 2016.

4.6 Intellectual Property

All Intellectual Property relevant to this contract, whether background, historic or foreground, is governed by the Intellectual Property from Publicly Financed Research and Development (IPR-PFRD) Act 51 of 2008.

4.7 Protection of Personal Information

The CSIR is cognisant of the protection of personal information. To this end it has established a Privacy Office, which is responsible for compliance with the Protection of Personal Information Act 4, 2013 (POPIA) once POPIA is fully in force.

4.8 Cost Recovery

Should the contract be terminated at any point in time due to no fault of the CSIR, the CSIR will be entitled to payment for work performed to date plus commitments incurred.

4.9 Security Clearances

In general, DAS staff has Defence Intelligence vetted security clearances. Should it be necessary for other security clearances, the client must make this visible as soon as possible and all costs associated with such vetting requirements are for the cost of the client.

4.10 Validity

This quotation is valid for **120** (one hundred and twenty) days.

4.11 Notes

VAT will be charged at the prevailing rate. Should it change, our price will be adjusted accordingly.

5 Profile of the Project Team (Professional Qualification and Experience)

The CSIR has an experienced and highly qualified team of experts to execute this project. These personnel are professionally qualified and have vast experience providing cyber security services for Department of Labour. This team of professionals can be relied upon to offer cutting-edge expert operational, tactical, and strategic recommendations that are based on new trends and industry standards of good practice in Information and Cyber Security, governance, risk, and compliance thereof. Our team is ready to walk hand-in-hand with your team in also helping address the identified shortcomings.

Name	Professional Qualification	Certification	Experience	Proposed Project Role
Mr Jabu Mtsweni	PhD (Computer Science)	CISSP (Training) PECB ISO27032 Cybersecurity Manager Certified Certified Chief Information Security Officer (Training)	22 Years Cybersecurity Strategy Cyber Risk Assessment/Management Application Development and Implementation Programmes Digital forensics Strategic leadership Lead the Information Security Centre and its associated research groups to contribute to the strategy Contract R&D Leadership Management experience Human capital development Supervise and lead development of junior staff	Contract Manager
Mr Muyowa Mutemwa	MSc (Computer Science)	CISSP - Certified Information Systems Security Professional (544903) – 2022 CEH - Certified Ethical Hacking (ECC48905747097) – 2016 CompTIA CASP+ (COMP001021239259) – 2021 CompTIA Security Analytics Expert (CSAE) (COMP001021239259) – 2021 CompTIA CySA+ (COMP001021239259) - 2019 CompTIA Security Analytics Professional (CSAP) (COMP001021239259) 2019 CompTIA Security+ (COMP001021239259) – 2017 CCNA Cyber Operations Certification 2017 University of the Western Cape, Cisco CCNA 1 - 4 2009 ITIL® Foundation Certificate in IT Service Management - 2015 HP0-S36 - Server Solutions Architect V2 HP ExpertOne - 2015 HP0-S40 - Building HP Server Solutions – 2015	15 Years Cybersecurity Strategy Cyber Risk Assessment/ Cybersecurity Management Application Development and Implementation Programmes Cyber Incident Response Implement and Managing a SIEM SOC Management Digital forensics SOC Management	Pen-Test and Vulnerability Assessments - Technical Expert

Name	Professional Qualification	Certification	Experience	Proposed Project Role
Mr Lungisani Mncwango	BTech	Cisco ACI Test Drive ACI-TD – 2015 CISM certified ISO 27001 Lead Implementer (Downgraded to : ISO/IEC 27001 Provisional Implementer) CCNA Security Certified Security + (Expired)	10 Years Vulnerability Assessment and Pen-testing Threat modelling and risk assessments Network security Digital forensics Threat modelling and risk assessments Cybersecurity incident management Cybersecurity operations centre management	Pen-Test and Vulnerability Assessments – Team Member - Cybersecurity Specialist
Dr Moses Dlamini	PhD	CISSP Training, GDPR Training	20 Years Development of ICT Strategy and ICT Governance Framework Development of Cybersecurity Strategy Cybersecurity/IT relate policy and SOPs review Cybersecurity/IT related GAP analysis Strategic information security & privacy research Information security design, model, and architect Cybersecurity trend analysis and provide insights on the direction and outlook of cybersecurity and how to defend against futuristic cyber threats Information security audit assessments Supervise junior staff and M&D students	Cybersecurity Governance - Team Member - Expert
Mr Alex Ramantswana	Diploma Information Technology	CompTIA Security + Training	6 Years Vulnerability Assessment and Pen-testing Threat modelling and risk assessments Network security Digital forensics Threat modelling and risk assessments Cybersecurity incident management Cybersecurity operations centre management Cybersecurity and IT auditing on domain controller, Windows Server, Linux, SQL Server, DB2 and AIX	Pen-Test and Vulnerability Assessments - Team Member – Cybersecurity Specialist
Mr Samson Chishiri	BSc Honours	CISSP Certified CompTIA Security + Cisco Certified Security Core CCNA Security	9 Years Data centre audits Cybersecurity Audit assessments	Pen-Test and Vulnerability Assessments - Team Member - Firewall Engineer

Name	Professional Qualification	Certification	Experience	Proposed Project Role
		CCNA Routing and Switching Microsoft Certified Technology Specialist NSE4 Network Security Professional Training	Vulnerability assessments and pen-test Network security Digital forensics Threat modelling and risk assessments Cybersecurity incident management Cybersecurity operations centre management Cybersecurity and IT auditing on domain controller, Windows Server, Linux, SQL Server, DB2 and AIX	
Mr Rofhiwa Netshiya	BSc Honors	CompTIA Security+ CompTIA CySA+ CompTIA PenTest+	5 Years Network Security Management Cybersecurity Incident Response Vulnerability Assessments and Penetration Testing	Pen-Test and Vulnerability Assessments - Team Member - Expert Cybersecurity Engineer
Mr Mfundo Masango	BTech Software Development	CEH Certified Security+ Certified PenTest+ (Training) Splunk CySA (Training)	6 Years Vulnerability Assessment Penetration Testing Cybersecurity Awareness Training Software Development Cyber Incident Response Configure, Implement and Manage a SIEM SOC Management Infrastructure Management Cybersecurity Awareness	Cyber Security Specialist Pen-Test and Vulnerability Assessments - Team Member
Ms Kele Masemola			2 Years Digital Forensics Cybersecurity Engineer SOAR Cybersecurity Engineer VMWare	Cybersecurity Specialist
Mr Norman Nelufule	Mphil Electrical and Electronics Engineering	ISO 27001 Lead Implementer (Downgraded to : ISO/IEC 27001 Provisional Implementer) NIST Training	5 Years SOC Management Cybersecurity incident management Digital forensics Cybersecurity Awareness Training	Cybersecurity Specialist and Researcher
Ms Ntombizodwa Thwala	Bachelor's degree (Information Systems)		2 years SOC Management Digital forensics Awareness Training Data Collection, visualization and analytics Penetration Testing	Cyber Security Analyst



Name	Professional Qualification	Certification	Experience	Proposed Project Role
			Vulnerability Assessment	

6 SIMILAR ASSIGNMENTS AND REFERENCES

Clients	Contact Person	Physical Address	Email Address	Phone Number	Service Provisioned
City of Johannesburg (South Africa)	Mr Thokozani Nkosi	Metropolitan Centre, 158 Civic Boulevard, Braamfontein, Johannesburg	ThokozaniCyrilN@joburg.org.za	+27 11 018 6445	Establishment of the City of Joburg's ICT Security and Cyber Centre and Development of Smart City ICT Strategy and Advisory Services
Eswatini Electricity Company (Eswatini)	Mr Phiwokwakhe Dlamini	Eswatini Electricity Company (EEC), Eluvatsini House, Mhlambanyatsi Road, Mbabane, Eswatini	Phiwokwakhe.dlamini@eec.co.sz	+268 2409 4000	Information/Cyber Security Audit Assessment, IT Security Governance Review Assessment, Cybersecurity Strategy and Incident Response Plan
RAND Water Utility (South Africa)	Mr Dumisani Hlongwane	RAND Water Head Office, 522 Impala Road, Glenvista, 2058, South Africa	Dumisani.hlongwane@randwater.co.za	+27 11 682 0911	Cybersecurity Posture Assessment, Development of an IT and OT Gap Analysis and Cybersecurity Strategy and Implementation Plan
Senegal National Electricity Agency (Dakar, Senegal)	Mr Mouhamadou	Senelec, Head Quarters, 28 Rue Vincens, BP 93, Dakar, Senegal	Mouhamadou@senelec.sn	+221 33 839 30 30	Information Security Audit Assessment and Development of an IT and OT Security Strategy, Architecture and Implementation Plan
The Presidency (South Africa)	Ms Yasmeen Ismail	The Presidency, Union Buildings, Government Avenue, Pretoria, South Africa	Yasmeen.Ismail@presidency.gov.za	+27 12 300 5200	Review of the e-Government Strategy
Gauteng Department of e-Government (South Africa)	Mr Thulani Mafalala	Gauteng Department of e-Government, 75 Fox St, Marshalltown, Johannesburg, 2001	thulani.mafalala@gauteng.gov.za	+27 11 689 8506	CSIR/e-Gov Partnership on 4IR Implementation, use Gauteng as a prototype for the development of a National Cyber Security Strategy. 4IR Strategy Initiatives.

