

# **Request for Tender**

**For**

**Advanced Vulnerability Management  
Solution**

**For**

**Mobile Interim Company 1 S.A.L**

**Reference Number: MIC1/RFT/CFO-PRO/0034-24**

**Beirut-Lebanon, January 2024**

## Table of Contents

### Contents

Introduction: Company's Profile.....	3
Article 1: Object.....	3
Article 2: Scope.....	3
Article 3: General Terms .....	3
3.1. Participation in the RFT process .....	3
3.2. Joint Offer .....	4
3.3. Cost of Tender .....	4
3.4. Offer Ownership .....	4
3.5. Offer Errors .....	4
3.6. Miscellaneous .....	4
Article 4: Clarifications .....	5
4.1. General Terms .....	5
4.2. Q&As format .....	5
Article 5: Presentation of Offers.....	5
5.1. Envelop 1 .....	6
5.2. Envelop 2.....	7
Article 6: Time limit for Presenting Offers .....	7
Article 7: Period of Validity of Offer.....	8
Article 8: Compliance Matrix.....	8
Article 9: Special terms .....	9
9.1. Terms of Payment.....	9
9.2. Commercial/Financial Conditions.....	9
9.3. End of Sales .....	10
9.4. Delivery Penalty / Liquidated Damages .....	10
9.5. Miscellaneous .....	11
Article 10: Technical Specifications .....	11
Article 11: Information Security Specifications.....	21
Article 12: Evaluation of Offers.....	21
Article 13: Entering into Contract.....	22
Article 14: Termination and Assignment.....	22
Article 15: Boycott of Israel Requirement .....	22
Article 16: Applicable Law and Dispute Resolution.....	23

## Introduction: Company's Profile

MIC1, operating under the brand name Alfa Nowadays, Alfa caters for the mobile needs of more than 2M subscribers including businesses and offers a variety of services and products that fit all age groups and preferences. Alfa vision is to provide competitive telecommunications services, while maintaining the highest quality of service and upholding sustainable commitments.

## Article 1: Object

Bidders as defined in article 2 hereunder are hereby invited to submit their offers (herein referred to as "**Tender**" or collectively as "**Tenders**") for the supply of Advanced Vulnerability Management Solution to the Mobile Interim Company 1 S.A.L (herein referred to as "**MIC1**") who is managing one of the two national Mobile networks for the benefit of the Republic of Lebanon.

The services required by MIC1 from the Bidders under the RFT (as defined in article 2 hereunder) are mentioned in appendix 1.

This tender process is subject to the provisions of Public Procurement law (PPL) no. 244 dated 19<sup>th</sup> July 2021.

## Article 2: Scope

This request for tender (herein referred to as "**RFT**") is restricted to companies which are specialists in Cybersecurity, Vulnerability management and related services (herein referred to as "**Bidders**" or "**Bidder**" for any one of them separately), have signed a non-disclosure agreement or a confidentiality agreement with MIC1 and have received an invitation letter from MIC1 to participate in the RFT.

## Article 3: General Terms

### 3.1. Participation in the RFT process

Bidders shall participate in the RFT process at their own risk. Such participation does not give the Bidders any grounds whatsoever for any right for compensation from MIC1.

The Bidders expressly acknowledge that their participation in the RFT process will be deemed as an undertaking that: (i) they have the full capacity, right, power and authority and have taken all necessary actions to enter into the RFT process; and (ii) the performance of their obligations under the RFT and or any potential purchase order (hereinafter "**PO**") / contract will not result in the breach of any terms or provisions of, or constitute a default under, any judgment, decree, or agreement or instrument to which they are a party or by which they are bound. Furthermore, the Bidders expressly acknowledge that their participation in the RFT process will be deemed as an undertaking that: (i) they are not and shall not be, directly or indirectly, associated with any person or entity involved in terrorism and / or money laundering; (ii) they shall not be engaged, directly or indirectly, in any illegal, corrupt, and / or fraudulent practices; (iii) they shall adhere to the highest ethical standards in the performance of their obligations under the RFT and / or any potential PO / contract, and (iv) they shall not be engaged, directly or indirectly, in activities involving child labor, trafficking in arms, sexual exploitation or discrimination.

Thus, Bidders will be solely liable for and will hold MIC1 harmless from any claim, damage, action of any nature by any third party, and any consequences thereof, relating to any such breach or default as mentioned hereabove.

### 3.2. Joint Offer

Two or more Bidders may form a consortium and submit a joint offer under the terms and conditions defined herein. The offer must be submitted under the name of one member of the consortium which shall be responsible for undertaking all negotiations and discussions with MIC1 and performing the services under the RFT.

### 3.3. Cost of Tender

Bidders shall bear any and all costs, expenses, or investments in connection with the preparation and / or submission of their offer and / or any presentation and / or any other cost or expense incurred by the Bidders as a result of the RFT.

MIC1 shall not be, in any case, directly or indirectly, responsible, or liable for any cost, expense or investment associated with the preparation and / or submission of the offers and / or any presentation and / or any other cost or expense incurred by the Bidders as a result of the RFT.

### 3.4. Offer Ownership

Notwithstanding the ultimate outcome, all the offers submitted by the Bidders shall become the sole property of MIC1.

### 3.5. Offer Errors

Bidders are solely responsible for any error, misstatement or omission contained in their offer.

If any Bidder identifies an error, misstatement, or omission contained in its offer, it may at its own risk, effort and expense submit a replacement offer (herein referred to as "**Replacement Offer**") provided that the Replacement offer fully complies with the RFT and is delivered within the Closing Date. Bidders will not be allowed to alter their Offer after the Closing Date.

However, if a Bidder identifies, after the Closing Date, a material error, misstatement, or omission contained in its Offer, it must notify MIC1 in writing within 5 days as of the date of such identification.

In the event the Offer contains an error in cost, time or other calculations, quoted items shall prevail. In case of inconsistencies between various sections in the Offer, MIC1 retains the right to select the option which shall be applied and be valid for the Offer.

