NATIONAL MARITIME SAFETY AUTHORITY
INFORMATION & COMMUNICATION TECHNOLOGY DEPARTMENT

Terms of Reference (ToR)

Windows Server 2012 Active Directory Upgrade
And
Microsoft Exchange Server 2016 Upgrade

1   BACK GROUND

Papua New Guinea (PNG) is a member state of the International Maritime Organization (IMO) whose key responsibilities are to provide machinery for cooperation among Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation and prevention and control of marine pollution from ships".

The National Maritime Safety Authority (NMSA) was established by an Act of Parliament in 2003. NMSA is the autonomous statutory authority responsible for all maritime safety needs of the general public, especially those in isolated coastal communities, the maritime industries and their customers. Its purpose is to regulate the maritime safety standards, coordinate Search and Rescue operations and control marine pollution in PNG waters. NMSA also fulfills Papua New Guinea's obligations under international conventions through implementation of national and international maritime laws.

To ensure efficient and effective maritime administration NMSA has embarked on projects to improve its operations which include upgrading its Information and Communications Technology systems and infrastructure.

The Authority is inviting suitably qualified companies to express their interest to assist NMSA ICT in the installation, configuration and support of Windows Server 2012 Active Directory and Microsoft Exchange Server 2012.

2   TASK DESCCIPTION

This project will be accomplished in phases as per the requirements of the Finance and Administration Department.

Project/Task:	To engage suitably qualified ICT companies to design, build, configure, implement and support Windows Server 2012 Active Directory Forest.
Executing Agent:	National Maritime Safety Authority (NMSA)
Implementing Body:	ICT Department
Project Sponsor:	General Manager/CEO – National Maritime Safety Authority
Project Location:	NMSA Head Office, Level 2 Pacific MMI Building, Port Moresby
Closing Date for Bid:	COB 25th August 2017
Commencement Date:	To be determined
Project Duration:	One (1) Month

3   OBJECTIVE

The specific objectives include:
- Improved Security across the servers and the network;
- Better management and allocation of resources on the servers and network
- Improved security from external intrusion and attacks on servers
- Higher Capacity Servers and high level of availability

4   SCOPE OF WORKS

NMSA has a virtualised server environment on a VMware platform (ESXIi 5.5) with two physical Dell PowerEdge R720 servers hosting fourteen (14) virtual servers all running Windows Server 2008 R2. NMSA also has 3 other physical servers running Windows 2008 R2 that will also be upgraded.

Work for this project includes;
- A) Clean up AD environment
- B) Backup AD environment and all servers
- C) Design AD and Server Architecture and design
- D) Test AD and Server Architecture and design
- E) Implement/Migrate AD
    1. Upgrade of Active Directory (Domain controllers, DHCP, DNS)
    2. Upgrade of File Servers
    3. Upgrade of Application Servers
        - a) CRM (SQL)
        - b) Ship Registry (SQL)
        - c) Exchange
        - d) SharePoint
    4. Upgrade of Security Server
    5. Upgrade of Printer Server
    6. And other servers
- F) Post Implementation Support
- G) Project close-up

All servers running Windows Server 2008 R2 must be upgraded to Windows Server 2012 R2. A list of the individual servers to be upgraded will be provided to the approved service provider.

5   WORK SCHEDULE

A detailed road map for the project must be submitted along with the proposal, which will be used as progress assessment tool.

6   TECHNICAL REQUIREMENTS

The proposed design of the AD environment must take into account existing setup and recommendations made in the AD Review Report provided in **ToR Annexure I**.

7   SECURITY REQUIREMENTS

The service provider shall adhere to the following security requirements:
- The service provider will create and use IDs and passwords in accordance with NMSA naming conventions;
- The service provider will provide all IDs and credentials to NMSA ICT Department upon completion of project;
- The service provider will ensure security of AD is maintained and any changes must be done in collaboration with NMSA.