The above is just a snapshot of some of our work and is by no way an exhaustive list.

7 Additional Previous Project Experience

The CSIR regularly performs information and cyber security capability development and assessments for both private and public sector clients, including: Military, State Security Agency (SSA), Law Enforcement Agencies (LEAs) and Department of Communications and Digital Technologies (DCDT) - Cybersecurity Hub, City of Johannesburg, Department of International Relations and Corporation (DIRCO), Department of Justice (DoJ), Senelec SA (Senegal Electricity Company), Eswatini Electricity Company (EEC), Rand Water, Reutech, and others. Due to client confidentiality, this section will only be discussed with regards to three environments and none of the clients are to be mentioned.

7.1 Military Environment

The military environment is one of the main focuses of the CSIR. Since 2005 the military has requested that the CSIR perform information and cyber security capability development, and assessment services on specific military bases on an annual basis. This assessment aspect of the work is focused on determining whether there are any known security vulnerabilities, threats, or any malware present on the infrastructure. Additional tests are performed to determine whether there is adequate network separation due to specific requirements within the environment. After the assessments a report is provided and the CSIR assists the military to act upon the remediation techniques. The relationship that the CSIR has had with the military has led to a significant improvement, concerning national cybersecurity, in the network deployments or existing infrastructure.

7.2 Public Sector

The CSIR also provides cybersecurity capability development and assessment services to the public sector, such as municipalities and state departments. This type of security assessment is more in line with determining whether 3rd party vendors are adequately implementing the correct security control measures. The CSIR has ongoing relationships with these organisations and continuously assists the government departments to improve their information and cyber security maturity level and overall posture. The focus of these security assessments is more focused on determining the gap in current infrastructure and how the infrastructure can be upgraded to improve security concerns. The CSIR is also assisting municipalities, such as the City of Johannesburg (CoJ) to create a security operations centre for their own environment. The CSIR has also assisted in formulating Rand Water's cybersecurity strategy.

7.3 Private Sector

The CSIR has several clients within the private sector. Some specific organisations do utilise the CSIR though, due to the complexity of their information and cyber security requirements and the experience the council has. The employees at the CSIR are also researchers and thus have the capability of performing information and

cyber security capability development and assessments on cutting edge technologies and can ensure that our clients are future-proof when it comes to the informed and well-researched recommendations. In the case where the private sectors require information and cyber security capability development and assessments on these new and upcoming technologies, the CSIR is called upon to assist. In this case, the CSIR focuses on assisting the organisation to deploy new solutions with the required security constraints as per industry best practices. It is important to mention that the CSIR is not affiliated with any of the Information and Cyber Security vendors. Therefore, our recommendations are solely based on how best to address the needs of our clients.

8 CSIR Institution Profile

General Information	
Registered Name of the Institution	The Council for Scientific and Industrial Research
Address of the Registered Office of Head Office	The Council for Scientific and Industrial Research Meiring Naude Rd Brummeria Pretoria 0001
Mailing Address	Defence & Security Unit Information Cyber Security Center, Building 44 Meiring Naude Rd Brummeria Pretoria 0001
VAT Number	4470114283
Phone Number	+ 27 12 841 2911
Type of Entity	Research, Development and Innovation Organization
Date of Establishment	1945, 78 years in business
Name of Chief Executive	Dr Thulani Dlamini
Name of Authorized Signatory	Dr Jabu Mtsweni
Name of Contact Person	Mr Muyowa Mutemwa

9 CSIR General Contract Conditions

Next page.

CSIR GENERAL CONTRACT CONDITIONS

1. DEFINITIONS AND INTERPRETATION

1.1. The headings of the clauses in this Contract are for the purpose of convenience and reference only and shall not be used in the interpretation of nor modify nor amplify the terms of this Contract nor any clause hereof. Unless a contrary intention clearly appears. Words importing -

1.1.1. any one gender includes the other two genders;

1.1.2. the singular includes the plural and vice versa; and

1.1.3. persons include natural and juristic persons and state organs.

1.1. The following terms shall have the meanings assigned to them hereunder and cognate expressions shall have corresponding meanings, namely -

1.1.1. **"Affiliate"** shall mean, in relation to either Party, any natural or juristic person that is an owner, partner, parent company, subsidiary, collaborators, sub-contractors or any person that is otherwise directly and/or indirectly related to such Party;

1.1.2. **"Background Intellectual Property"** means any Intellectual Property which was owned or controlled by the CSIR prior to the Works but which is relevant and required for the successful execution of the Works.

1.1.3. **"Business Day"** means any day other than a Saturday, Sunday or proclaimed public holiday officially recognised as such in the Republic of South Africa.

1.1.4. **"Client"** means the recipient of the Work.

1.1.5. **"Commercialisation"** means the process by which any intellectual property emanating from publicly financed research and development is or may be adapted or used for any purpose that may provide any benefit to society or commercial use on reasonable terms, and **"Commercialise"** shall have a corresponding meaning

1.1.6. **"Contract"** means the Proposal as accepted by the Client together with these general conditions of contract, which - read together - comprise the agreement between the Parties in respect of the Work.

1.1.7. **"Compliant Tax Status"** means a tax status of compliant at the relevant date, as depicted on the central supplier database, the SARS' tax compliance status system, or by valid tax clearance certificate obtained from SARS or from the SARS' tax compliance status system.

1.1.1. **"CSIR"** means the CSIR, a juristic person, established in accordance with the Scientific Research Council Act, Act No. 46 of 1988.

1.1.2. **"Foreground Intellectual Property"** means inventions, patent applications and patents; branding and trade marks (whether or not registered); copyright and works of authorship; registered and unregistered designs; trade secrets and know-how; software and algorithms; domain names and web presence; advertising and promotional material; and all tangible and intangible representations and manifestations of such intellectual property, which are developed in the course of the Work.

1.1.3. **"Parties"** means the CSIR and the Client, and **"Party"** shall mean any one of them, as the context may require.

1.1.4. **"POPI Act"** means the Protection of Personal Information Act No. 4 of 2013.

1.1.5. **"Prime Rate"** means the publicly quoted basic rate of interest, compounded monthly in arrears and calculated on a 365 (three hundred and sixty-five) day year, irrespective of whether or not the year is a leap year, from time to time published by the Reserve Bank of South Africa bank as being its prime overdraft rate, as certified by any representative of that bank whose appointment and designation it will not be necessary to prove.

1.1.6. **"Proposal"** means the proposal attached hereto, and setting out the scope of the Works.

1.1.7. **"SARS"** means the South African Revenue Service.

1.1.8. **"Work"** means the goods and/or services and/or deliverables as outlined in the Proposal, and includes any work that may have been involved in the preparation of the Proposal.

1.2. When any number of days is prescribed in this Contract, same shall be reckoned exclusively of the first and inclusively of the last day unless the last day is not a Business Day, in which case the last day shall be the next succeeding Business Day.

1.3. Where figures are referred to in numerals and in words, and there is any conflict between the two, the words shall prevail, unless the context indicates a contrary intention or the Party supporting the accuracy of the numerals over the words is able to prove, on a balance of probabilities, that the numerals are correct.

1.4. The expiration or termination of this Contract shall not affect such of the provisions of this Contract as expressly provide that they will operate after any such expiration or termination or which of necessity must continue to have effect after such expiration or termination, notwithstanding that the clauses themselves do not expressly provide for this;

1.5. The rule of construction that a contract shall be interpreted against the Party responsible for the drafting or preparation of the contract, shall not apply.

2. PURPOSE AND SCOPE OF THE PROPOSAL

2.1. The Client confirms that the purpose for the request of the Work as set out in the accompanying Proposal has been disclosed in full to the CSIR.

2.2. Unless specifically indicated otherwise by the Client as part of the disclosure envisaged by 2.1 above, CSIR will assume that the Work is not to be conducted for purposes of any dispute, litigation or arbitration proceedings. In the event that CSIR or any of its employees are subsequently ordered to testify on aspects of the Work, the Client shall be liable to pay CSIR a fee equal to CSIR's prevailing hourly rate for the individual(s) required to testify and the reasonable costs incurred in connection with attendance at the relevant proceedings.

2.3. The contents of the Proposal (as well as all discussions and/or documents leading to the finalisation thereof) constitute Confidential Information, and shall specifically not be divulged by the Client to any unauthorized third party.

3. WORK, RISK, PRICING AND OWNERSHIP

3.1. The Work shall be executed according to the Proposal and subject to any conditions contained in such Proposal. In the event of any conflict between the provisions of these general contract conditions and those as contained in the Proposal, the provisions as contained in the Proposal shall prevail.

3.2. The Client assumes all liability for risk and/or loss in respect of any item placed in possession of the CSIR under the Proposal.