### 3.6. Miscellaneous

MIC1 reserves the right to cancel, postpone or modify the RFT, including all its terms and conditions, at any time before the bid assignment, or to repeat the RFT, at its absolute discretion, under the provisions of Article 25 of the Public Procurement Law n0. 224 dated July 19<sup>th</sup>, 2021, without incurring any liability towards the Bidders and/ or any third party. No offers will be opened after the bid cancellation decision. No responsibility or liability is or will be accepted by MIC1 in respect of any error or misstatement in or omission from the RFT and / or any response to request for Clarifications (as defined in article 4 hereunder) and / or any information or data provided by MIC1 in connection with the RFT.

All information regarding MIC1 included in the RFT and / or any response to request for Clarifications is intended to assist the Bidders in the preparation and submission of their Offer. This information is provided for information purposes only and is not exhaustive. No representation or undertaking is given as to accuracy, adequacy, or completeness of this information. MIC1 shall not be liable for any inaccuracy, oversight, or omission in or from any such material.

**Bidders have the right to object as per article 103 of the PPL no.244/2021.**

## Article 4: Clarifications

### 4.1. General Terms

Clarifications needed by the Bidders to prepare the Offer (herein referred to as "Clarifications") should be consolidated and submitted to MIC1 in 1 set. Applications for Clarifications should be submitted within a maximum of 5 calendar days before the Closure Date of the RFT set by MIC1 to:

Mr(s): amanda.nicolaselhachem@alfamobile.com.lb

CC: technology.purchasing@alfamobile.com.lb

MIC1 answers will be submitted to all Bidders after **6** calendar days before the Closure Date of the RFT set by MIC1.

Bidders should not contact, directly or indirectly, MIC1 concerning the RFT process, starting from the Issue Date until the final selection. The only contact would be for clarification purposes and only by virtue of the mechanism described in this article.

### 4.2. Q&As format

The Clarifications submitted as per article 4.1 above should be in excel format filled as per below:

RFT Name REF# xxx- 1x (Q&As)		
AREA	Bidder Questions	ALFA- MIC1 Answers

Questions should be "serious and valid". This means that any inquiry should be in connection with the subject of this Tender and the response to which could be of impact on the offer to be offered by the Bidder. MIC1 upon its discretionary authority shall determine if the questions are serious and valid, and subsequently whether or not a response shall be given.

Failure to submit serious and valid Questions will be considered as an attempt to delay the tender process and MIC1 will have the right to ignore such Questions without any justification.

## Article 5: Presentation of Offers

- The technical offer part (herein referred to as "**Technical Offer**") described hereafter should be enclosed in an envelope separated from the commercial/financial offer part (herein referred to as "**Commercial/Financial Offer**").
- All Offers shall be written in English language.
- The RFT has to be reviewed thoroughly by bidders. The selected bidder, and as a prerequisite for his award, will be requested to remit back the RFT document after being initialed on all its pages.

- A copy of “Alfa Security Terms & Conditions for Third Party “and “Supplier Compliance Form” are enclosed to this RFT for Bidders’ review and reference.  
However, it should be noted that the selected Bidder will be requested to sign these documents upon project award and prior to the PO / contract signature. These documents are an integral part of the issued PO / contract, and their signature is mandatory to execute / implement any solution in MIC1 network.
- The Bidders shall submit a clear and complete list of references for similar implementations / projects in a relevant environment.
- **All Offers shall be in US Dollars / Lebanese Pound**, shall include all taxes, duties and levies (excluding only Lebanese VAT), and shall be fixed, unconditional, unreserved and binding for the Period of Validity (as defined in article 7 hereunder). All Offers should cover the full range of services requested under the RFT.
- Each Bidder shall be solely responsible to pay and bear its own taxes and duties levied on it under any relevant jurisdiction or territory. For the sake of avoiding any doubts, Bidder shall be individually responsible to ascertain its tax liabilities under any subject territory and settle the same with its own resources without having any recourse whatsoever towards MIC1.
- Bidders should submit their Offer in a sealed envelope, with RFT Name and Reference clearly mentioned, which should contain two separate sealed envelopes, containing the below:

### 5.1. Envelop 1

Envelop 1 is labelled by the “RFT reference- Technical Offer & the Bidder ‘s name”, and should include:

- A cover letter, in two copies, addressed to MIC1 showing the Bidder’s interest in submitting the Offer to the RFT (where the name of project as mentioned in this RFT is explicitly mentioned) duly signed and stamped by the authorized representative and listing the documents enclosed whether in hard or soft copy. The cover letter should also mention the names of partners (if any) that are participating under the umbrella of the company in question.
- Thus, the technical submission should be limited to the cover letters (2 copies) and the sheet special terms (2 copies) within the attached document named “Compliance matrix- incase it is part of this RFT and shared by MIC1 in the invitation email”.
- The complete version of the filled compliance matrix is not needed in hard copy, only on CD in both excel and PDF versions including bidder logo.
- The cover letter, however, should confirm that, in case selected, bidder commit to deliver according to the complete compliance matrix submitted as part of the technical response on the CD.
- No need to share a hard copy version of the executive summary or technical solution; it can be only part of the technical submission on CD.
- 3 labeled CDs with the complete Technical Offer to RFT, in WinWord, Compliance Matrix in MS Excel and in PDF format with company logo, unpriced BoM in MS Excel & supporting technical documentation in WinWord or PDF format.

- A signed copy of the enclosed contract draft as proof of approval on the terms & conditions. The selected bidder shall sign the contract within 15 days after tender award, otherwise he will be excluded from the tender and MIC1 shall retain the bid bond.
- If the Bid Bond amount can be determined in advance and specified as a lump sum by MIC1, it should be enclosed in envelope 1.

