PART A REQUEST FOR INFORMATION(RFI)			
Description of the works/goods/services	**Determine technology options available in the market to enable the Cyber Forensic lab capability to do Cyber/Digital Forensics, as well as associated indicative costing, timelines, processes, training and professional services. The technology modules need to include cloud ready interfaces of technologies that is positioned off premises as well.**		
Deadline for submission	**09 June 2022**	**At (South African Standard Time)**	**10:00am**
Tender Office address	**Eskom Megawatt Park Tender Office Northside No 1 Maxwell Drive Sunninghill**		

Eskom Holdings SOC Ltd ("Eskom") invites you to respond to a Request for information (RFI) for Cyber Forensic lab capability that will enable it to do Cyber/Digital Forensics intelligence analytics in support of investigations.

This RFI is a stand-alone information-gathering and market-testing exercise, intended only to inform and assist Eskom's further deliberation and development of a strategy for the Market Price analysis. Please supply indicative pricing and/or pricing structure(s).
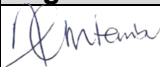
Respondents are required to provide documentation detailing their different offerings especially around functionality, processes, pricing training, professional services, technology, and indicative prices in order to assist Eskom. The technology modules need to include cloud ready interfaces of technologies that is positioned off premises as well.

Only Suppliers who responded and shown ability to offer the required services or an alternative solution with equivalent functionality will be invited to respond to the enquiry process that will follow this request unless otherwise approved in the strategy.

Eskom has delegated the responsibility for this **RFI** to the signatory of this document, whose details can be found below.

We look forward to receipt of your response.

Yours faithfully

Name	Designation	Signature	Date
Nothukela Sereo	**Procurement Manager**	*[signature]*	12 May 2022

File name: Request for Information (RFI)_Cyber _Final

PART B **REQUEST FOR INFORMATION** **To be completed by the supplier**			
To	Eskom Holdings SOC Ltd	**Date**	
Attention			
Tel no		**Fax no and /or e-mail address**	
From		**Address**	
Address			
Sender			
Description of the works/goods/services	**Determine technology options available in the market to enable the Cyber Forensic lab capability to do Cyber/Digital Forensics, as well as associated indicative costing, timelines, processes, training and professional services. The technology modules need to include cloud ready interfaces of technologies that is positioned off premises as well.**		

Please find below our response to Eskom's questions:

No.	Question	Please indicate your response in this column
1.	**Your name and contact details**	
2.	**Company registration number**	
3.	**Brief description of previous experience and Description of the solution that you can offer**	
4.	**Indicative prices (Only for use of RFI)**	
5.	**B-BBEE Status**	
6.	**Central Supplier Database (CSD number)**	

Yours faithfully

Name	Designation	Signature	Date
Telephone number		**Fax and/or e-mail address**	

File name: Request for Information (RFI)_Cyber _Final

PART C

1. INTRODUCTION

Eskom Holdings SOC Limited ("Eskom") – Request information for the Cyber Forensic lab capability that will enable it to do Cyber/Digital Forensics intelligence analytics in support of investigations

2. BACKGROUND INFORMATION

Eskom has an increase of internal and external investigations that requires digital forensics analysis. The External Investigation teams include a range of Government Department (i.e. SIU, SAPS, NPA). The Investigations require that the Chain of Custody digital processes is compliant with the regulatory and legal guidelines so that the Information is appropriately processed and secured and needs to stand in Court of Law.

The absence of a Cyber Forensics capability within Eskom, result in the following security challenges:

- Lack of a Cyber Forensics deep analytics platform (LABRATORY) to support Investigations of Fraud and Cyber- Crime incidents at enterprise level.

- Non-compliance to governance controls and compliance standards related to Eskom Enterprise wide digital investigations.

- In-time decision-making support, due to the lack of an automated Cyber Forensics acquisition of Fraud and Crime data to support the Cyber Forensics intelligence lifecycle.