- 3.3. The prices are based on the prevailing cost of material and labour, subject to:
- 3.3.1. alteration in time and costs;
- 3.3.2. exchange rates; and
- 3.3.3. price of goods quoted or of any part of the Work sub-contracted to a third party and import duty, freight and cartage.
- 3.4. All costs of delivery to Client will be for the account of the Client, unless otherwise stated in the Proposal.
- 3.5. The Client shall not be entitled to reduce the contract price, or contract amount, or scope of work stated in the Proposal without the CSIR's prior written consent. In the event of the Client unilaterally reducing the scope of the Work, the Client shall nevertheless remain liable for the full contract price.
- 3.6. The Client shall ensure that it:
- 3.6.1. co-operates with the CSIR in all matters relating to the Work;
- 3.6.2. provides, in a timely manner and at no charge, access to its premises, office accommodation, data and other facilities as may be reasonably required by the CSIR for the purpose of the Work; and
- 3.6.3. provides, in a timely manner, all documents, information, items and materials in any form (whether owned by the Client or third party) as may be reasonably required by the CSIR in connection with the Work and ensure that they are accurate and complete in all material respects.

4. WORK, RISK, PRICING AND OWNERSHIP

- 4.1 The Work shall be executed according to the Proposal and subject to any conditions contained in such Proposal. In the event of any conflict between the provisions of these general contract conditions and those as contained in the Proposal, the provisions as contained in the Proposal shall prevail.
- 4.2 The Client assumes all liability for risk and/or loss in respect of any item placed in possession of the CSIR under the Proposal, where applicable.
- 4.3 The prices are based on the prevailing cost of material and labour, subject to:
- 4.3.1 alteration in time and costs;
- 4.3.2 exchange rates; and
- 4.3.3 price of goods quoted or of any part of the Work sub-contracted to a third party and import duty, freight and cartage.
- 4.4 All costs of delivery to Client will be for the account of the Client, unless otherwise stated in the Proposal.
- 4.5 The Parties shall not be entitled to amend the contract price, or contract amount, or scope of work stated in the Proposal. In the event of a change in scope, the Parties shall agree the amendment of such scope together with any changes to the contract price.
- 4.6 The Client shall ensure that it:
- 4.6.1 co-operates with the CSIR in all matters relating to the Work;
- 4.6.2 provides, in a timely manner and at no charge, access to its premises, office accommodation, data and other facilities as may be reasonably required by the CSIR for the purpose of the Work; and
- 4.6.3 provides, in a timely manner, all documents, information, items and materials in any form (whether owned by the Client or third party) as may be reasonably required by the CSIR in connection with the Work and ensure that they are accurate and complete in all material respects.

5. USE OF NAMES/LOGOS

Neither Party is, by virtue of their association hereunder, authorised to use the name, logo(s) or trademarks of the other in connection with any advertising, publicity, marketing or promotional materials or activities, or for any other purpose whatsoever, without the prior written consent of the other Party. FOR PURPOSES OF THIS CLAUSE, THE CLIENT ALSO RECOGNISES THAT, UNDER THE PROVISIONS OF SECTION 15 (1) OF THE MERCHANDISE MARKS ACT, 1941 (ACT 17 OF 1941), THE USE OF THE ABBREVIATION OF THE NAME OF THE COUNCIL FOR SCIENTIFIC AND INDUSTRIAL RESEARCH, "WNNR" AND CSIR, IS PROHIBITED IN CONNECTION WITH ANY TRADE, BUSINESS, PROFESSION OR OCCUPATION OR IN CONNECTION WITH A TRADE MARK, MARK OR TRADE DESCRIPTION APPLIED TO GOODS, OTHER THAN WITH THE CONSENT OF THE CSIR.

6. ACCEPTANCE OF CONDITIONS

- 6.1. Acceptance of the Proposal or instruction by the Client to the CSIR to commence with the Work shall constitute acceptance of these conditions, save to the extent where the same has been modified as envisaged by clause 3.1 above.
- 6.2. The person accepting the Proposal on behalf of the Client, where applicable, warrants that he/she is duly authorized so to act on behalf of the Client and also warrants that the legal entity of the Client is as stipulated in the Proposal. Should it subsequently appear that he/she was not in fact so authorised, or that incorrect information was supplied with regard to the Client's legal status, he/she will be liable as surety and co-principal debtor, in his/her personal capacity, as against the CSIR, for the fulfilment of all the obligations contained herein, and will in his/her personal capacity be bound by all the terms and conditions contained in both the Proposal and herein.

7. PAYMENT

- 7.1. If the attached Proposal stipulates an advance payment, the CSIR will not commence Work as set out in the Proposal until the said advance payment has been received by the CSIR. Any delay occasioned by a late payment, shall be added to the contract period.
- 7.2. All payments will be strictly made within thirty (30) days of the date of invoice, or the date on which payment is due to the CSIR, in terms of the Proposal.
- 7.3. All payments shall be made by the Client without deduction or set-off of whatsoever nature, and no discounts for early settlement will be allowed on the amounts due to the CSIR.
- 7.4. Failure by the Client to make any payment punctually on due date shall constitute a material breach of this Contract and shall entitle the CSIR to forthwith claim payment of the remainder of the contract price, as well as all legal costs incurred by the CSIR on the scale as between attorney and own client, including collection commission – and in addition shall also entitle the CSIR to invoke the provisions of clause 17 (*Breach and Termination*) below.
- 7.5. Any payments due to the CSIR which are not remitted within the time period contemplated in clause 7.2 will incur interest at a rate equal to the Prime Rate, calculated monthly in arrears from the due date of such payment to the date of payment in full.
- 7.6. To ensure the Client's fulfilment of its on-going payment obligations for the Works in terms of the Contract, the CSIR shall be entitled to require a parent payment guarantee issued against an Affiliate of the Client specified by the CSIR. In the event of a payment guarantee being a contractual requirement, this Contract shall be subject to the suspensive condition that the Client or its Affiliate furnishes a parent guarantee to the satisfaction of the CSIR.
- 7.7. The Client's signatory warrants that he/she is duly authorised to enter into this agreement on behalf of the Client, and hereby binds himself/herself as surety and co-principal debtor in favour of the CSIR for all the obligations of the Client in terms of this Contract (including any amounts which may become owing arising out of any breach of this Contract) and renounces the benefits of excussion, division, cession of action and de duobus vel pluribus reis debendi the meaning and full force and effects of such benefits the signatory/surety acknowledges he/she knows and understands.

8. INTELLECTUAL PROPERTY

8.1. Background Intellectual Property, whether registered or unregistered, vests in the CSIR, unless agreed otherwise between the parties in writing.

8.2. The CSIR hereby grants to the Client a non-exclusive option to Commercialise CSIR Background Intellectual Property on terms to be agreed and recorded in future agreements, as required. The Client acknowledges that the licensing or other Commercialisation of CSIR Background Intellectual Property will attract a once off upfront payment and royalty payments throughout the term of the agreement, for such licensing or other Commercialisation.

8.3. The Client shall provide the CSIR with written notification of its intention to exercise its option to Commercialise CSIR Background Intellectual Property within one (1) month of the conclusion of the Works, unless otherwise agreed to in writing. The Parties shall act in good faith to conclude an agreement giving effect to this option so exercised, within two (2) weeks of receipt of such notice by the CSIR. Should the Client not wish to exercise its option, and/or fail to notify the CSIR within the prescribed period, the option to Commercialise CSIR Background Intellectual Property shall automatically convert to a non-exclusive option. The Client will have been deemed to have abandoned its non-exclusive option to Commercialise the CSIR Background Intellectual Property within six (6) months of the conclusion of the Works, unless otherwise advised in writing by the Client.

8.4. Foreground Intellectual Property shall be dealt with in terms of the Intellectual Property Rights from Publicly Funded Research and Development Act, 2008, as amended, with the intention of the Parties being that the Client may acquire rights to any Foreground IP that may be created pursuant to the Works.

9. CONFIDENTIALITY

9.1. For purposes of this clause, "Confidential Information" means any information received or obtained by the Parties: (i) as a result of entering into this Contract; or (ii) in connection with the business of either of the Parties relating to this Contract, including, without limitation, any past, present, or future research, development, commercial, financial, technical, marketing or other data, know-how, trade secrets or any other information of whatever nature in whatever form. The Party disclosing the confidential information is referred to as "the Disclosing Party" and the Party receiving such information as "the Recipient".

9.2. The contents of any interim reports issued by the CSIR comprise CSIR confidential information unless the CSIR has granted its written consent to the Client to divulge the contents of such report.

9.3. The Recipient shall:

9.3.1. treat as strictly confidential and secret any and all information given or made known to it during the contract period.

9.3.2. keep all Confidential information secret towards third Parties and only use it in co-operation with the Disclosing Party for the purpose expressly agreed upon by the Parties and to disclose same to its employees or professional advisors, only on the basis of the need to know, and then and provided that such Party undertakes to ensure that such employees or professional advisors are made aware of the confidential nature of the information being made available to them; and

9.3.3. accept responsibility for the observance by its employees and professional advisors of the secrecy undertakings contained herein; and

9.3.4. not directly or indirectly use for its benefit or the benefit of any other person any Confidential Information other than for the purposes of fulfilling its obligations under this Contract.