**N.B: No prices even Free of Charge (FoC) term shall be mentioned in the technical offer envelope whatsoever.**

**All submitted documents should be Signed and Stamped by bidder.**

## **5.2. Envelop 2**

Envelop 2 is labelled by the "RFT reference- Commercial Offer & the Bidder 's name", and should include:

- 2 copies of the Commercial/Financial offer **summary** showing the **high-level** deliverables and their prices (**detailed pricing / BoQ should be included as soft copy on CD only**) duly signed by the authorized signatory and stamped –in Hardcopy. Thus, the commercial/financial submission should be limited to the summary sheet (2 copies) of the attached "financial sheet" in case it is part of this RFT and shared by MIC1 in the invitation email; all remaining sheets and detailed BoQ should be put on the CD.
- 2 labeled CDs with the complete price list in MS Excel Softcopy with formulas and equations clearly applied along with the filled commercial sheet - commercial.xlsx (in case embedded within this RFT).
- If the Bid Bond amount cannot be determined in advance and it is well specified as a percentage of the total offer amount, it shall be placed within envelope 2.  
A Bid Bond amounting 2% of the total offer, from the participating bidders' bank to MIC1 is requested. This bid bond is ruled by article 34 of the Public Procurement Law dated July 19<sup>th</sup>, 2021, and is considered as a major condition for the compliance to this Tender document and selection criteria. The validity of the LOG should be for 208 days as of offers submission date (shall exceed the Offer's validity by 28 days as per article 4.2.17).

**"RFT envelopes must be sealed with a large adhesive tape. Envelop must hold RFT Reference and title without mentioning the bidder's name".**

N.B: Bidders must strictly comply with all the requirements above mentioned in this article 5. Any Bidder which fails to comply with any of the requirements listed in article 5 above will be immediately disqualified.

## **Article 6: Time limit for Presenting Offers**

Every Bidder is bound to present its complete offer along with all the required and additional documents as mentioned in the RFT, to MIC1, at the latest **15** days from the date of its signature of the RFT (herein referred to as "**Closing Date**") for the attention of:

Mobile Interim Company 1  
Procurement Department  
Attention: **Amanda El Hachem**  
Office: +961 3 391 000 - Fax: +961 3 391 620  
Email: [amanda.nicolaselhachem@alfamobile.com.lb](mailto:amanda.nicolaselhachem@alfamobile.com.lb)



Address:

Parallel Towers, 17th floor, near Freeway Center, Dekwaneh, Beirut.

P.O.B: 55-534 Sin El Fil.

MIC1 may, at its own discretion, extend the Closing Date for the submission of Offers by notifying all Bidders thereof in writing.

Any Proposal received by MIC1 after the Closing Date will be automatically rejected.

## **Article 7: Period of Validity of Offer**

The Offers submitted by the Bidders shall be commercially/financially and technically binding for the Bidders for a period of 6 months at least as of the Closing Date or any extension of the Closing Date decided by MIC1 (herein referred to as "**Period of Validity**").

Any Offer valid for a shorter period may be rejected by MIC1 at MIC1's sole discretion. The latter may solicit the Bidder's consent to an extension of the Period of Validity. The request and the response thereto shall be made in writing. Any Bidder granting its consent to such extension will not be entitled / permitted to modify its Offer.

No offer may be withdrawn before the expiration of the Period of Validity.

## **Article 8: Compliance Matrix**

The following should be considered, while filling the compliance matrix (herein referred to as "**Compliance Matrix** "):

- Every Offer shall contain a clear reference to the supporting documentation within the Bidder's provided set of technical documentation. The reference must indicate explicitly the document title, page and section.
  - "Fully Compliant", when the Bidder fully complies with the requirements or fully agrees to the related statement, along with a clear explanation in both cases, in addition to the related reference to the supporting documentation when applicable.
  - "Partially Compliant", when the Bidder partially complies with the requirements or partially agrees to the related statement, along with a clear explanation in both cases for the compliance limits and / or agreement limitation, in addition to the related reference to the supporting documentation when applicable.
  - "Non Compliant", where the Bidder does not comply with the requirements or does not agree to the related statement, along with a clear explanation in both cases for the non-compliance / limitation, and with the related reference to the supporting documentation when applicable.
  - "Noted" when a statement is not a requirement but is only for information purposes. "Noted" will be accepted as meaning that the Bidder has read and understood the information. "Noted" is not accepted when a "Compliant" or "Non-Compliant" is the proper response.
- In cases of doubt, during the evaluation of the Offer by MIC1 as provided for in article 12 hereunder, any "Noted" statement shall be considered as "Compliant" for the purpose of such evaluation, and for PO / contract purposes as the Offer to the RFT will form an integral part of any potential PO / contract signed with the Bidder.



- The Compliance Matrix will be analyzed by MIC1 in detail and the compliance statements will be used within the RFT assessment model.
- In case the Offer states “Compliant” to a MIC1 requirement and the analysis of the solution shows that there is no full compliance, such statement will be assessed as “Non-Compliant” and an additional penalty will be applied.
- In case the Offer states “Compliant” to a MIC1 requirement while not specifying any reference, such statement will be assessed as “Non-Compliant” and an additional penalty will be applied.
- For any item that is not supported and / or for which no quote exists in the Commercial/Financial Offer, the price penalty is computed by taking the highest price amongst other Bidders.

If at any stage during the evaluation of the Compliance Matrix it becomes obvious to MIC1, that the solution offered by the Bidder substantially deviates from the requirements as defined in this RFT, such Offer will be disqualified at MIC’s sole discretion with **immediate effect**.

## Article 9: Special terms

### 9.1. Terms of Payment

The below describes the minimum payment requirements which are based on a careful analysis of the solution components and required deliverables. However, such minimum payment requirements are not in any way binding to MIC1 and modification of the same might be applied by MIC1 at its sole discretion after selection, on PO or contract level, in case the same is deemed necessary by MIC1.

For SW & Licenses:

100% Upon PO Signature

For Implementation & Services:

50% down payment on PO issuance 45 days from invoice receipt

50% on Final acceptance

### 9.2. Commercial/Financial Conditions

Bidders shall submit their best and final price. **No negotiations shall be made after offers submissions.**

- MIC1 reserves the right to negotiate with the selected Bidder all or part of the Offer as MIC1 deems convenient. In other words, MIC1 has the full flexibility to buy the full scope of the Offer or certain parts of it without any impact on unit rates and discount granted. It might also select different Bidders to supply different parts of the RFT’s scope of work depending on its strategy and needs.
- A Bid Bond from the participating bidders’ bank to MIC1 with a value of 2% of the total offer should be presented for participation within envelop 2. The validity of this LG should be for 208 days as of offers submission date; it will be returned to non-selected bidders.