- Secure Threat Intelligence and Cyber Forensics capability over the medium to long-term in support of Eskom's Counter Fraud and Counter Cyber-crime investigations operations.

3. SCOPE OF WORK/BUSINESS REQUIREMENT

The request for information is for advance Cyber Forensics LAB and intelligence analytics capability as a medium term (x5 years) Operational capability to assist Audit and Fraud Investigations for Eskom. The response to this request for information must include training, professional services, processes, technology, and budget cost indication. The technology modules need to include cloud ready interfaces of technologies that is positioned off premises as well.

The industry needs to enable Eskom to establish a cyber-forensic lab on premise - in-house, capability, which can assist with deep digital forensic analyses, response and investigations.

Confidential

File name: Request for Information (RFI)_Cyber _Final

This Cyber Forensics LAB capability must consist of the following summarized scope:

- Deception cyber forensic solution.
- Advanced Digital Forensic Intelligence Analysis solution.
- Cyber forensic workbench system solution (Hardware)

3.1. Deception Cyber Forensics capability solution:

- **New Deception Triangle Technology module:**

  - Decoys: Manually configure decoys and control user definition.
  - Breadcrumbs: Add application breadcrumbs, control network deception settings, and add/deploy Active Directory in deception component.
  - Data deception: Perform data deception tasks including addition of Real OS image file, control file system spoofing and settings for decoys requiring TLS services.

- **Deception Coverage:**

  The Deception menu option in the GUI includes a line that indicates the amount of Deception Coverage in your system. Users can hover over the menu option to see suggestions about how to increase coverage

- **Deception Activity:**

  This new feature is available at the DETECTIONS menu and enables users to view information from the Decoys via Conclusions, Alerts, Credentials Access, and uploaded files.

- **New Alert Type:**

  Deception User: This alert type is generated. It is triggered based on monitoring the activity of Deception users on the Active Directory server.

- **Training/Skills development:**

  Solution provider to provide intermediate advanced training related to deception technology. Solution provider to indicate the availability of training local in South Africa or international.

- **Active Directory Deception:**

  Analysis solution: Deception module for Active Directory includes defining faked user credentials in Active Directory, binding these faked users to Decoys, and periodically have these Decoys access the Active Directory. Attackers can use these fake users to access decoys and to access other assets in the organization.

Confidential

File name: Request for Information (RFI)_Cyber _Final

3.2. Advanced Digital Forensic Intelligence Analysis:

Forensically Sound: Digital Forensics Intelligence Analysis solution	
Forensically defensible collections module.	Comprehensive file collection logging and reporting records file hash values, access date attributes, file ownership and other metadata. Over a dozen other log files track the list of intentionally ignored files, and any warnings or errors, etc. These logs provide a forensically defensible collection process.
Preserve collected data within tamper-proof, encrypted File Safe logical evidence files module	Collected files can be saved within a read-only "File Safe" file. A File Safe is an evidence file container that protects the data and the metadata. A File Safe can be validated or verified using a tool (provided) at any time post-collection. The solution provider to the meet FIPS140 standard
Digital Forensic data sanitizer module.	The solution provider to the meet DoD 5220.22-M standard

Advanced Digital Forensics Collection Features	
Targeted file collection, including full-text search	Collect only what you need. Powerful file selection features allow the collection of only relevant data. Full-text search is supported for hundreds of common file formats. Exclude duplicate files or known non-data files from collection, massively reducing the workload of subsequent processing and review.
Flexible selection of collection targets	Select computers to collect from based on computer name or type, operating system, custom label, custodian/user or group.
Collect open files from Windows computers	ECC can collect open from any local drive using the Microsoft Volume Shadow Copy Service
Collect volatile system information	From each selected endpoint computer, collect a list if running processes, open handles, screenshots of running applications, RAM images, and network packets.