9.3.5. The above undertakings shall not apply to:

9.3.6. Information which at the time of disclosure is published or otherwise generally available to the public;

9.3.7. Information which the Recipient can show was in its possession at the time of disclosure by the Disclosing Party;

9.3.8. Information rightfully acquired from others who did not obtain it under pledge of secrecy to either of the Parties;

9.3.9. Information contained in any final report issued by the CSIR; and

9.3.10. Information which the Recipient is obliged to disclose in terms of a court order, subpoena or other legal process.

9.4. In the event that the Recipient is required by legal process to disclose any of the Confidential Information, covered by this clause 9 (*Confidentiality*), it shall provide the Disclosing Party with prompt written notice of such requirements so as to enable the Disclosing Party to seek a protective order or waive compliance with the provisions of this clause. In the event that a protective order or other remedy is obtained, the Recipient shall use all reasonable efforts to ensure that only the information covered by such order or other remedy is disclosed. Whether or not a protective order or other remedy is obtained or a Party has waived compliance with the provisions of this clause 9 (*Confidentiality*), the Recipient shall take all reasonable steps to ensure that only that portion of the information that it is legally required to disclose is so disclosed.

9.5. Each Party agrees to return to the other or destroy, at such other Party's election and request, all copies of any documents which it may have obtained from the disclosing Party as a result of Confidential Information being made available to them as contemplated in clause 9.1.

10. PERSONAL INFORMATION

10.1. Each Party consents to the other Party holding and processing "personal information" (as defined in the POPI Act) relating to it for legal, personnel, administrative and management purposes (including, if applicable, any "special personal information" relating to him/her, as defined in the POPI Act). Notwithstanding the generality of the aforesaid, each Party hereby undertakes to comply with all relevant provisions of the POPI Act and any other applicable data protection laws. The Client further agrees to comply with all CSIR's reasonable internal governance requirements pertaining to data protection.

10.2. Each Party consents to the other Party making such information available to those who provide products or services to such parties (such as advisers, regulatory authorities, governmental or quasi-governmental organisations and potential purchasers of such Party or any part of their business).

10.3. The Client consents to the transfer of such information to CSIR's business contacts outside South Africa in order to further its business interests.

10.4. While performing any activity where a Party is handling personal information as a "responsible party" (as defined in the POPI Act), each Party undertakes that it will process the personal information strictly in accordance with the terms of the POPI Act, this Contract, and the other Party's instructions from time to time, and take appropriate operational measures to safeguard the data against any unauthorised access.

10.5. Each Party acknowledges that in the course of conducting business with each other, each Party intends to maintain and process personal information about the other Party in an internal database. By signing this Contract, each Party consents to the maintenance and processing of such personal information.

10.6. Where relevant, the Client shall procure that all of its personnel, agents, representatives, contractors, sub-contractors and mandataries shall comply with the provisions of this clause 10 (*Personal Information*). The CSIR shall be entitled on reasonable notice to conduct an inspection or audit Client's compliance with the requisite POPI Act safeguards.

11. NO WARRANTIES

11.1. The CSIR does not warrant the merchantability, commercial viability or fitness for particular purpose of the Work as specified in the Proposal.

11.2. Where the Works incorporate the provisions of any goods or products to the Client such goods and/or products are provided "voetstoots".

11.3. The CSIR hereby warrants that:



- 11.3.1 it has the authority and capacity to develop the Work and that, to the best of its knowledge, its development of the Work does not infringe on the IP rights of any other party; and
- 11.3.2 it possesses the requisite skills and expertise to carry out the Works and shall use its best endeavours to ensure that any changes to the project team shall not affect the development of the Work.
12. **LIMITATION OF LIABILITY**
- 12.1. Subject to the provisions of clause 3.2 above and clause 13 (*Force Majeure*) below, the CSIR's total liability for all claims brought against it under this Contract for damages, whether in delict or based on this Contract, and for all legal, accountancy and other costs, fees and expenses incurred by the Client in seeking to enforce its rights in respect of such claims, shall not exceed an amount equal to total value of the Contract or the amount actually paid by the Client to the CSIR in respect of the work performed in terms of this Contract, whichever is the lesser (the "Cap"). For the avoidance of doubt, the Client shall not be entitled to claim any amounts in excess of the Cap under this Contract, save in respect of circumstances where there has been fraud or wilful misconduct.
- 12.2. The Parties shall not be liable to each other for any indirect or consequential loss or damage, including, but not limited to, loss of profit, revenue, anticipated savings, business transactions or goodwill.
- 12.3. Nothing in this Contract shall be construed as relieving the Client of its common law duty to mitigate its loss.
13. **FORCE MAJEURE**
- 13.1. If either Party is prevented or restricted directly or indirectly from carrying out all or any of its obligations under this Contract, including but not limited to, by reason of strike, lock-out, fire, explosion, floods, riot, war, accident, acts of God, embargo, legislation, shortage of or a breakdown in transportation facilities, civil commotion, unrest or disturbances, cessation of labour, government interference or control, or any other cause or contingency beyond its foreseeable control ("*force majeure event*"), the Party so affected shall be relieved of its obligations hereunder during the period that such event and its consequences continue, but only to the extent so prevented and shall not be liable for any delay or failure in the performance of any obligations hereunder or loss or damages either general, special or consequential which the other Party may suffer due to or resulting from such delay or failure, provided always that written notice shall be given by the Party claiming force majeure of any such inability to perform by no later than [5 (five)] Business Days after the start of the force majeure event.
- 13.2. For the avoidance of doubt, this Contract, or the affected part of it, shall be suspended for the period during which the force majeure event continues and the time for performance of an obligation so suspended, shall be extended accordingly. The party not claiming *force majeure* shall not be obliged to comply with reciprocal obligations to those obligations suspended in the period during which the *force majeure* subsists.
- 13.3. Either Party invoking *force majeure* shall, within 5 (five) Business Days of the termination of the *force majeure* event give written notice thereof to the other Party.
- 13.4. An event of *force majeure* will not relieve a Party from any obligation which arose before the occurrence of the *force majeure event*.
- 13.5. Should such *force majeure* continue for a period of more than 90 (ninety) [Business Days] then either Party shall be entitled forthwith to cancel this Contract in respect of any obligations still to be performed hereunder.
14. **NON-WAIVER**
- No relaxation or indulgence granted by the CSIR and no omission by the CSIR timeously or diligently to enforce any right under this Contract shall be deemed to amount to a waiver of that or any other rights.

15. **GOVERNING LAW**

This Contract and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed and enforced according to and governed by the laws of the Republic of South Africa.

16. **DISPUTE RESOLUTION**

16.1. Mediation

16.1.1. In the event of any dispute arising from or out of the Contract, the Parties shall use every reasonable effort to settle such dispute amicably within twenty (20) Business Days of such dispute rising, at project level.

16.1.2. If the Parties fail to resolve any dispute at project level, such dispute must be elevated to the Parties' respective senior management, i.e. Chief Executive Officers, Managing Directors or their duly designated representatives for mediation purposes.

16.1.3. To the extent that no settlement is reached in terms clause 16.1.2 within twenty (20) Business Days of referral, the dispute may be referred to a competent court with jurisdiction, unless the Parties agree to resolve such dispute through arbitration, in which event clause 16.2 would apply.

16.2. Arbitration

16.2.1. Save to the extent stipulated in the agreement contemplated in clause 16.1.3, disputes referred for arbitration shall be determined in accordance with the commercial arbitration rules of the Arbitration Foundation of Southern Africa ("AFSA");

16.2.2. The Parties shall agree on the arbitrator who shall be an attorney or senior advocate (with at least 10 years' experience in commercial legal practice) on the panel of arbitrators of AFSA. If agreement is not reached within 10 Business Days after any Party calls in writing for such agreement, the arbitrator shall be an attorney or senior advocate (with at least 10 years' experience in commercial legal practice) nominated by the Chairman of AFSA for the time being;

16.2.3. The request to nominate an arbitrator shall be in writing outlining the claim and any counterclaim of which the Party concerned is aware and, if desired, suggesting suitable nominees for appointment as arbitrator, and a copy shall be furnished to the other Parties who may, within 5 Business Days, submit written comments on the request to the addressee of the request with a copy to the first Party;

16.2.4. The Arbitrator shall determine the dispute in accordance with Arbitration Act, 1965 (as amended) and shall have the same remedial powers as a court of law would have were it adjudicating the dispute; and

16.2.5. The arbitration shall be held in Pretoria (or virtually if agreed by both Parties) unless the Parties agree in writing of an alternative place. The Parties shall endeavour to ensure that the arbitration proceedings are completed within 90 days after notice requiring the claim to be referred to arbitration is given.

16.3. Nothing contained in this clause 16 shall prohibit a Party from approaching any court of competent jurisdiction for urgent or interim relief pending the determination of the dispute by arbitration. In respect of such proceedings, each of the Parties specifically consents to the non-exclusive jurisdiction of a High Court of South Africa.