This LG will be returned to selected bidder after submission of the Performance Bond mentioned below.

The Bid Bond is ruled by the article 34 of Public Procurement Law 244 dated 19 July 2021.

- Another mandatory Performance bond from winning bidder' bank to MIC1 with a value of 5% of the quoted services should be presented upon tender award only within 15 days from contract start date.
- The performance bond shall remain valid and effective from the date of issuance up to the contract expiry date.
- The Performance Bond is ruled as by the article 35 of Public Procurement Law 244 dated 19 July, 2021.
- The bidder is not allowed to introduce any new technical offer in the commercial envelop which will be considered a subject to disqualification.
- Fees submitted by bid winner will be announced on PPA website following tender award as per Public Procurement Law requirements.
- Any subcontracting scope by the bidder shall be clearly indicated in the offer. Bidders should not in any way subcontract more than 50% of the bid scope inline with Clause 30 of PPL.

### 9.3. End of Sales

End of sales date of proposed servers / appliances / systems shall be at least more than 6 months from the Closing Date. If by the time the PO is issued by MIC1 the proposed servers / appliances / systems have reached end of sales, then the Bidder shall offer the next generation equipment with equivalent or better specifications **at no extra cost for MIC1.**

End of sales date of proposed hardware shall be at least 8 years from the date of the Closing Date. If, for any reason, by the time the PO is issued by MIC1 the proposed hardware has reached 60% of its overall life span, then Bidder shall offer the next generation equipment with equivalent or better specifications **at no extra cost for MIC1.**

### 9.4. Delivery Penalty / Liquidated Damages

- In case of delay in the delivery, a penalty of 1% per day of delay shall be deducted from the total amount for a maximum of 20%.
- The filled Compliance Matrix as well as the Offer and BoQ are an integral part of the PO to be issued by MIC1 following the selection of the Bidders. Bidders 'abidance by and respect of their Offer, and more particularly on the delivery date mentioned therein, and based on which the PO is issued, is mandatory.  
In case the above is not respected by the Bidder or in case the latter fails to deliver a feature, functionality or item for which he has already inserted "Compliant" in the Compliance Matrix and included in the Offer, then the following will be applied:
  - A penalty of 5% from the total amount of the project cost will be applied for each feature/functionality or item.

- Not delivered by the Bidder. This amount will be deducted from the final acceptance payment.
- If the penalty value exceeds the amount remaining to be paid for the project, then MIC1 has the right to cancel the project with immediate effect and the Bidder will have to refund the total amount paid to the Bidder without the need for a prior notice or any judicial or extra-judicial proceedings.

If a feature, functionality or item, is marked as a Killer Point (as defined in article 11 below) and the Bidder fails to deliver it upon implementation, then MIC1 has the right to cancel the project with immediate effect and the Bidder will have to refund the total amount paid without the need for a prior notice or any judicial or extra-judicial proceedings.

## 9.5. Miscellaneous

- Bidder must explicitly mention, in the Offer and the BoQ, any prerequisite not stated within the RFT requirements and specifications and that might entail additional cost or impact while adding its respective price or the additional deliverables it needs (if not within Bidder's scope).
- Based on the provisions of the income tax law (Articles 41, 42 and 43), a 7.5% (on Opex) and 2.25% (on Capex) are to be deducted from the invoice for the Bidders that do not maintain a place of business or do not have a legal structure in Lebanon.
- All Bidders with local presence should have a corporate contract with MIC1 that covers 100% of their employees' business lines before entering into business relations with MIC1. If the selected Bidder does not fulfill this option at the time of project award, MIC1 corporate sales team will contact its representative for this purpose.
- The bidder to any tender launched by Alfa should declare any relative relations with any Alfa employee up to the 4th degree under Clause 30 of the PPL, for MIC1 to be able to assess the existing of any potential conflict of interests which may lead to deprive the bidder from participating to the tender under the risk of disqualification,
- The bidder will be automatically disqualified in two cases according to Clause 8 of PPL: in case of bribery or corrupted activity or conflict of interest.

## Article 10: Technical Specifications

GENERAL REQUIREMENTS
The bidder is invited to bid for an advanced Vulnerability management solution and in compliance with the following requirement:
The solution must support automatic asset discovery and maintain an accurate inventory of all assets , including devices, servers, applications, and endpoints, across the organization.
The solution should seamlessly incorporate vulnerability and compliance scanning, encompassing the merging of licensing and data consolidation, as well as the analysis and querying for IP addresses 3500."
The vendor must be positioned among the leaders in the vulnerability management industry. i.e ( provide reports from Gartner, IDC or forrester ..)

The software should enable monitoring for compliance with industry standards (e.g., CIS, NIST, ISO27) and regulatory requirements. i.e: Specify the % coverage of CIS benchmarks between the vendors in the vulnerability management domain.
The vendor must have the highest coverage of vulnerabilities between vendors in this domain.
The solution must be deployed on-premises.
The bidder shall provide a detailed explanation of their licensing schema as part of their proposal for the advanced vulnerability management solution. The explanation should clearly outline the licensing model(s) offered, including any hybrid or alternative licensing approaches available.
<b>ASSET DISCOVERY CAPABILITIES</b>
The solution should offer an asset discovery feature that does not count towards licensing limitations.
The solution must provide an active scanning capability and passive network monitoring capability for asset discovery.
The solution must be able to discover mobile devices.
The solution must provide integrated web and database service discovery.
The solution must be capable of detecting services that are running on non-standard ports.
The solution must be capable of detecting services configured not to display connection banners.
The solution must be capable of testing multiple instances of the same service running on different ports.
The solution must be capable of scanning dead hosts (devices which do not respond to ping)
The solution must support the use of SMB and WMI for scanning Windows systems.
The solution must be capable of automatically starting remote registry services on Windows systems when performing a credentialed scan, then automatically stopping the service again once the scan is complete.
The scanner must support secure shell (ssh) with the ability to escalate privileges for vulnerability scans and configuration audits on Unix systems.
The solution must be able to collect/import and display both IT and OT asset data for a single view of converged IT/OT environments.
The solution must provide the ability to tune scan policies for minimal impact on networks and targets.
The solution must provide active and passive discovery of wireless access points (WAPs).
The solution must provide the ability to detect new devices and send alerts via email, syslog, or console notifications.
The solution must provide the ability to automatically launch scans against new devices.
The solution must have the capability to discover all assets without impacting their license count and then be able to choose which assets to actively manage.
Asset tagging and grouping capabilities: The solution should allow for categorizing assets (tags) based on various attributes, simplifying management and reporting
The solution should include a static and dynamic asset lists where static does not change unless manually updated and dynamic asset uses rules to automatically update the assets within them based on a defined criteria

The solution should contain a list of asset templates including web servers, SSH servers, Network Printer, SQL servers etc... then after choosing a template, the discovered assets will be added to the group

#### **VULNERABILITY SCANNING CAPABILITIES**

The solution must be capable of authenticated and non-authenticated scans for both local and remote vulnerability detection without the need for a client-side agent installed on the target device.