File name: Request for Information (RFI)_Cyber _Final

Collect deleted files	Deleted files, unallocated clusters, and the MFT / FAT file allocation tables can be collected from Windows endpoint computers having NTFS or FAT-formatted volumes.
Biometric analysis	Solution provider may be able to conduct forensic on digital forensics i.e., fingerprint, facial recognition, and social media, smart identity card systems analysis (standard CAC201)

COLLECT ACTIVE DATA SETS OF ANY SIZE OR COMPLEXITY

Manage data collections and relocations from any number of connected and remote devices, including laptops, desktops, enterprise file shares, and Microsoft SharePoint sites.

EXCLUDE IRRELEVANT DATA

Preview the target file system across the network; pre-filter collections by document type, content, custodian, and timeframe; and collect only what you need for processing, analysis, and production. You can add data to the collection iteratively as the matter or investigation evolves.

Optional Functions

Forensically defensible collections. Collect data from an unlimited number of devices across the enterprise, including devices running Windows, macOS, and popular Linux distributions. Don't miss deleted files from NTFS and FAT file systems, preserve metadata that may have been modified by malware, and preserve the chain of custody by creating strongly encrypted File Safe logical evidence files, E01, or dd, forensic and disk images.

Search every endpoint. Search for specific keywords or regular expressions to find and collect responsive files across every endpoint in your enterprise and within thousands of file types. Use out-of-the-box common searches for credit card numbers, bank accounts, IP addresses, and more to find and delete personally identifiable information and other sensitive or valuable data.

Targeted collection. Reduce internal costs and resource strain by collecting only the data you need. Preview the target file system across the network and select the volumes, folders, or files to collect. Pre-filter data by document type, content, timeframe, and custodian to reduce the volume of data fed into processing, analysis, production, and review workflows.

Streamlined, enterprise targeted collection process. Collection can be a time-intensive process, but it doesn't have to be. With the Collection Center, you can automate repetitive tasks with email alerts, reports, and logs about the state of collections. Avoid collection failures due to network dropouts, with fault tolerance and the ability to resume incomplete file collections, disk image collections and relocations. You can also schedule recurring collections and multi-job sequences, remotely execute commands on target computers, and securely move or copy files between devices, all depending on the needs of your current task.

Confidential

File name: Request for Information (RFI)_Cyber _Final

On-Premises Primary LAB infrastructure:

• High Level Concept Architecture (HLCA) 3 TIER Solution design layout for lab.

• Hardware Infrastructure Analysis Options for lab 10GB network fibre baseline.

• Mini 20TB NAS storage modular options for lab.

• Add Complementary virtualization and/or cloud interfaces for threat intelligence feeds if so required or Operation system patches and version updates

• 4 Seat Cyber Forensics Workbench system

• High Level Concept Architecture (HLCA) 3 TIER Solution design layout for lab.

• Hardware Infrastructure Analysis Options for lab 10GB network fibre baseline.

• Mini 20TB NAS storage modular options for lab.

• Add Complementary virtualization and/or cloud interfaces for threat intelligence feeds if so required or Operation system patches and version updates.

Training/Transfer of skills: Solution provider to provide intermediate to advanced training related to advanced deep forensic analytics technology. Solution provider to indicate the availability of training local in South Africa or international

Basics skills required for Digital Investigation in a Cyber Forensics Lab domain + Training for 5 people to manage on premise Cyber Forensics Lab

Software Related Requests:

- Year 1 advance analytics system that consists of hardware and software licences. This includes end-user LAB software or server licenses for five Investigators.

- Year 2-Year 5 for the support and maintenance of the delivered solution

- Professional services for year 1 - 5.

  * The solution provider to indicate the implementation and operationalisation timeframe for the solution.