17. **BREACH AND TERMINATION**

17.1. In the event of either of the Parties ("**the defaulting Party**") committing a material breach of any of the terms and conditions of this Contract, and remaining in default for a period of seven (7) Business Days after receipt by it of written notice from the other Party ("**the innocent Party**") calling for such breach to be remedied, the innocent Party shall be entitled, without prejudice to any other rights it may have in terms of this Contract or in law, to terminate this Contract by written notice to that effect given to the defaulting Party.

17.2. Either Party may terminate this Contract at any time by giving to the other ("**the defaulting Party**") notice of such termination if:



17.2.1. the defaulting Party or any of its Affiliates is, other than for the purposes of reconstruction or amalgamation, placed under voluntary or compulsory liquidation or under judicial management or under receivership or under the equivalent of any of the foregoing;

17.2.2. a final and un-appealable judgement against the defaulting Party or any of its Affiliates remains unsatisfied for a period of fourteen (14) Business Days or more after it comes to the notice of the management of the defaulting Party;

17.2.3. the defaulting Party or any of its Affiliates makes any arrangement or compromise with its creditors generally, or ceases, or threatens to cease, to carry on business.

17.3. In the event that any of the milestones/deliverables set out in the Proposal are not met either at all or sufficiently to allow the progression of the project, or if any of the project dependencies are not realized, then either Party shall be entitled to terminate the Contract on 14 days' prior written notice to the other.

18. SUSPENSION, NON-BREACH TERMINATION AND CONSEQUENCES FOR TERMINATION

18.1. The CSIR may, on good grounds shown, at its sole discretion, suspend the provision of Work on notice to the Client for such period/s as the CSIR may determine. The suspension may be revoked and/or suspension period shortened or extended on such reasonable terms as may be communicated by the CSIR.

18.2. In the event of a suspension of Works for a period of more than sixty (60) consecutive days, the Client may terminate the Contract on thirty (30) days' prior written notice to the CSIR, subject to the prevailing terms of the Contract.

18.3. The CSIR may at any time terminate the Contract on thirty (30) days prior written notice to the Client, at no cost or further recourse to the Client.

18.4. This Contract may at any time be terminated by mutual and written agreement between the Parties.

18.5. The suspension of Work, or expiry, termination, or cancellation of the Contract for any reason shall not affect either Party's rights that may have accrued prior to such suspension, expiry, termination, or cancellation. CSIR's accrued rights shall include the right to payment in respect of Work undertaken or commenced, expenses incurred, and/or commitments undertaken prior to the effective date of any of the abovementioned events.

18.6. Any termination of this Contract shall not absolve the Parties from the obligation to observe the confidentiality measures and other restraints as set out herein. It is specifically recorded that the provisions of clauses 8, 9, 15, 16 and 20 (all inclusive) shall survive the termination of this Contract for whatever reason, and in perpetuity.

19. REVENUE

19.1. For the purposes of this clause 19 (*Revenue*), "Termination Date" shall mean the "Termination Date" specified in the Proposal.

19.2. The Parties hereby agree and record that all payments made by the Client to the CSIR for the work performed under this Contract, shall be non-refundable. For the avoidance of doubt, notwithstanding anything to the contrary contained in this Contract, should this Contract be terminated by either Party for whatsoever reason on or before the Termination Date, the CSIR shall not be obliged to refund or return to the Client any amounts already paid by the Client to the CSIR in terms of this Contract, and, all outstanding invoices at such date will remain due and owing by the Client to the CSIR.

19.3. Notwithstanding the termination or cancellation of this Contract, for any reason whatsoever, this clause 19 (*Revenue*) shall remain valid and enforceable for so long as any amounts remain due and owing by the Client to the CSIR, including without limitations any and all amounts in respect of which the CSIR has issued an invoice to the Client and which remain unpaid.

20. ANTI-CORRUPTION

20.1. "Anti-Corruption Laws" means any and all local and/or foreign anti-corruption laws that are directly or indirectly applicable to (a) this Contract; (b) either Party to this Contract; (c) the Work; and/or (d) the transactions contemplated by this Contract, including the Prevention and Combating of Corrupt Activities Act 12 of 2004.

20.2. The Client acknowledges that the CSIR is subject to the Anti-Corruption Laws and understands its and the CSIR's obligations under the applicable Anti-Corruption Laws.

20.3. The Client warrants that to its best knowledge and belief neither the Client nor any of its personnel or principals is or has been:

20.3.1. convicted or charged with any crime involving corruption; and

20.3.2. the target or subject of any criminal investigation involving corruption or other criminal wrongdoing.

20.4. As an on-going warranty throughout the duration of this Contract, the Client warrants that it shall not make, or authorise or tolerate to be made, in the performance of this Contract, any payments, loans or gifts, or promises or offers of payments, loans or gifts, of any money or anything of value, directly or indirectly, to or for the use or benefit of any person the making of which would violate the Anti-Corruption Laws.

20.5. Without prejudice to any other rights which the CSIR may have under this Contract or by law, if the Client breaches any of the warranties set forth in this clause 20 (*Anti-Corruption*):

20.5.1. the CSIR shall have a right of action against the Client for the amount of any monetary payment or thing of value made or given by the Client in breach of any of the above mentioned warranties;

20.5.2. all obligations by the CSIR to pay any amounts of monies to the Client shall cease immediately and without notice; and

20.5.3. the CSIR may, in its sole discretion rescind this Contract with immediate effect and the Client shall hold harmless and indemnify the CSIR from any damage or loss, of whatever kind or nature, arising from any transaction in violation of this clause 20 (*Anti-Corruption*).

21. NON-SOLICITATION

21.1. Neither Party will, for the duration of this Contract and for twelve (12) months after the termination of this Contract, without the prior written consent of the other Party, solicit for employment or entice away from the other Party, whether directly or indirectly, any person who during the currency of this Contract is/was an employee or contractor of the other Party.

21.2. To the extent that either Party breaches the provisions of this clause 21 (*Non-Solicitation*) (the "Defaulting Party"), then such Defaulting Party will pay the other Party (the "Innocent Party") a fee equal to [twelve (12) times] the gross monthly remuneration or consideration (in the event of contractors) paid by the Innocent Party to the person concerned. Such amount will be payable by the Defaulting Party within 30 (thirty) days of commencement of such person's appointment with the Defaulting Party.

22. DOMICILIUM CITANDI ET EXECUTANDI

The Parties hereto respectively choose as their *domicilium citandi et executandi* for all purposes of, and in connection with this Contract, the addresses stated in the Proposal.

23. NOTICES

23.1. Any notice to be given hereunder shall be given in writing and may be given either personally or may be sent by post, facsimile or email, shall be addressed to the relevant Party at its *domicilium* or to such other address as shall be notified in writing by any of the Parties to the other from time to time. Any notice given by post shall be deemed to have been received on the expiry of five (5) Business Days after same is posted by registered mail. Any notice delivered personally or transmitted per telefax, or by email shall be deemed to have been served at the time of delivery or dispatch.

- 23.2. Notwithstanding anything to the contrary herein contained, a written notice or communication (including email) actually received by a Party shall (provided that, in the case of a Party that is not a natural person, the notice or communication is actually received by a director or duly authorised representative (in the case of a company), member (in the case of a close corporation) or trustee (in the case of a trust)) be an adequate written notice or communication to it notwithstanding that it was not sent to or delivered at its chosen *domicilium citandi et executandi*.

24. SEVERABILITY

In the event that any one or more of the provisions of this Contract shall, for any reason, be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provisions of this Contract, but this Contract shall be construed as if such invalid, illegal or unenforceable provisions had never been contained herein, unless the deletion of such provision or provisions would result in the entire Contract being invalid, illegal or unenforceable.

25. TAX COMPLIANCE

- 25.1. The Client hereby undertakes in favour of the CSIR to maintain a Compliant Tax Status for the duration of this Contract.
- 25.2. The Client hereby undertakes to submit to the CSIR on or before each date on which the CSIR shall invoice the Client, proof of its Compliant Tax Status.
- 25.3. The CSIR hereby reserves the right, notwithstanding anything to the contrary contained in this Contract, to verify the Client's tax status from time to time. The Client, accordingly, hereby authorises the CSIR to verify its tax status on the central supplier database or on the SARS' tax compliance status system.
- 25.4. Accordingly, the Client shall provide the CSIR with an electronic access pin to the central supplier database and the SARS' tax compliance status system on the Signature Date, and on each subsequent date when such pin(s) is amended/updated during the term of this Contract.
- 25.5. The Parties hereby agree that any failure on the part of the Client to maintain a Compliant Tax Status at any time during the term of this Contract, shall constitute a material breach of this Contract, pursuant to which the CSIR shall be entitled to exercise its rights in terms of clause 17 (*Breach and Termination*).