The solution must support agent-based and agent-less scanning capabilities.

The solution must provide both authenticated and non-authenticated network-based scanning of target systems.

The solution must provide a significant amount of vulnerability checks beyond the Windows operating system.

The solution must be capable of tracking DHCP changes by associating scan results with system hostnames.

The solution must support the ability to preserve scan results of inactive hosts for a customizable period of time.

The solution must include detailed output of scan findings to include information such as DLL versions expected and found.

The solution must be CVE compatible and provide at least 10 years of CVE coverage.

The solution must report on known weaknesses in a given target identified by security advisory organizations (e.g., Common Vulnerabilities and Exposures database (CVE) or the Open Sourced Vulnerability Database (OSVDB) or the SecurityFocus Bugtraq (BID) or any combination of them).

The solution must support PCI Compliance vulnerability scanning. The solution must include pre-defined PCI scan profiles that meet current PCI DSS criteria for network scanning. Functionality must exist to filter all other non-PCI relevant vulnerabilities.

The solution must provide patch auditing for Microsoft operating systems and applications such as Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008 / 2008 R2, Windows Server 2012 / 2012 R2, Windows Server 2016, Windows Server 2019, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange, and more.

The solution shall support the scanning of containerized environments, such as Docker and Kubernetes, to identify vulnerabilities within containers and their associated images.

The solution must provide patch auditing for all major Unix operating systems to include macOS, Linux (multiple distributions), Solaris, IBM AIX, HP-UX, and more.

The solution must provide patch auditing for network infrastructure to include Cisco, Juniper, F5, Fortinet, HP Aruba, and more. List network infrastructure available for patch auditing.

The solution must be able to collect/import and display both IT and OT vulnerability data for a single view of converged IT/OT environments.

The solution must provide coverage for 3rd party applications such as Java and Adobe. List 3rd party applications available for patch auditing.

The solution must provide integration with patch management systems for patch auditing and delta reporting against scan findings such as Microsoft WSUS/SCCM, Red Hat Satellite, IBM BigFix (formerly IBM Tivoli Endpoint Manager), Symantec Altiris, VMWare Go.

The solution must provide integration with Mobile Device Managers (MDM) for mobile device discovery and auditing.
The solution must provide reputation and threat intelligence feeds for malware and botnet discovery.
The solution must provide predictive vulnerability prioritization that uses real-time threat intelligence and machine learning algorithms to score vulnerabilities and predict which ones are most likely to be exploited in the near future Or propose any equivalent feature.
The solution must provide vulnerability prioritization context that helps users understand the key factors influencing each vulnerability score (e.g., threat recency, exploit code maturity, intel source categories) or equivalent features.
The Solution must provide a comprehensive and contextual vulnerability scoring methodology that goes beyond traditional CVSS scores. The scoring methodology should consider factors such as CVSS, exploitability, asset exposure, and real-time threat intelligence to assess vulnerabilities accurately. It should also incorporate real-time threat data and intelligence feeds to dynamically adjust vulnerability scores based on emerging threats.
The solution must utilize Asset Criticality Rating (ACR) score or equivalent feature
The solution must also include vulnerability scoring according to the Common Vulnerability Scoring System (CVSS).
The solution must provide customizable weighted scoring mechanism based on industry accepted standards such as CVSS.
The solution must provide vulnerability exploitability information from Core Impact, Metasploit, Canvas and more
The solution must provide malware exploitability information.
The solution must intelligently select tests based on information gained from initial scans to attempt further testing based on the previously obtained information about a given device or host.
The solution must track the lifecycle of vulnerability instances as it relates to individual hosts as well as the environment, to include when a vulnerability was first discovered, last observed, and mitigated.
The solution must support vulnerability and compliance scanning of VMware servers using the native VMware API.
The solution must allow for scheduled scanning of devices.
The solution must allow selected tests to be enabled or disabled during scans.
The solution must include the ability to disable potentially harmful checks.
The solution must automatically start and stop scans to the schedule without user interaction.
The solution must allow the ability to interactively pause and resume scans.
The solution must allow scans that are not completed within an established timeframe to rollover to the next scheduled timeframe.
The solution must be able to accept scan targets in multiple formats including DNS names, IP ranges and IP classes, and pre-defined asset lists. For instance, 10.0.1.1 – 10.0.1.100. Importing of a list of IPs contained within a file must also be supported. Describe the manner in which targets can be input to the solution.
The solution must support IPv6 scanning, with passive discovery of IPv6 targets.
The solution must provide the ability to exclude the scanning of peripheral devices such as printers.



### Asset Criticality & Asset Exposure Score (AES)

The solution should Leverage Asset Criticality Rating (ACR) or equivalent feature offered in the solution to predict the priority of assets based on indicators of business value and criticality. Pairing Asset Criticality with Predictive Prioritization brings a tailored approach to vulnerability management to show what vulnerabilities and their associated assets to prioritize first.

The solution should calculate a dynamic AES Asset Exposure Score or equivalent metric for each asset on the network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES or equivalent metric indicates higher exposure.

This calculation should consider factors such as asset criticality (adjustable as needed) and vulnerability severity, represented by a metric equivalent to the Vulnerability Priority Metric (VPM). Furthermore, it should provide real-time updates to reflect changing conditions, supporting informed risk mitigation decisions.