Hardware Requirements:

Cyber Forensics Workbench system to be provided as per Eskom's requirements.
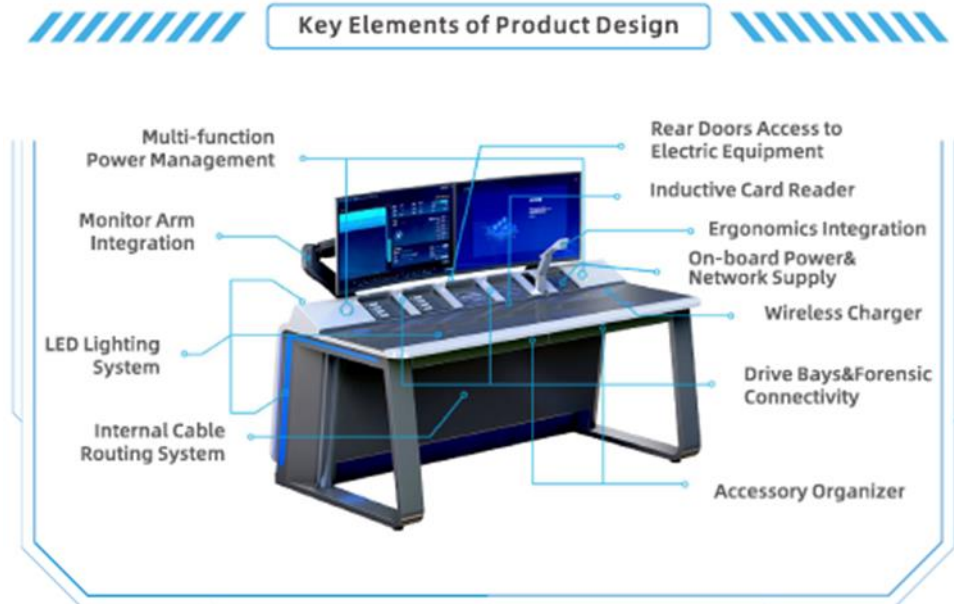Below is just an example of a workbench.

File name: Request for Information (RFI)_Cyber _Final

Functional Criteria:

A. The Solution providers that respond to this RFI need to advise on their ability to enable the Cyber Forensics LAB on the following requirements and need to assist Eskom by including responses to the following information as part of their response.

REQUIREMENTS QUESTIONAIR	RESPONSE
The capacity scope is to process about 2000 investigations per year. The solution providers must indicate that the solution can support and implement the as per the requirements.	If Yes, and substantiate
The solution provider needs to indicate any international certification or accreditation and affiliation with International Cyber and/or Digital Forensics forums and institutions.	If yes, provide relevant , certification and or accreditations on the institutions.
The solution provider needs to indicate successful previous deployment for Cyber Forensics LAB capabilities	If Yes, provide relevant experience and size of deployments.
Do you have a technology footprint or vendor presence in South – Africa?	If yes, provide vendor information.
Is the Solution provider registered with RSA or is the solution provider an International registered company.	Provide company national or international footprint.
The solution provider needs to provide a High-Level Concept Architecture (HLCA) design explaining how the system will align with the	Provide high level conceptual architecture information

Confidential

File name: Request for Information (RFI)_Cyber _Final

functional requirements indicated in this document	
The solution provider needs to indicate the time to implement and the estimated cost to setup and enable an Operational ready Cyber Forensics LAB solution. This needs to include type of professional services needed to operationalise the system.	If yes, provide project plan, cost.
The solution provider needs to indicate the certification training and skills transfer options.	If yes, provide training curriculum, cost and type of skills transfer.
The solution provider needs to provide indicative pricing for the technology modules, professional services and support & maintenance.	If yes, provide cost breakdown. asper the Indicative Cost table below.

