Request for Information (RFI)

Communication for Static and Mobile Communications

RFI No.7030/17/06/2022

Date of Issue	Thursday 02 June 2022	
Compulsory briefing session	No briefing session	
Closing Date	Friday 17 June 2022 at 16h30	
Place of tender submission	**Online only submission at tender@csir.co.za** If the size of the documents exceed 25MB, send multiple emails. Use the RFI number and description as the subject on the email.	
Enquiries	Strategic Procurement Unit	E-mail: tender@csir.co.za
CSIR business hours	08h00 – 16h30	
Category	Engineering	

Table of Contents

Glossary

Abbreviation	Term	Description
CSIR	Council for Scientific and Industrial Research	A statutory body established in terms of Scientific Research Council Act 46 of 1988, as amended
DSI	Department of Science & Innovation	

List of Acronyms

Acronym	Site Name
CSIR	Council for Scientific and Industrial Research
IP	Internet Protocol
ETSI	European Telecommunication Standards Institute
ICASA	Independent Communications Authority of South Africa
RFI	Request for Information
TBD	To be determined
DOCX	Document format used for open Microsoft Word documents
XLSX	Document format used for open Microsoft Excel spreadsheets
MB	Megabyte

SECTION A – TECHNICAL INFORMATION

1 INTRODUCTION

The Council for Scientific and Industrial Research (CSIR) is a leading scientific research and technology development organisation in Africa. In partnership with national and international partners, CSIR undertakes directed and multidisciplinary research and technology innovation that contribute to the improvement of the quality of life of South Africans and the world at large. The CSIR's main site is in Pretoria while it is represented in other provinces of South Africa through regional offices.

Problem Statement: The provision of physical and advanced security operations requires that there be a secure continuous means of communication internally at various facilities (intra-facility communication) amongst security officials and different role-players as well as secure communication between different facilities (inter-facility communication) where each facility can securely communicate with the next with no compromise of information. Secure communications are also essential for vehicles and convoys travelling between these facilities.

The request for information details the background and main requirements to allow prospective suppliers to provide CSIR with a brief on their respective products.

2 BACKGROUND

The CSIR is currently supporting a client with the design and specification of a system that can address the communications requirement as indicated above.
The system will be implemented at multiple facilities across the country. An IP network is connecting these facilities and can be utilised as part of the system design.
The system must also facilitate amongst a convoy between these facilities as well as from the convoy to the main facilities. The convoy will mostly travel along national highway routes.

3 REQUEST FOR INFORMATION

The purpose of this RFI is to gather relevant information from industry to enable the CSIR client to:

a. Adopt technologies available in South Africa.
b. Determine what solutions are available in Industry to address the Problem Statement.
c. Conduct technology evaluation and testing
d. Identify prospective bidders who have the capability to supply, maintain and support a suitable UHF trunking network, and
e. Generate the specification that can be used to acquire such a system in a subsequent competitive bidding process

Respondents must take note that a framework of detailed information on what is included or excluded from the scope of this RFI is not provided. The reason for this is to give respondents the opportunity to suggest approaches and technologies and to define their own integrated mobile device and management solution.

Respondents must provide explicit technical specification and network topology detail against the functional requirements defined. Additionally, all technical detail must be supported by manufacturer published literature. The evaluation team will only consider responses where manufacturer literature is provided.

The evaluation team will only consider responses from vendors formally recognised by the manufacturer/s.

Vendors who qualify may be requested to demonstrate their respective technology recommendations, including multi-vendor inter-operability and multi-technology inter-connectivity. Equipment suggested by the vendor must be available in South Africa for testing.

Interested parties should provide details of their Static and Mobile Communications offerings with regards to the following aspects.

1. Technologies proposed.
2. Adherence to ETSI standards of the proposed technologies.
3. ICASA approval of the proposed technologies.

4 RFI Functional Requirements

The following table indicate the main functional requirements. Respondents must indicate how the proposed technologies and solutions will be able to cater for these requirements.

The Physical Secure Communications solution must enable the definition, management and utilisation of user groups and profiles.
The Physical Secure Communications solution communication means can include radio, cell phone and VoIP.
The Physical Secure Communications solution must be able to log violation incidents when violations occur.
The Physical Secure Communications solution must be able to generate alerts for the violation incidents as they occur according to the delegations of authority of the radio communication network.
The integrated system must be able to send pre-defined notifications to user groups as per the operational deployment e.g., shifts, teams/unit/Group in relation to awareness or communication.
The Physical Secure Communications solution must be able to record all communication 24/7/365.
The recordings must only be accessible by the authorised user/administrator.
The authorised user/administrator must be able to download the recordings.
User(s) must be able to make emergency calls via voice and text.
User(s) must be able to make a master call override via voice and text.
User(s) must be able to make an individual (one-to-one) call.
The Physical Secure Communication solution must allow a user(s) to send a short messaging service (SMS).
The Physical Secure Communications solution must be able to track radios on the network within and between facilities.
A user must be able to report a suspicious article via the communication device.
A user must be able to report a hostage situation.
A user must be able to report a suspicious vehicle and person with descriptive details.
A user must be able to receive a photo via the communication means.
The Physical Secure Communications solution must be able to block a radio on the network to guard against unauthorised access to information should it be stolen.
The Physical Secure Communications solution must be able to create different teams (at least 5) with dedicated channels and alternative channels of communication.
Each Facility Security Control Room, Advance Control Room or National Operational Centre must be able to broadcast messages to their operational members or within the Group via voice or data.
The secure communication device must be able to offer bi-directional information sharing and feedback between participants via voice and data within a secure “bubble”.
The Physical Secure Communications solution must be able to cater or contain a maximum of 50 users at one location or within a specific group and cater for around 500 users simultaneously.
The Physical Secure Communications solution must be able to integrate with the current technology being utilised in the Group’s different facilities e.g., CCTV
Each Facility Security Control Room, Advance Control Room or National Operational Centre devices utilised must be able to automatically log all events/actions and communications for audit trails and governance purposes.
Two-way radios communication devices must be enclosed in anti-tamper-resistant housing.