### External Attack Surface management

The Solution provided should be able to perform External Attack Surface management discovery (EASM) qty: 2 Domains

### ARCHITECTURE - SCALABILITY & PERFORMANCE

The solution must provide a centralized server for collection and management of security information that resides locally within the organization's network.

The solution must provide the capability to deploy a tiered architecture of multiple consoles.

The solution must centralize and fully automate updating of vulnerability and threat intelligence feeds from the vendor on a daily schedule.

The solution must provide an offline update process to update the server in air gapped networks.

The solution must be configurable to retain results for a defined and configurable period of time after which the results are expired and purged from the database automatically.

The server must provide a comprehensive API for automated scripting of scanning and exports of security data.

The solution licensing must allow for a standby server to be synchronized with the primary server for failover.

### User and Role Management

The solution must provide role-based access control with enough granularity to control users access to specific data sets and functionality that is available to those users.

The solution must allow administrators to define roles based on job functions and appropriate levels of access to functionality.

The solution must have support to integrate with LDAP for user authentication.

The solution must have support for multiple LDAP servers for authentication.

The solution must support Security Assertion Markup Language (SAML) in order to provide multiple SSO/authentication options such as Shibboleth and Okta.

The solution must support detailed user activity auditing. A robust audit trail is essential for tracking changes and user activities within the vulnerability management system.

The solution must allow administrators to limit access on a per user or per group basis to specific asset lists, scan policies, and vulnerability repositories.

The solution must allow administrators to assign resources on a per user or per group basis such as scan policies, asset lists, queries, and credentials.



The solution must allow administrators to limit scanning permissions to full scanning, scanning using specific policies, or no scanning.
The solution must include the ability to schedule scan blackout windows to prevent scanning during prohibited hours.
The solution must support logical organizations with full separation of data between different organizational customers.
The solution must provide the ability to define restricted ranges of IP addresses for each tenant.
The solution must provide the ability to restrict workflow permissions to include accepting and recast risk of vulnerabilities.
Elevated privileges for DB users/login such as DB owner will have to be checked by the supplier so that all DB users will conform to the principle of least privilege.
No one shall have access on the system directories that contains database binaries / database files / database backups / database scripts except system and database administrators OS user accounts.
Application administrator/owner should be able to run, operate and administer the application without the need of "Administrator/root" and DBAs OS user account.
<b>DISTRIBUTED SCANNING</b>
The solution must support a variety of scan engine platforms to include Windows, Linux, macOS, ..
An optional externally hosted scanning service that is PCI ASV must be available for scanning perimeter networks.
The solution must support multiple geographically or logically distributed scanning engines managed by a central console.
The solution must support load balancing and failover across multiple scanners by dynamically distributing the scanning load between scanners based on scanner availability throughout the entire scan job. Describe load balancing strategy used by the solution .
The solution must provide the ability to deploy additional scanners throughout the environment at no additional cost.
The solution must provide the ability to configure ports, protocols, and services for connections to scanners deployed throughout the network.
The solution must be configurable to allow for scan throttling to prevent generation of sufficient traffic to disrupt normal network infrastructure.
The solution must provide the ability to support offline scanning and importing results in the server.
The solution must allow for entry and secure storage of user credentials, including Windows local and domain accounts, and Unix su and sudo over ssh.
The solution must provide the ability to escalate privileges on targets from normal users to root/administrative access.
The solution must support an unlimited number of "ssh" credentials.
The solution should support the integration with privileged access management (PAM) solutions, such as CyberArk, BeyondTrust, Thycotic, PrivX and Lieberman for credential management.
<b>COMPLIANCE &amp; AUDITING</b>
The solution must be capable of authenticated and non-authenticated compliance auditing without the need for a client-side agent installed on the target device.
The solution must provide a consolidated view of all vulnerability and compliance auditing results.

The solution must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and vendor best practice standards. List the benchmarks supported.
The solution must provide security and configuration auditing benchmarks for vendor best practices such as Microsoft, Cisco, and VMware. List the best practice benchmarks supported.
The solution must provide auditing of VMWare ESXi and vCenter using the VMWare SOAP API.
The solution must provide auditing of Microsoft operating systems for security and configuration settings. List the operating system vendors and versions supported with available benchmarks.
The solution must provide auditing of all major Unix operating systems for security and configuration settings. List the operating system vendors and versions supported with available benchmarks.
The solution must provide auditing of databases for security and configuration settings. List the database vendors and versions supported with available benchmarks.
The solution must provide auditing of applications for security and configuration settings. List the application vendors and versions supported with available benchmarks.
The solution must provide auditing of network infrastructure for security and configuration settings. List the network infrastructure vendors and versions supported with available benchmarks.
The solution must provide auditing of specific endpoint security solutions for installation and boot status. List the endpoint security products and versions supported with available benchmarks.
The solution must provide auditing of personally identifiable information (PII) and other sensitive content. List the content auditing benchmarks available.
The solution must allow audit policies to be customizable for organizational specific needs.
The solution must provide CIS Certified Benchmarks.
The solution must be NIST SCAP 1.2 Validated.
The solution must be capable of running DISA STIG compliance audits.
<b>WORKFLOW, AUTOMATION, and TICKETING</b>
The solution must provide full automation of scanning, reporting, and alerting.
The solution must provide separate views for active, passive, compliance, and mobile vulnerabilities.
The solution must aggregate the results of individual scans into cumulative vulnerability views with filtering and analysis to allow drilldown and pivot capabilities.
The solution must have separate views of active and mitigated vulnerabilities with automatic migration of vulnerabilities from active to mitigated once a scan determines that the vulnerability is no longer present.
The solution must have the ability to flag a vulnerability as having been previously mitigated, but which has appeared again as might happen when a system is restored from backup or an old copy of a virtual machine is brought back online.
The solution must provide comprehensive filtering of aggregate vulnerability results with drilldown capabilities.
The solution must provide a comprehensive view of plugins with the ability to filter plugins by family type
The solution must provide attack path analysis.
The solution must have a tagging ability to label assets, policies, credentials or queries with a custom description to improve filtering and object management.