B. TECHNICAL CRITERIA

Serial Number	Question	Slighlty Aligned 0%-3%	Partialy Aligned 3.1%-6%	Fully Aligned 6.1%-8.33%	% 100%
	(Example: Indicate with X)			x	8.33%
1	Indicate that the solution for the Datacentre HW appliances intergration comply with Eskom DC standards for fibre needs to be 10 Gbps capacity				8.33%
2	Indicate if technology solution is cloud ready.				8.33%
3	Indicate that the solution technology have a deception response module that is fully intigrated to the LAB.				8.33%
4	Indicate that the solution technology can conduct deep social media analysis.				8.33%
5	Indicate that the solution technology can deploy software agent on stealth mode for active investigation to endpoints.				8.33%
6	Indicate that the technology platform is able to integrate in Eskom SIEM, SOAR, XDR technology.				8.33%
7	Indicate that the solution technology is able to analysis Microsoft and Linux favours operating systems.				8.33%
8	Is the technology to be able to integrate and cloud based O365/Azure technology.				8.33%
9	Is the technology able to analyse all e-mail technology formats				8.33%
10	Is the technology to be able to do Object relationship maps and this include geo graphical location indications				8.33%
11	Is the solution provider able to Integrate all systems to Physical Lab Test Office bench				8.33%
12	Indicate costing module for the technology solution modules,training and professional services.				8.33%

Service Level Agreement requirements
The indication of a support and maintenance framework is necessary.

File name: Request for Information (RFI)_Cyber _Final

4. INDICATIVE COST

Scope	Unit Price	QTY	Y1	Y2	Y3	Y4	Y5
Hardware A- System Hardware		**2**					
B - Work Bench		**2**					
A- Analyst Software		**5**					
B- Endpoint Software		**2000**					
C- Database		**2**					
Maintenance and Support - HW		**Y1-Y5**					
Maintenance and Support - SW		**Y1-Y5**					
Professional Services		**200 hours**					
Training(5 Employees)		**** See Note Below***					

* Supplier to indicate training schedule in accordance to the required technology.

File name: Request for Information (RFI)_Cyber _Final

5. SUBMISSION GUIDELINES

To ensure the receipt of communication with regard to this request for information process, kindly complete Appendix A – Acknowledgement Form and return it by email as indicated on the form within 3 days of receiving this Invitation.

6. METHOD OF DELIVERY

The RFI submissions must be sealed and delivered at the Tender Office Box located at the following address:

Eskom Holdings SOC Limited,
Megawatt Park, North side
1 Maxwell Drive, Sunninghill
Johannesburg, 2000

All submission responses must be clearly marked as follows:
- Offer Confidential Enquiry Reference no: MWP1364CX
- Closing date: 09 June 2022
- Closing time: 10h00 AM South African Standard Time.

NB: **PLEASE NOTE: THE TENDER BOX WILL ONLY BE AVAILABLE FROM 6:00 TO 18:00 (MONDAY TO FRIDAY)**

7. HANDLING OF CORRESPONDENCE AND DOCUMENTS

The submission may not be addressed to any Eskom Holdings employee, nor may any Eskom employee deposit a tender in the tender box on behalf of a respondent, except one lodged by courier.

Eskom Holdings does not take responsibility for tenders delivered to any other site than the Tender Office as specified in the above. Any tender which is not delivered as above will be deemed a late tender.

You are urged to ensure that all issues in your submission are sufficiently clear and all documentation completed and incorporated in your submission at the time of submission. Non-adherence to this will prejudice and may disqualify your offer from further consideration.

Your RFI submission should have a thorough index and reference all documentation submitted. RFI documentation should be neatly filed / bound.

File name: Request for Information (RFI)_Cyber _Final

FORMAT OF SUBMISSION

EACH RFI SHALL BE SUPPLIED IN PRINTED AND IN ELECTRONIC FORMAT. ALL PRINTED AND ELECTRONIC COPIES OF EACH SUBMISSION SHALL BE IDENTICAL TO THE ORIGINAL SUBMISSION IDENTIFIED AS FOLLOWS:

- **1 X ORIGINAL RFI**
- **1 X COPY RFI AND**
- **1 X COPY RFI – ELECTRONIC COPY (MEMORY STICK)**

QUERIES AND QUESTIONS

No questions, during the RFI period will be answered telephonically.
Questions must be submitted in writing, either via e-mail to:
Attention: Tamara Mda
E-mail MdaT@eskom.co.za