26. VAT AND WITHHOLDING TAX

- 26.1. Unless stated otherwise in the Proposal or agreed to by the Parties, all fees and amounts stated in the Proposal are exclusive of Value Added Tax, which shall be paid by the Client upon submission of the relevant tax invoice.
- 26.2. Any withholding tax as levied by any foreign country shall, where applicable, be for the account of and payable by the Client.

27. ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

No data message (as defined in the Electronic Communications and Transactions Act No. 25 of 2002), including an e-mail, SMS, and recorded voice message, sent by a Party to the other Party, shall amend these contract conditions, or the rights and duties of the Parties in any manner, unless and until such data message is reduced to paper and signed by both Parties or their duly authorized signatories as an addendum hereto.

28. ENTIRE AGREEMENT

- 28.1. This document, together with the Proposal, contains the entire agreement between the Parties in regard to the subject matter thereof, and neither Party shall be bound by any undertaking, representation or warranty not recorded herein.
- 28.2. No alteration, variation, addition or agreed cancellation of this Contract shall be of any force or effect unless reduced in writing and signed by both Parties and their duly authorized signatories.

Acceptance Sheet

CSIR QUOTATION / PROPOSAL

OUR REF:

I, the undersigned *[Full names of Signatory]*, on behalf of Senegal's Department of Labour by my signature hereto, and in my capacity as Managing Director being duly authorized to do so, hereby accept, on behalf of the Department of Labour the CSIR's Project Quotation/Proposal No and all the CSIR's General Conditions of Contract contained in the attached Quotation/Project Proposal as binding on Department of Labour.

Signed at:

Date:

Signature:

For: Department of Labour

AS WITNESSES:

(1)

(2)

Signed at:

Date:

Signature:

For the CSIR, duly authorised

AS WITNESSES:

(1)

(2)

Please sign this page in full, initial each page of the quotation/project proposal and fax the signed copy to us. Please also return the signed original document to the address of the CSIR as specified in the accompanying Quotation/Proposal.



CSD REGISTRATION REPORT

SUPPLIER IDENTIFICATION

CSD cannot electronically verify the identity of a supplier other than a South African Individual / Sole Proprietor (through Home Affairs) or a company registered at the Companies and Intellectual Property Commission (CIPC). It is the responsibility of an organ of state supply chain practitioner to obtain supporting documentation to verify the identity and legitimacy of this supplier.

Supplier number	MAAA0014771	Have Bank Account	Yes
Is supplier active?	Yes	Total annual turnover	More than R50 million
Allow associates?	Yes	Financial year start date	01 Mar 2016 00:00:00:000
Supplier type	State Owned Entity	Created by	sharmse@csir.co.za
Supplier sub-type	PFMA Schedule 3B - National Government Business Enterprises	Created date	19 May 2016 15:39:45:000
Legal name	Council for Scientific and Industrial Research	Edit by	csd.reverifybatch@treasury.gov.za
Trading name	CSIR	Edit date	06 Sep 2024 11:19:09:153
Identification type	Organ Of State ID Number	Restricted Supplier	No
Government breakdown	Council for Scientific and Industrial Research	Restricted Director	No
Country of origin	South Africa	Government Employee	Yes

SUPPLIER INDUSTRY CLASSIFICATION INFORMATION

INDUSTRY CLASSIFICATION 1

Main group	Professional, scientific and technical activities	Core industry	Scientific research and development
Division	Scientific research and development	% share of annual turnover	100.00

SUPPLIER CONTACT INFORMATION

CONTACT 1

Contact type	Bid Office	Telephone number	012 841 2711
Is this your preferred Contact?	No	Cellphone number	082 467 6580
Name(s)	Rachel Kerina	Website address	www.csir.co.za
Surname	Chikwamba	Do you want this contact to also be a CSD user ?	No
Identification type	South African Identification Number	Created by	sharmse@csir.co.za
Prefer communication via email	Yes	Created date	14 Feb 2017 15:08:57:283





CSD REGISTRATION REPORT

Email address

rchikwamba@csir.co.za

Edit by

sharmse@csir.co.za

Edit date

26 Apr 2019 16:55:57:210

CONTACT 2

Contact type

Bid Office

Is this your preferred Contact?

No

Name(s)

Bronwen

Surname

Cadle de Ponte

Identification type

South African Identification Number

Prefer communication via cellphone

Yes

Prefer communication via email

Yes

Email address

bcadle@csir.co.za

Cellphone number

082 337 9867

Do you want this contact to also be a CSD user ?

Yes

Created by

sharmse@csir.co.za

Created date

03 Sep 2018 17:05:12:110

Edit by

sharmse@csir.co.za

Edit date

26 Apr 2019 16:55:57:223

CONTACT 3

Contact type

Finance

Is this your preferred Contact?

No

Name(s)

Nomcebo

Surname

Monama

Identification type

South African Identification Number

Prefer communication via email

Yes

Email address

nmonama1@csir.co.za

Telephone number

012 841 3335

Cellphone number

073 046 4674

Do you want this contact to also be a CSD user ?

Yes

Created by

sharmse@csir.co.za

Created date

03 Sep 2018 17:05:12:143

Edit by

jskosana2@csir.co.za

Edit date

16 Mar 2020 16:23:09:790

CONTACT 4

Contact type

Administration

Is this your preferred Contact?

No

Name(s)

John Mandla

Surname

Skosana

Identification type

South African Identification Number

Prefer communication via email

Yes

Email address

jskosana2@csir.co.za

Telephone number

012 841 3206

Cellphone number

071 175 5855

Website address

www.csir.co.za

Do you want this contact to also be a CSD user ?

No

Created by

sharmse@csir.co.za

Created date

26 Apr 2019 16:55:57:210

Edit by

sharmse@csir.co.za

Edit date

30 Aug 2023 11:04:16:143





CSD REGISTRATION REPORT

CONTACT 5

Contact type	Finance	Telephone number	012 841 4361
Is this your preferred Contact?	No	Cellphone number	083 388 4921
Name(s)	Margaret	Do you want this contact to also be a CSD user ?	Yes
Surname	Makaleng	Created by	sharmse@csir.co.za
Identification type	South African Identification Number	Created date	26 Apr 2019 17:03:52:780
Prefer communication via email	Yes	Edit by	csd.datafix@treasury.gov.za
Email address	debtors@csir.co.za	Edit date	26 Apr 2019 17:03:52:780

CONTACT 6

Contact type	Administration, Bid Office	Do you want this contact to also be a CSD user ?	Yes
Is this your preferred Contact?	Yes	Created by	welhelmna.modisakeng@treasury.gov.za
Name(s)	Tshegofatso	Created date	30 Aug 2023 11:04:16:050
Surname	Moremi	Edit by	tmoremi@csir.co.za
Identification type	South African Identification Number	Edit date	17 Oct 2023 09:03:45:757
Prefer communication via email	Yes		
Email address	tmoremi@csir.co.za		
Cellphone number	076 792 7494		

SUPPLIER ADDRESS INFORMATION

ADDRESS 1

Is this a preferred address?	Yes	Postal code	0169
Address line 1	Meiring Naude Road	Ward Number	46
Address line 2	Brummeria	Country	South Africa
Suburb	Brummeria	Created by	sharmse@csir.co.za
Province	Gauteng	Created date	19 May 2016 15:03:28:000
Municipality	City of Tshwane	Edit by	tmoremi@csir.co.za
City	Pretoria	Edit date	05 Sep 2024 10:43:30:677

ADDRESS 2

Is this a preferred address?	No	Postal code	0001
------------------------------	----	-------------	------





CSD REGISTRATION REPORT

Address line 1	PO Box 395	Ward Number	3 - [Removed]
Address line 2	Pretoria	Country	South Africa
Suburb	Pretoria SP - [Removed]	Created by	sharmse@csir.co.za
Province	Gauteng	Created date	19 May 2016 15:39:29:000
Municipality	City of Tshwane	Edit by	sharmse@csir.co.za
City	Pretoria	Edit date	19 May 2016 15:39:45:137

SUPPLIER BANK ACCOUNT

The "Bank Verification Status" field indicates that the bank account details submitted by the supplier exist at the bank and that the bank account details are valid. However, as this supplier does not have an identifying number (like a South African ID number, or Company Registration number, or NPO number or Trust number) linked to their bank account details at their respective bank, the CSD system cannot electronically verify that the bank account belongs to the specific supplier. The supply chain practitioner is therefore responsible to obtain supporting documentation to verify that this bank account belongs to this supplier.

BANK ACCOUNT 1

Account type	Current Accounts	Created by	sharmse@csir.co.za
Bank	ABSA BANK LIMITED	Created date	10 Jun 2016 10:16:24:000
Branch number	632005	Edit by	csd.safetynetbatch@treasury.gov.za
Branch name	ABSA ELECTRONIC SETTLEMENT CNT	Edit date	15 Jun 2016 16:12:50:307
Account number	540002258	Bank Verification Status	Verification Succeeded
Account holder	CSIR	Foreign Bank Account	No
Is this a preferred account?	Yes	Is the identifier linked at the bank	No
Active start date	19 May 2016 15:07:07:000	Is this a Shared Funding Account	No

TAX INFORMATION

The "Overall Tax Status" field indicates the compliance status of the tax information submitted. However, as this supplier does not have an identifying number (like a South African ID number, or Company Registration number, or NPO number or Trust number) linked to their tax details at SARS, the CSD system cannot electronically verify that the tax reference numbers belongs to the specific supplier. The supply chain practitioner is therefore responsible to obtain supporting documentation to verify that the tax reference numbers belongs to this supplier.