The solution must provide remediation views that are automatically prioritized and streamlined for the IT and OT audience.
The solution must provide the ability for approved users to run remediation scans to verify vulnerabilities have been addressed correctly.
The solution must provide the ability to automatically group targets together using scan results to generate dynamic asset lists.
The solution must allow a user to accept risk (make an exception) with configurable expiration dates of a detected vulnerability, or to recast risk (change severity levels) to a level other than what the vendor defined for that vulnerability.
The solution must provide ticketing functionality and the ability to integrate with 3rd party ticketing systems.
The solution must support assigning tickets to individual users.
The solution must provide alerting capabilities for vulnerabilities and events.
The solution must support the definition of alerts based on vulnerability scan or configuration audit results.
Alert actions must include: customizable email with multiple context variables, creation of a ticket, initiation of a scan, generation of a syslog event, report generation and notify users.
<b>REPORTING</b>
The solution must support the generation of customized reports either using vendor supplied templates or without templates.
The solution must provide the ability to filter results in reporting by a variety of criteria to include asset lists, repositories, addresses, vulnerability types, raw text, and date fields.
The solution must provide integrated reporting of scanning, sniffing.
The solution must provide the ability to fully automate reporting to include scheduled report execution and delivery and post-scan report delivery.
The solution must provide the ability to produce ad hoc reports while viewing results in the console. i.e: Mean Age of Open Vulnerabilities, Mean Time to Patch (MTTP)—Critical Vulnerabilities, ..
The solution must support the ability to produce reports in the following report formats: PDF, CSV, XML
The solution must provide customizable trending of scan results in reports using filtered results to define multiple trend lines in a single graph.
The solution must provide matrix tables that summarize numbers across many filtered sets of results.
The solution must provide an automated reporting feed of templates for security and compliance themes.
The solution must provide regulatory compliance reporting at no additional cost.
The reports must have the ability to include hostnames (NetBIOS, DNS) along with IP addresses.
The solution must provide the ability to encrypt and password-protect reports.
The solution must provide the ability to automatically email reports.
The solution must provide the ability to push reports using web-publishing services.
The solution must allow customized images to be uploaded for report customization.
<b>DASHBOARDS</b>
The solution must provide high-level report cards of security metrics and compliance.

The solution must include customizable graphical and list based dashboard elements for displaying vulnerabilities and status of the assessed environment.
The solution must provide customizable trending of scan results in dashboards using filtered results to define multiple trend lines in a single graph.
The solution must allow each user to define multiple user-specific dashboards.
Dashboard elements must be fully customizable by filtering to display data based on asset list, vulnerability or compliance checks, time, key word search, IP address, etc.
The dashboards' refresh rates must be configurable to update on scheduled and ad hoc basis.
The solution must provide the ability to import/export the dashboard and reporting templates.
The solution must provide the ability to define various visual elements for customized dashboards to include pie charts, bar charts, matrix, and trending.
The solution must provide the ability for users to share dashboards.
The solution must provide a dashboard feed that includes templates that are themed around different audiences, compliance standards, and security controls.
The solution must accommodate customizable layout and formatting options for dashboards.
<b>Implementation / Installation &amp; Migration</b>
Successful bidder will be responsible for supply, install, configure, customize and fine tune the Solution according to MIC1 ( Alfa) requirements;
All installation that will be performed shall be performed by certified engineers and under the vendor's supervision.
Partnership level: The Bidder should provide documents proving that he is certified to sell, implement, and support the proposed systems and solution and that he has acquired the highest expertise implementation and support level .
Reference List: the Bidder shall provide a reference list for similar installations that have been performed by his team and are still being supported by the bidder
Contractor shall provide and install during the Warranty/support period all updates and upgrades which occur as a result of continuous improvement or enhancements
Contractor shall provide the detail of the computing resources needed (CPU, MEM, Network) for the optimal performance of the solution.
The Bidder shall provide a data flow diagram along with the accesses required between the proposed solution and MIC1 already existing systems. The purpose is to update the internal access-lists to allow the normal traffic flow for the solution. It will be MIC1s responsibility to apply the needed access restrictions on the existing network infrastructure in terms of routers, firewalls, or IPS. The bidder shall clearly list any concern or special requirement regarding this point.
Bidder shall specify if access to the internet is required. In the positive case, the possibility of configuring proxy settings for the proposed application is a must.
Bidder shall provide detailed SOW for the implementation
<b>Warranty, Maintenance and support</b>
Bidder shall provide a warranty for 1 year (12 months) after the successful implementation of the solution Based on 24/7; Warranty period shall start from the date of acceptance
System support should be provided on 24/7 basis.

Warranty/support: any failure, defect or problem in the Solution provided for MIC1 (Alfa) is considered as critical and supplier shall remedy to that failure in terms of labor & parts and restore the service within 4 to 6 hours of placing the service call. Each time the resolution is not implemented within 4 to 6 hours the bidder will be subject to a penalty of 2% from total amount of the project.
The New Releases Upgrade, Update and compatibility resolving issues shall be at no extra cost and shall be deemed part of the services provided under this Contract
The warranty / support of the solution shall start after the final acceptance date.
The Bidder must have a back to back support agreement with the vendor that enables him escalate immediately any issues he fails to remedy during the installation or warranty period as specified below . Bidder shall provide proof of this back to back agreement
Contractor shall install and provide MIC1 (Alfa) with all new versions and release of the Solution software which occurs as a result of continuous improvement or enhancements
<b>Integration and Extensibility</b>
The Solution should be Support for RESTful APIs. APIs facilitate integration with other security and IT systems, streamlining workflows.
The Solution should be able to integrate with other security solutions (e.g., SIEM, IDS/IPS) to provide a holistic security view.
<b>Data Privacy and Security</b>
Implementation of data encryption in transit and at rest to safeguard sensitive data.
<b>Backup and recovery</b>
Vendor should provide the adopted backup strategy and its related documentation noting that all backups to disk should be taken on a separate partition.
The vendor shall give details about the backup needed for system and database if any (Backup size and window) as well as the retention policy for the backup to disk (at least 2 full backups should be available on disk).
Vendor should provide the adopted recovery process and its related documentation. Backup should be configured in a way that doesn't tolerate any loss of data for any type of failure. Full recovery time and data loss should be specified.
<b>Training</b>
Bidder shall include in his offer the necessary vendor certified trainings on the proposed solution. Cost shall cover cost of training, travel and accommodation for (2 persons) if training is not available locally . This training shall take place before the implementation
Training details (course name, location, etc.) should be included in the technical offer
Bidder shall also provide hands on training during the implementation of the project
<b>Documentation</b>
Bidder shall provide detailed documentation related to design, functional, operational and maintenance aspects of the solution