REQUEST FOR INFORMATION AS FOLLOWS:

- **Determine technology options available in the market to enable the Cyber Forensic lab capability to do Cyber/Digital Forensics, as well as associated indicative costing, timelines, processes, training and professional services. The technology modules need to include cloud ready interfaces of technologies that is positioned off premises as well.**

Clarification of questions and queries is **3 working days** before the deadline of the submission

10. REQUIREMENTS OF YOUR SUBMISSION

This submission will not be considered unless it is -
Received on or before the time and date as indicated
Sealed and signed by person(s) duly authorised to act on behalf of your company
Received in full
Eskom reserves the right to cancel this RFI process at any time prior to entering into any contract that may result from this process and will not accept or incur any liability for such cancellation.
Eskom is not bound to accept any of the submissions, nor give reasons for any decisions in this respect.
The Information provided below may be used when going out on enquiry for a request for proposal or a quotation.

IMPORTANT NOTES

10.1   Please note that this enquiry is not a Request for Quotation/Proposal but a Request for Information only and therefore non-committal and does not constitute a guarantee of business, or an agreement to negotiate a binding agreement.

<div align="center">

Confidential

</div>

File name: Request for Information (RFI)_Cyber _Final

10.2   Due to the specific need that this RFI process has to fulfil, Eskom wishes to clarify that this invitation is not intended to impede, amend or replace any current or future procurement process that Eskom has engaged in or will engage in.

10.3   This RFI is a stand-alone information-gathering and market-testing exercise, intended only to inform and assist Eskom's further decisions. No respondent, through submission of information will gain any right to participate in any future process, and participates herein on the basis that it is providing information voluntarily to strengthen a potentially beneficial process for all stakeholders. In addition, no participant shall be prevented or excluded from participation in the bidding process due to submission of information in response to this RFI.

10.4   Any information provided pursuant to this RFI process and any subsequent processes and/or engagement is not confidential but Eskom will use the information only in the course of its process for a strategy for Customer Information and Billing Replacement.

10.5   Through making a submission, a respondent accepts the terms and conditions which govern this process.

10.6   All participants responding to this RFI process need to ensure that they have received all information and remain solely responsible for satisfying themselves as to the information required in responding hereto and are fully responsible for all costs incurred in relation hereto and under no circumstances will any resultant cost be borne by Eskom.

10.7   Eskom reserves the right not to proceed with any further engagements on the requirements presented.

10.8   Please complete the attached Acknowledgement Form and return it by email as indicated on the form within 3 days of receiving this Invitation.

File name: Request for Information (RFI)_Cyber _Final

APPENDIX A: RETURNABLE ACKNOWLEDGEMENT FORM

TO:	ESKOM HOLDINGS SOC LIMITED's *Representative*	FROM: **11.2**	
Attention:	Tamara Mda	Sender:	
Contact No:	011 800 3599	Contact No:	
e-mail:	MdaT@eskom.co.za	E-mail address::	

RFI reference number: MWP1364CX Confirmations of respondents to participate in a Request for Information on the technology options available in the market to enable the Cyber Forensic lab capability to do Cyber/Digital Forensics, as well as associated indicative costing, timelines, processes, training and professional services. The technology modules need to include cloud ready interfaces of technologies that is positioned off premises as well

We are in receipt of Eskom Holdings SOC Limited request for information dated………….

We confirm the following (please mark the appropriate response):

No	Statement	Yes	No	Comments
1.	We are interested in submitting a response in terms of Eskom's RFI process requirements			
2.	We have noted the deadline for the RFI submission			
3.	We intend to submit the information in the name of the organisation stated above			
4.	We would like to receive all further information and correspondence at our e-mail address as above			
5.	We have read and understood all the "important notes" under point 9 above.			

Yours faithfully

_____

Confidential

File name: Request for Information (RFI)_Cyber _Final