The external parts of the Physical Secure Communications solution must have environmental proof to (IP65) protect against unique elements associated with the South African weather.
The Physical Secure Communications solution must be able to encrypt voice communication from the point of transmission until it reaches the intended recipient.
The Physical Secure Communications solution must be able to transmit clear voice quality (capability to remove hisses and crackles (noise)).
The Physical Secure Communications solution must be able to restrict voice transmission to the intended recipient or a defined group only.
The Physical Secure Communications solution must be able to protect transmissions from malicious jamming and signal interception

5 VENUE FOR SUBMISSIONS

All submissions must be submitted to: tender@csir.co.za

In light of the Covid-19 pandemic, the CSIR requires that all RFI submissions be submitted electronically to tender@csir.co.za. Should the submission file size exceed 25 MB, respondents can submit in multiple emails. Use the RFI number 7030/17/06/2022 and description of the RFI as the subject on your email.

6 RFI PROGRAMME

The RFI programme, as currently envisaged, incorporates the following key dates:

Table 2: RFI Programme

• Issue of RFI documents:	02/06/2022
• Briefing session:	None
• Closing / submission Date:	17/06/2022
• Estimated contract duration	N/A

7 SUBMISSION OF RFI RESPONSE

Respondents are to submit at least the following (3) documents as part of their response:

1. Detailed technical description of the capabilities of the respondents ……. Response to be submitted in DOCX or PDF format
2. Pricing plan breakdown indicating the elements that will be once-off payments and the elements that will require renewable licenses.
3. Completed Technical Checklist indication how/if the functional requirements will be met by the proposed system.
4. List of client references that utilises the proposed solution.

Additional supporting documentation may be submitted as needed.

RFI submissions must be submitted at: tender@csir.co.za

All RFI submissions are to be clearly marked with the RFI number in the subject line of the email submission.

8 DEADLINE FOR SUBMISSION

RFI submissions shall be submitted to tender@csir.co.za no later than the closing date of **17 June 2022** during the CSIR's business hours. The CSIR business hours are between 08h00 and 16h30.

9 REVIEW PROCESS

Review of RFI submissions

All submissions will be reviewed by a review team.

10 ENQUIRIES AND CONTACT WITH THE CSIR

Any enquiry regarding this RFI shall be submitted in writing to CSIR at tender@csir.co.za with "7030/17/06/2022" as the subject.

Any other contact with CSIR personnel involved in this RFI is not permitted during the RFI process other than as required through existing service arrangements or as requested by the CSIR as part of the RFI process.

11 MEDIUM OF COMMUNICATION

All documentation submitted in response to this RFI must be in English.

12 COST OF SUBMISSION

Respondents are expected to fully acquaint themselves with the conditions, requirements, and specifications of this RFI before submitting proposals. Each respondent assumes all risks for resource commitment and expenses, direct or indirect, of their submission preparation and participation throughout the RFI process. **The CSIR is not responsible directly or indirectly for any costs incurred by respondents.**

13 CORRECTNESS OF RESPONSES

13.1 The respondents must confirm satisfaction regarding the correctness and validity of their submission and that all prices and rates quoted cover all the work/items specified in the RFI.

13.2 The respondents accepts that any mistakes regarding the solution and budgetary pricing and calculations will be at their own risk.

14 VERIFICATION OF DOCUMENTS

Respondents should check the numbers of the pages to satisfy themselves that none are missing or duplicated. No liability will be accepted by the CSIR in regard to anything arising from the fact that pages are missing or duplicated.

15 ADDITIONAL TERMS AND CONDITIONS

15.1 A respondent shall not assume that information and/or documents supplied to CSIR, at any time prior to this request, are still available to CSIR, and shall consequently not make any reference to such information document in its response to this request.

15.2 Copies of any affiliations, memberships and/or accreditations that support your submission can be included at the respondent's discretion.

16 CSIR RESERVES THE RIGHT TO

16.1 Extend the closing date;

16.2 Verify any information contained in a submission;

16.3 Engage with specific respondents to clarify the technical specifications/performance of respondents' solution either through electronic communication or through site/facility visits to verify respondents' capabilities, infrastructure, processes, etc.

17 DISCLAIMER

This RFI is a request for information only and not an offer document. Submissions to this RFI must not be construed as an acceptance of an offer or imply the existence of a contract between the parties. By submission of its information, respondents shall be deemed to have satisfied themselves with and to have accepted all Terms & Conditions of this RFI. The CSIR makes no representation, warranty, assurance, guarantee or endorsements to respondents concerning the RFI, whether with regard to its accuracy, completeness or otherwise and the CSIR shall have no liability towards the respondent or any other party in connection therewith.