9   DELIVERABLES

- Preliminary checks and preparation of AD Environment
- Server and Active Directory architecture design document; (must be in Proposal)
- Test setup for all servers, systems and services in test environment;
- Migration of AD and Go Live;
- Project Completion Report and As-Built documentation submission.

10   RESPONSIBILITY

NMSA
- Shall ensure daily updates are reviewed and comprehensive requirement specifications are provided within review period;
- Shall maintain the delay register and notify the service provider of all delays in writing;
- Shall appoint the point of contact or project focal person (s);
- Inform the stakeholders and arrange joint sessions with consultants.

Service provider
- Shall ensure timely delivery of deliverables;
- Shall provide the AD design and schema acceptable to NMSA; and
- Shall appoint a project manager who shall be the point of contact.

11   ELIGIBILITY CRITERIA

    The service provider
- should be primarily an IT Company with experience in Server Infrastructure and System Administration projects with Dell, HP, IBM and others.
- must be fully committed to undertake this engagement in accordance with the scope of work defined and any instructions issued by the CEO and the Board, where necessary.
- will maintain professional independence throughout the duration of the engagement.
- must be registered, as required by the provisions of the Companies Act 1997, must be in compliance with the guidelines of the Companies Regulations 1998, the Investment Promotion Act and the Internal Revenue Commission.
- should have successfully completed at least three projects of similar nature in past five years and vast experience in server architecture design and implementation. (The details of such jobs should be furnished.)
- Service provider must prove their qualifications concerning the following criteria:
  - Ability to fulfil and abide by the terms and specifications;

- The service provider must have technically qualified, skilled and competent personnel with certifications in Microsoft systems necessary to be able to perform the engagement. Copies of certifications and CVs can be provided to support EOI; and
- Experiences in similar projects are relevant and the vendor must be able to demonstrate these experiences. The vendor must provide evidence of similar.

- Service provider shall not be under a declaration of ineligibility for corrupt and fraudulent practices issued by the Government of PNG (GoPNG)/Provincial Governments / Regulatory agencies.
- NMSA reserves the right to carry out the capability assessment of the Suppliers and its decision in this regard shall be final & binding to all.
- Upon award of contract, the successful Service provider shall sign an agreement with NMSA within **7** days.
- NMSA will provide all required licenses of Windows Server 2012, Exchange, SQL and other systems.

12   PAYMENT SCHEDULE

The payment terms of the project will be as follows:
- 30% after signing of contract
- 20% after completion of Design and Testing
- 20% after Migration and Go-Live
- 30% after project Closure and submission of As-Built-Document

13   CONTRACTUAL TERMS AND CONDITIONS

Terms and conditions are requirements that are binding upon the service provider awarded the contract and form a part of all contract documents. They communicate NMSA's expectations in regards to the supplier's performance in connection with any NMSA ICT Department purchase.

a) **Negligence:** The service provider will be responsible for any mishap during the upgrade which may occur due to negligence on the part of the supplier.

b) **Insurance:** The service provider must show proof of General Liability, Professional Liability and Property Damage insurance. This insurance must be adequate to cover claims for damages caused by the supplier(s) and must remain in force throughout the duration of the project.

c) **Termination:** The performance of work under this order may be terminated in whole or in part by the NMSA ICT Department in accordance with this provision. Termination of work hereunder shall be effected to the vendor with a "notice of Termination" specifying the extent to which performance of work under the order is terminated and the date upon which such termination becomes effective.

d) **Warranty**

   Provide support under warranty after the user acceptance signoff. During this period, the service provider is responsible for following technical support:

   - Update patches;

- Resolve technical issues;

e) **Invoices and Payments**

    a. The Service provider shall submit separate invoices as per payment schedule. Invoices must also indicate respective payment schedule description.

    b. Invoices are Mailed to:

Attn: Mrs Lena Korugl, ICT Manager, National Maritime Safety Authority, Level 2 Defens Haus, P.O Box 668, **Port Moresby**, NCD