REQUEST FOR PROPOSAL

“PENETRATION TESTING PROJECT”

ATOMA/RFP#A25007

Date: September 30, 2025

Table of Contents

1. Introduction

ATOMA Telecom is a leading mobile operator in Afghanistan. We deliver innovative and reliable telecom services to empower individuals and businesses. Our mission is to bridge the digital divide and drive Afghanistan's connectivity forward. With a focus on quality and growth, we are expanding our 4G network across the country. With our experienced team, we're building a modern digital ecosystem. At ATOMA, we value talent, innovation, and progress. Join us in shaping the future of telecommunications in Afghanistan.

2. Purpose

ATOMA is seeking proposals from qualified vendors for a comprehensive penetration testing project and crisis simulation testing to assess our cybersecurity defenses. This initiative aims to address potential vulnerabilities and enhance our incident response capabilities against various cyber threats, including data breaches, malicious insider attacks, ransomware attacks, and phishing attacks.

The scope of this project includes:

- Penetration Testing:
- Two mobile applications (Android and iOS)
- 173 API
- Five web applications
- API Testing
- 173 API
- Forty-five host/node (intrusive test of a mix of Linux and Windows).

The goal is to identify vulnerabilities, assess risks, and evaluate the organization's preparedness and response capabilities during cyber incidents.

3. Objective

The primary objectives of this engagement are:

- Identify and exploit vulnerabilities in the defined scope.
- Assess the potential impact of identified vulnerabilities.
- Evaluate the organization's incident response and crisis management capabilities.
- Provide detailed remediation and improvement recommendations.
- Ensure compliance with industry standards and best practices (e.g., OWASP, NIST, ISO 27001)

4. Scope of Services ("Scope of Work")

The penetration testing engagement shall cover a comprehensive assessment of the organization's digital assets, with a focus on identifying security vulnerabilities, validating controls, and simulating real-world attack scenarios. The scope includes, but is not limited to, the following areas:

- 4.1 Penetration Testing Activities
- 4.1.1 General Methodology:
- Conduct both external and internal penetration testing.
- Utilize a combination of automated tools and manual testing techniques to ensure thorough coverage.

- Follow established security standards and frameworks such as OWASP, NIST SP 800-115, PTES, and MITRE ATT&CK where applicable.
    - 4.1.2 Mobile Applications
    - Number of Applications: 2
    - Platforms: Android and iOS
    - Testing Types:
    - Static Application Security Testing (SAST) – review of source or compiled code for vulnerabilities.
    - Dynamic Application Security Testing (DAST) – runtime analysis of application behavior.
    - Authentication and Authorization Testing – assess session handling, role-based access control, and token management.
    - Data Security – test secure storage, encryption, and secure transmission of sensitive data.
    - Reverse Engineering & Binary Analysis (where applicable) – detect obfuscation weaknesses, hardcoded secrets, and logic flaws in compiled code.
    - 4.1.3 Web Applications
    - Number of URLs: 5
    - Testing Types:
    - Assessment against OWASP Top 10 risks.
    - Evaluation of authentication and session management mechanisms.
    - Identification of input validation issues, including XSS and injection flaws.
    - Review of output encoding and sanitization practices.
    - Detection of business logic flaws and insecure workflows.
    - Identification of security misconfigurations and exposed sensitive information.
    - 4.1.4 API Security Testing
    - Number of API Endpoints for web: 169
    - Number of API for mobile: 173
    - Testing Approach:
    - Testing aligned with OWASP API Security Top 10.
    - Authorization testing (e.g., broken object-level authorization, IDOR).
    - Authentication testing (e.g., improper token handling, credential stuffing resistance).
    - Input validation, rate limiting, and error handling.
    - Analysis of data exposure via verbose responses or improper filtering.
    - Evaluation of encryption in-transit and at-rest.
    - 4.1.5 Operating Systems
    - Number of Systems: 45
    - Testing Approach:
    - Vulnerability discovery via authenticated and unauthenticated scanning.
    - Exploitation of known vulnerabilities for validation.
    - Privilege escalation and post-exploitation techniques.
    - Enumeration and testing of exposed network services, open ports, and running daemons.
    - Misconfiguration and patch management analysis.

5. Deliverables

The vendor is expected to provide the following deliverables:

5.1 Pre-Engagement Documentation

- Detailed testing plan and methodology.
- List of tools and techniques to be used.
- Signed Non-Disclosure Agreement (NDA) and Statement of Work (SOW).
- 5.2 Testing Phase
- Regular status updates and communication.
- Immediate notification of critical vulnerabilities or incidents.
- 5.3 Post-Engagement Documentation

Penetration Testing Report:

- Executive summary.
- Methodology and tools used.
- List of vulnerabilities (categorized by severity: Critical, High, Medium, Low).
- Evidence of exploitation (screenshots, logs, etc.).
- Risk assessment and impact analysis.
- Remediation recommendations.

Crisis Simulation Testing Report:

- Executive summary.
- Scenarios simulated and objectives.
- Observations and findings (e.g., detection time, response effectiveness).
- Gaps in incident response and crisis management.
- Recommendations for improvement.
    - Retesting Report (if applicable):
- Results of retesting after vulnerabilities are remediated.