VAT number	4470114283	Overall Tax Status	Tax Compliant
Is this supplier a VAT vendor?	Yes	Created by	sharmse@csir.co.za
PAYE number	7170713160	Created date	19 May 2016 15:39:45:000
Are you Registered with SARS?	Yes	Edit by	csd.reverifybatch@treasury.gov.za
Last validation date	19 Mar 2025 09:46:00:000	Edit date	18 Jul 2024 11:42:21:000
Would you like to receive notifications?	Yes		





CSD REGISTRATION REPORT

B-BBEE INFORMATION

B-BBEE verification regulator	Verification agency accredited by SANAS	SANAS accredited agency	Moore Stephens BW BEE Verification (Pty) Ltd
Sector charter	Other	% Owned by black people	0.00
Subsector charter	NOT APPLICABLE	% Owned by black people who are women	0.00
B-BBEE certificate number	MS-5835-0824-06	% Owned by black people who are youth	0.00
B-BBEE certificate issue date	15 Aug 2024 00:00:00:000	% Owned by black people with disabilities	0.00
B-BBEE certificate issue expiry date	14 Aug 2025 00:00:00:000	% Owned by black who are unemployed	0.00
Value adding supplier or empowering supplier	No	% Owned by black people living in rural or underdeveloped areas	0.00
Verification Status	Manual Verification Required		
Skills Development Score	27.39	Created by	sharmse@csir.co.za
Socio-Economic Development Score	5.00	Created date	14 Jun 2016 11:26:10:293
Management Control Score	15.65	Edit by	tmoremi@csir.co.za
Enterprise Supplier Development Score	46.99	Edit date	05 Sep 2024 10:43:31:007
Total Score	95.03	Status	Active

DIRECTORS / MEMBERS / OWNERS INFORMATION

DIRECTOR/MEMBER 1

Director type	Chief Executive Officer	Edit by	sharmse@csir.co.za
Director status	Active	Edit date	14 Feb 2017 15:02:24:000
Name(s)	Thulani Humphrey	Restricted Director	No
Surname	Dlamini	Restriction Last Verification Date	19 Mar 2025 09:47:02:007
Country	South Africa	Government Employee	No
Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:10:737
South African identification number	7002155463085	SA identification number Verified	Yes
Appointment date	01 Feb 2017 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:17:780
Owner	No	Ownership verification status	Manual Verification Required





CSD REGISTRATION REPORT

Created by	sharmse@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	14 Feb 2017 15:02:24:000		

DIRECTOR/MEMBER

2

Director type	Non Executive Director	Edit by	sharmse@csir.co.za
Director status	Active	Edit date	23 Jan 2019 11:41:14:000
Name(s)	CHRISTINE LOUISE	Restricted Director	No
Surname	RENDER	Restriction Last Verification Date	19 Mar 2025 09:47:02:020
Country	South Africa	Government Employee	No
Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:10:847
South African identification number	5705210200183	SA identification number Verified	Yes
Appointment date	01 Jan 2019 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:27:097
Owner	No	Ownership verification status	Manual Verification Required
Created by	sharmse@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	23 Jan 2019 11:41:14:000	Companies involved in	MAAA1577617;

DIRECTOR/MEMBER

3

Director type	Non Executive Director	Edit by	sharmse@csir.co.za
Director status	Active	Edit date	23 Jan 2019 11:42:25:000
Name(s)	VUYO LINDELWE	Restricted Director	No
Surname	MTHETHWA	Restriction Last Verification Date	19 Mar 2025 09:47:02:020
Country	South Africa	Government Employee	No
Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:11:003
South African identification number	6808160410080	SA identification number Verified	Yes
Appointment date	01 Jan 2019 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:30:017
Owner	No	Ownership verification status	Manual Verification Required
Created by	sharmse@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	23 Jan 2019 11:42:25:000		

DIRECTOR/MEMBER

4





CSD REGISTRATION REPORT

Director type	Non Executive Director	Edit by	tmoremi@csir.co.za
Director status	Active	Edit date	30 Aug 2023 16:39:44:000
Name(s)	ARNOLD	Restricted Director	No
Surname	VAN ZYL	Restriction Last Verification Date	19 Mar 2025 09:47:02:020
Country	South Africa	Government Employee	No
Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:11:143
South African identification number	5904015051087	SA identification number Verified	Yes
Appointment date	01 Jan 2023 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:31:543
Owner	No	Ownership verification status	Manual Verification Required
Created by	jskosana2@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	08 Feb 2023 09:10:44:000		

DIRECTOR/MEMBER 5

Director type	Non Executive Director	Edit by	jskosana2@csir.co.za
Director status	Active	Edit date	08 Feb 2023 09:14:44:000
Name(s)	MALEKE JOEL	Restricted Director	No
Surname	MATOLONG	Restriction Last Verification Date	19 Mar 2025 09:47:02:037
Country	South Africa	Government Employee	Yes
Identification type	South African Identification Number	Department	Rustenburg - NW Local Municipality;
South African identification number	7812125423088	Government Employee Last Verification Date	19 Mar 2025 09:46:11:317
Appointment date	08 Feb 2023 00:00:00:000	SA identification number Verified	Yes
Owner	No	SA identification number verification date	19 Mar 2025 09:46:38:653
Created by	jskosana2@csir.co.za	Ownership verification status	Manual Verification Required
Created date	08 Feb 2023 09:12:53:000	Ownership last verification date	01 Jan 1900 00:00:00:000

DIRECTOR/MEMBER 6

Director type	Chairman of the Board,Non Executive Director	Edit by	tmoremi@csir.co.za
Director status	Active	Edit date	30 Aug 2023 16:40:36:000
Name(s)	VUYANI	Restricted Director	No
Surname	JARANA	Restriction Last Verification Date	19 Mar 2025 09:47:02:053
Country	South Africa	Government Employee	No





CSD REGISTRATION REPORT

Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:11:490
South African identification number	7011265045088	SA identification number Verified	Yes
Appointment date	27 Jul 2023 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:47:250
Owner	No	Ownership verification status	Manual Verification Required
Created by	jskosana2@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	08 Feb 2023 09:15:39:000	Companies involved in	MAAA0463007; MAAA0510871; MAAA0559706; MAAA1002213; MAAA1003057; MAAA1049024...

DIRECTOR/MEMBER 7

Director type	Non Executive Director	Edit by	jskosana2@csir.co.za
Director status	Active	Edit date	08 Feb 2023 09:19:01:000
Name(s)	YUNUS	Restricted Director	No
Surname	BALLIM	Restriction Last Verification Date	19 Mar 2025 09:47:02:053
Country	South Africa	Government Employee	No
Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:11:630
South African identification number	5612315056082	SA identification number Verified	Yes
Appointment date	01 Jan 2023 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:55:747
Owner	No	Ownership verification status	Manual Verification Required
Created by	jskosana2@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	08 Feb 2023 09:19:01:000	Companies involved in	MAAA0663783;

DIRECTOR/MEMBER 8

Director type	Non Executive Director	Edit by	jskosana2@csir.co.za
Director status	Active	Edit date	08 Feb 2023 09:22:15:000
Name(s)	MAHESH	Restricted Director	No
Surname	FAKIR	Restriction Last Verification Date	19 Mar 2025 09:47:02:067
Country	South Africa	Government Employee	Yes
Identification type	South African Identification Number	Department	National:National Treasury;
South African identification number	6108145118084	Government Employee Last Verification Date	19 Mar 2025 09:46:11:740
Appointment date	01 Jan 2023 00:00:00:000	SA identification number Verified	Yes





CSD REGISTRATION REPORT

Owner	No	SA identification number verification date	19 Mar 2025 09:46:56:687
Created by	jskosana2@csir.co.za	Ownership verification status	Manual Verification Required
Created date	08 Feb 2023 09:22:15:000	Ownership last verification date	01 Jan 1900 00:00:00:000
		Companies involved in	MAAA0393349; MAAA0393366; MAAA0579387;

DIRECTOR/MEMBER

9

Director type	Non Executive Director	Edit by	jskosana2@csir.co.za
Director status	Active	Edit date	08 Feb 2023 09:23:19:000
Name(s)	MICHELLE	Restricted Director	No
Surname	GOVENDER	Restriction Last Verification Date	19 Mar 2025 09:47:02:067
Country	South Africa	Government Employee	No
Identification type	South African Identification Number	Government Employee Last Verification Date	19 Mar 2025 09:46:11:833
South African identification number	8605290152089	SA identification number Verified	Yes
Appointment date	01 Jan 2023 00:00:00:000	SA identification number verification date	19 Mar 2025 09:46:57:673
Owner	No	Ownership verification status	Manual Verification Required
Created by	jskosana2@csir.co.za	Ownership last verification date	01 Jan 1900 00:00:00:000
Created date	08 Feb 2023 09:23:19:000		