## Article 11: Information Security Specifications

- The Bidder shall commit to refrain from offering any product / equipment which can cause security threat or information leakage that jeopardizes MIC1 network security. (K)
- The Bidder shall accept that MIC1 runs a vulnerability scan on the proposed solution prior to issuing the acceptance and in case any vulnerability is found, the Bidder undertakes to take the necessary actions to remedy such vulnerability within \_15\_ days from its notification. (K)
- The Bidder shall mention the security standards adopted/followed in designing the proposed solution.
- The Bidder should specify if it has acquired the ISO27001 certification or any other equivalent security certification and submit with the Offer a copy of such certificate.
- The Bidder shall not hard code passwords in the proposed solution. (K)
- The provided application should run without the need of root (unix) and / or admin (win) privileges.
- System shall allow generation of user, operator as well as alarms logs. (K)
- Solution and storage shall be sized to host history logs for at least 1 year back. The Bidder shall change default errors / messages and configuration.
- Application should support role-based access, specific privileges per user (i.e specific access to application modules and reports)
- Database should support restricted access per user or groups to data (i.e access per field or per table, ...)
- Encryption shall be used in all communications / interactions between systems, especially if the communication is through web access. Web based access shall always be used through HTTP+SSL. (K)
- Each user shall have only one account / profile to access data.
- Least-privileges should always be specified on nodes / applications.
- The Bidder should commit to improve solution / systems information security weaknesses whenever needed or highlighted by MIC1 information security team. (K)

## Article 12: Evaluation of Offers

MIC1 reserves the right to accept or reject any or all Offers at its absolute discretion and without thereby incurring any liability to the affected Bidder / Bidders and / or any third party, or any obligation to inform the affected Bidder / Bidders of the grounds for MIC1's action.

The RFT does not bind in any way MIC1 which reserves the right to study the Offers, and to conclude PO/contract negotiations in relation to the RFT, in its totality or parts thereof, with any or several Bidders, as it sees fit and at its sole discretion. MIC1 also retains the right to enter into a contract or to issue PO only for parts of the offered solution.



Further to what is mentioned above, no Bidder may file any claim whatsoever against MIC1 or may claim any compensation from the latter based on the rejection of its Offer or on any ground whatsoever in relation to the RFT.

The Technical and Commercial/Financial Offers are opened sequentially, so that the evaluation of the Technical Offer will precede the evaluation of the Commercial/Financial one. Bidder selection is based on the combined results of the technical and commercial evaluations.

Although due consideration will be given to MIC1's general principles and criteria, including economy and efficiency, MIC1 does not bind itself in any way to select the Bidder offering the lowest price.

## **Article 13: Entering into Contract**

MIC1 shall enter into a contract with the selected Bidder for the services requested under the RFT and shall issue a PO to the selected Bidder in this regard, as the case may be.

At all times, the terms and conditions of said contract/PO shall be defined in accordance the RFT.

MIC1 is operating the Mobile Network for the benefit of the Republic of Lebanon and therefore, in case MIC1 enters into any contract with or issues a PO to the Bidder, this will be for the benefit of the Republic of Lebanon.

## **Article 14: Termination and Assignment**

At any time, MIC1 shall have the right at its sole discretion to cancel the RFT process or terminate the PO/contract with the selected Bidder, with immediate effect, without the need for any judicial or extra-judicial proceedings and such termination shall not entitle the Bidder to any compensation or indemnity whatsoever.

It is to be highlighted that any PO/contract is de facto terminated if the Republic of Lebanon / Ministry of Telecommunications requests its termination. Such termination shall have an immediate effect, and shall be effective without the need for any judicial or extra-judicial proceedings and such termination shall not entitle the Bidder to any compensation or indemnity whatsoever.

MIC1 shall have the sole discretionary right to assign at any time and with immediate effect the PO/contract to the Republic of Lebanon or any designee assigned by the Republic of Lebanon to manage the first mobile network in Lebanon.

## **Article 15: Boycott of Israel Requirement**

Bidder is informed of, and undertakes to abide by, the legal requirements of the Republic of Lebanon concerning the Boycott of Israel in accordance with the law dated June 23rd, 1955.

Therefore, Bidder shall not hold Israeli nationality, or be domiciled in or resident of Israel, or work for it, directly or indirectly, or represent or act for, in any way, directly or indirectly, the interests of Israel or an Israeli entity. Bidder shall not have any main or branch factories or assembly plants or offices in Israel and shall not participate in any Israeli business. Bidder shall not license its name, trademarks, manufacturing or technological patents to any Israeli individual or entity and shall not provide any technological assistance to any Israeli business.



In addition, no person holding Israeli nationality or domiciled in or resident of Israel or working for it directly or indirectly or representing or acting for, in any way, directly or indirectly, the interests of Israel or an Israeli entity may be employed or used, in any way, directly or indirectly, by the Bidder in the project subject to the RFT. Bidder is explicitly obliged to take into consideration this requirement in the allocation and management of its personnel resources, employees, contractors and subcontractors for any activity or solution or mean whatsoever linked to Israel and contributing to the project subject of the RFT.

Any time the Bidder violates such requirements and / or any direct or indirect relation between the Bidder and Israel is brought to MIC1's knowledge, MIC1 shall immediately exclude the Bidder from the RFT process or terminate the PO/contract without the need for any judicial or extra-judicial proceedings and without incurring any liability whatsoever to the affected Bidder / Bidders and / or any third party.

## **Article 16: Applicable Law and Dispute Resolution**

All disputes, which might arise from the validity, interpretation, implementation, or termination of the RFT, shall be exclusively settled by the competent Courts of Beirut in Lebanon.

The RFT shall be governed by and construed in accordance with the applicable Lebanese laws.