6. Vendor Qualifications

Interested vendors must demonstrate the following qualifications:

- Proven experience in conducting penetration testing and crisis simulation testing.
- Certified professionals (e.g., OSCP, OSCE, CEH, CISSP, GPEN, GCIH).
- Familiarity with industry standards and frameworks (e.g., OWASP, NIST, PTES, MITRE ATT&CK).
- Strong references from previous clients.
- Ability to work within the defined timeline and budget.

7. Requirements Process

7.1 Participation in RFP

Suppliers willing to submit their offers should confirm by sending an Intent to Respond through an email to ATOMA procurement team sadeequllah@atoma.com.af, asahibzada2@atoma.com.af,

7.2 Apology

In case the requested items are not available, or you do not want to participate in this bid, you are kindly requested to respond by submitting a written apology indicating the reason and the bid reference number to sadeequllah@atoma.com.af, asahibzada2@atoma.com.af, no later than the bid closing date indicated in section

7.3 RFP Schedule

Milestone	**Date/Time**
RFP issuing date	August 31, 2025
Deadline for Bidders' inquiries	Sept 04, 2025
Answers to Bidder's inquiries	Sept 05, 2025
Pre-Bid meeting	No needed, referred to the end user
Deadline for receiving offers	September 10, 2025

7.4 Submission Date and Time

Offers must be submitted on or before: **September 10, 2025**

No bids shall be accepted after the specified submission date or outside specified hours.

7.5 Submission Address

Offers must be submitted to ATOMA main office or through emails which shall be password protected to be the below email address: sadeequllah@atoma.com.af, asahibzada2@atoma.com.af,

Offers submitted by hand or via post mail shall be enclosed in a sealed envelope clearly marked the RFP number.

In the event that ATOMA offices are officially closed on the date the proposals are due, the deadline for submission shall be automatically extended until the next business day.

Bids submitted by, or erroneously sent directly to other departments other than the Procurement/Bid team, will not be considered or even acknowledged.

7.6 Proposals Submission

a. Financial and technical proposals should be separated and include a reference number, each in a sealed envelope with an additional copy for each. Documents need to be

signed by an authorized representative of the supplier. Each page must be initialed, and the final page must be signed and dated.

b. Soft copies of the proposed offer (Technical) EXCLUDING PRICED and another one (Financial) INCLUDING PRICES with all proposal documents including catalogues (Formatted in MS Word, Excel) should be presented on the CD accompanying the submission.
   Any submitted proposal that doesn't include complete soft copies as indicated above will be subject to possible disqualification.

c. Proposal may be submitted by hand, mail or by means of e-email attachments in MS work or Excel format, to sadeequllah@atoma.com.af, asahibzada2@atoma.com.af, before the closing date (please refer to Section 7.3 for submission address). However, the confidentiality of electronic submissions through emails cannot be guaranteed by ATOMA, unless encrypted.

d. Bids must be submitted in sealed envelopes on which the bid reference number and bidder's name shall be shown clearly. The envelope should be sealed with the stamp of the bidder on the back or where appropriate.

7.7 Clarification and Questions

- All communication regarding this RFP must be directed **exclusively** at the Procurement and Contracts Administration Department. No other ATOMA representative is authorized to discuss or provide guidance related to this RFP. ATOMA will not be responsible for, and bidders must not rely on, any verbal or written statements made by unauthorized persons.
- Each bidder is responsible for thoroughly reviewing the RFP and identifying any uncertainties, inconsistencies, errors, or ambiguities. Bidders must conduct their own investigations and due diligence in preparing proposals.
- Questions must reference the relevant **section number** and **page** of the RFP.
- All questions should be submitted **in writing** prior to the bidders' conference by email to: sadeequllah@atoma.com.af, asahibzada2@atoma.com.af
- Clarifications will be addressed during an **online bidders' conference**. Details (date, time, access link) will be provided at bid launch. Bidders are strongly encouraged to attend. Registration is required by email to **procurement_atoma_.af@atoma.com** .
- The Procurement and Contracts Administration Department will prepare and circulate official **minutes of the pre-bid meeting**, including all clarifications, questions, and answers.

7.8 Supplier Checklist

Each bidder must submit the following information and documents. **Failure to provide any item may result in disqualification.**

Requirement	**Details**
a. Detailed Proposal	Complete and detailed offer in accordance with the RFP.
b. Firm Qualifications & Experience	i. General overview and history of the firm.
	ii. Office location(s) and number of employees allocated to this project.
	iii. ATOMA reserves the right to request replacement of any resource deemed unsatisfactory.

c. Staff Qualifications & Expertise	i. List supervisory and management staff (partners, managers, supervisors, specialists).
	ii. Provide resumes of proposed team members.
d. Relevant Engagements	i. List significant past engagements of similar size/scope.
	ii. Provide references from at least **3 customers** willing to meet ATOMA management.
e. Quality of Service	i. Approach and methodology to deliver scope of work.
	ii. Commitment to availability throughout the contract.
f. Cost Proposal	i. Detailed cost/pricing, including all project components.
	ii. Any perpetual or subscription-based license costs.
	iii. Separate **technical and financial bids**.
	iv. Man-hour estimates for out-of-scope requests.
g. Solution Demonstration	Shortlisted bidders must provide a live demonstration of proposed remote services.
h. Supporting Documents	Provide all relevant datasheets.

THE END