DIRECTOR/MEMBER

10

Director type	Non Executive Director	Created date	08 Feb 2023 09:25:09:000
Director status	Active	Edit by	jskosana2@csir.co.za
Name(s)	JULIET KAY	Edit date	08 Feb 2023 09:25:09:000
Surname	NEWTON	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	19 Mar 2025 09:47:02:067
Identification type	South African Identification Number	Government Employee	No
South African identification number	6712240115083	Government Employee Last Verification Date	19 Mar 2025 09:46:11:913
Appointment date	01 Jan 2023 00:00:00:000	SA identification number Verified	Yes
Owner	No	SA identification number verification date	19 Mar 2025 09:46:58:313
Created by	jskosana2@csir.co.za	Ownership verification status	Manual Verification Required
		Ownership last verification date	01 Jan 1900 00:00:00:000





CSD REGISTRATION REPORT

DIRECTOR/MEMBER 11

Director type	Non Executive Director	Created date	30 Aug 2023 16:36:44:000
Director status	Active	Edit by	tmoremi@csir.co.za
Name(s)	MICHAEL EUGENE	Edit date	30 Aug 2023 16:36:44:000
Surname	MULCAHY	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	19 Mar 2025 09:47:02:083
Identification type	South African Identification Number	Government Employee	No
South African identification number	8308185183083	Government Employee Last Verification Date	19 Mar 2025 09:46:12:053
Appointment date	27 Jul 2023 00:00:00:000	SA identification number Verified	Yes
Owner	No	SA identification number verification date	19 Mar 2025 09:46:58:737
Created by	tmoremi@csir.co.za	Ownership verification status	Manual Verification Required
		Ownership last verification date	01 Jan 1900 00:00:00:000
		Companies involved in	MAAA0156588;

Tips and Frequently Asked Questions (FAQ)





CSD REGISTRATION REPORT

Identifier

CSD cannot electronically verify the identity of a supplier other than a South African Individual / Sole Proprietor (through Home Affairs) or a company registered at the Companies and Intellectual Property Commission (CIPC). For this reason, a disclaimer is displayed for supply chain practitioners to obtain supporting documentation to verify the identity and legitimacy of a supplier in these cases.

Bank

For help on how to resolve bank failures click here: [I received an email stating the bank information I captured on the CSD was sent for bank account validation and could not be validated. The response received from the bank contains an error message.](#)

The various possible error messages received from the bank are highSemiBolded in red. Search for the applicable message and follow the detailed steps associated with that error message.

Tax

Tax Compliance Status

For help on how to deal with tax status differences between CSD and the tax clearance certificate click here: [What should a supplier do if the tax status on CSD difference from the tax clearance certificate?](#)

Tax Compliance Expiry Date

For help on how to deal with tax status differences between CSD and the tax clearance certificate click here: [How does CSD determine the tax compliance expiry date?](#)

CIPC

Should the director/member information reflected on the CIPC registration report differs to that reflected on CSD for help click here: [The active Directors/Members are not being populated on the CSD Directors/Members screen as they appear at CIPC, how can I rectify this?](#)

State Employee

For more information pertaining to government employment status click here: [Will there be verification done to identify if a supplier is a government employee?](#)

BBBEE

CSD does not automatically verify all certificate information with the various accreditation bodies. Organs of State are required, where not automatically verified by CSD, to manually verify this information with the applicable accreditation body as per current policies and procedures. Expired certificate information do not reflect on the report.

RESTRICTION

Restricted Supplier - A supplier is restricted by using the identification number of the entity e.g. CIPC registration -, trust -, Social Development non-profit -, South African ID -, Foreign company registration number or ID number. If there is more than one CSD Supplier profile registered on CSD with the same entity identification number, all those related supplier profiles will be restricted.

Restricted Director - A director/owner is an individual person and is restricted by using the South African ID or Foreign ID number. If a director belongs to different companies and has been restricted, the director will reflect as restricted in all companies where identification number is detected.

Restricted Suppliers & Directors are listed on CSD under Help - [Am I restricted?](#)

The CSD does not automatically verify foreign company registration number, international securities identification number, foreign identification numbers, foreign passport numbers, work permit numbers, foreign bank accounts, B-BBEE, demographic and accreditation information. Organs of State are required to manually verify this information with the applicable verification institutions as per their current policies and procedures.





CENTRAL SUPPLIER
DATABASE
FOR GOVERNMENT

Report Date:

19 Mar 2025 09:47:47.861 AM

Report Ran By:

bellah.gelebe@labour.gov.za

CSD REGISTRATION REPORT

Print Date:

3/19/2025 9:47:47 AM



national treasury

Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

DECLARATION OF INTEREST BY USERS

1. Any legal person, including persons employed by the principal, or persons having a kinship with persons employed by the principal, including a blood relationship, may make an offer or offers in terms of this invitation to bid. In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons employed by the principal, or to persons connected with or related to them, it is required that the bidder or his/her authorised representative declare his/her position in relation to the evaluating/adjudicating authority and/or take an oath declaring his/her interest, where-

- the bidder is employed by the principal; and/or
- the legal person on whose behalf the bidding document is signed, has a relationship with persons/a person who are/is involved in the evaluation and or adjudication of the bid(s), or where it is known that such a relationship exists between the person or persons for or on whose behalf the declarant acts and persons who are involved with the evaluation and or adjudication of the bid.

2. In order to give effect to the above, the following questionnaire must be completed before evaluation of the bid:

- 2.1 Are you or any person you know, connected with the any of the bidders?

YES/NO

- 2.1.2 If so, state particulars.

- 2.2 Do you, or any person connected with any of the bidders, have any relationship (family, friend, other) with a person employed by the principal and who may be involved with the evaluation and or adjudication of this bid?

YES/NO

- 2.2.1 If so, state particulars.

2/.....

- 2.3 Are you, or any person connected with any of the bidders, aware of any relationship (family, friend, other) between the bidder and any person employed by the principal who may be involved with the evaluation and or adjudication of this bid?

YES/NO

- 2.3.1 If so, state particulars.

.....
.....
.....
.....

DECLARATION

I, THE UNDERSIGNED (NAME).....RUDZANI NDOU.....

CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 2.1 TO 2.3.1 ABOVE IS CORRECT.
I ACCEPT THAT THE PRINCIPAL MAY ACT AGAINST ME IN TERMS OF PARAGRAPH 23 OF THE
GENERAL CONDITIONS OF CONTRACT SHOULD THIS DECLARATION PROVE TO BE FALSE.

.....
Signature

14/03/2025
Date

SP
Position

RUDZANI NDOU
Name of person

STANDARD DBAC SUBMISSION CHECKLIST – To be fully completed the User upon submission

Description of Request to DBAC	APPOINTMENT OF CSIR TO CONDUCT FORENSIC INVESTIGATION	
RFQ / Tender number		
Declaration by Chief of submission	-User on day of submission	I confirm that this checklist represents the true contents of this DBAC request and that I have thoroughly checked all calculations and attached all relevant supporting documentation: <u>Rudzani NDOU</u> [User name & signature] Date: <u>14/03/2025</u> Extension: <u>4728</u>

PLEASE NOTE ALL ITEMS MUST BE TAGGED		USER	SCM
		YES / NO or N/A	YES/ NO or N/A
1	Submission to DBAC by Chief-User : signed	Yes	Yes
2	Allocations signed off	Yes	Yes
3	Completed Demand Management Evaluation	N/A	N/A
4	iQual / manual Evaluation Report	N/A	N/A
5	Detailed and valid quotation	Yes	Yes
6	15% VAT indicated on quotation	Yes	Yes
7	Sole supplier letter (if applicable)	N/A	N/A
8	DG approval, National Treasury Approval (External Venues / Deviations) if applicable	Yes	Yes
9	Disposal Board Letter (if applicable) –Procurement of Furniture	N/A	N/A
10	HRD Training document (if applicable)	N/A	N/A
11	RFQ / Invitation to quote	N/A	N/A
12	SBD 4 (Company completed)	N/A	N/A
13	SBD 6.2 (if applicable) as per sector	N/A	N/A
14	Valid TCC / Pin	N/A	N/A
15	SANAS BBBEE certificate or an affidavit	N/A	N/A
16	CSD Compliance Status Report	N/A	N/A
17	Approved Specification / TORs	N/A	N/A
18	BSC Request to go out to Tender – Signed	N/A	N/A
19	BSC Minutes - Signed	N/A	N/A
20	BSC Attendance Register	N/A	N/A
21	Appointment letters of Bid Spec	N/A	N/A
22	Procurement Plan – Highlighted	N/A	N/A
23	BAS Report – Highlighted	N/A	N/A
24	User SBD 4	Yes	Yes
25	RT/ Transversal Contract	N/A	N/A
26	DBAC Approval Captured on DBAC register		
27	Approval Letter issued		
28	Award captured on contract register (NT website) if applicable		
29	Deviation report to National Treasury		