Section IV. Terms of Reference

REQUEST FOR QUOTE FOR CONFIGURING, AND MAINTAINING A DYNAMIC MULTIPOINT VIRTUAL PRIVATE NETWORK (DMVPN) SETUP FOR MIDAS SITES IN NIGERIA FOR A 2 YEAR LONG TERM AGREEMENT (LTA)

Nigeria Immigration Service (NIS) currently operates an integrated virtual private network (VPN) over Wide Area Network (WAN) for its Migration Information and Data Analysis System (MIDAS), as part of its IT infrastructure which contribute to the enhancement of the communication among the various entry/ exit locations already connected to this network. The NIS MIDAS architecture combines the use of fiber, radio and VSAT in specific terrains to have seamless interconnections resulting in an overall network architecture design of a Star Topology combined with fiber optic and radio backhaul links.

Having already carried out the setup and configuration of a Dynamic Multipoint Virtual Private Network (DMVPN) for secured data transfer between the Nigeria Immigration Service Headquarters (NIS HQ), five (5) international airports, seven (7) state commands and their corresponding border control points (BCPs), IOM is looking for a qualified vendor to support its planned DMVPN expansion across several locations of the Nigeria Immigration Service (NIS) using IPSec and GRE in a scalable way **on a 2 Year Long Term Agreement (LTA)**

The main objective of this contract is to engage the services of a Technical Expert **on a 2 Year Long Term Agreement (LTA)** to expand on the existing MIDAS DMVPN configurations, using NIS provided network security equipment, and subnet classification with initial maintenance period of 12 months. To ensure smooth connectivity across all sites (present and future) of Nigeria Immigration Service IT infrastructure, the successful vendor will provide detailed specifications on best practices in secured infrastructure management.

TECHNICAL REQUIREMENTS FOR THE CONFIGURATION

- The new Cisco devices (Cisco ISSR 4300/ Meraki routers and ASA 5506-X/ Meraki firewalls) must be installed and configured on the same physical LAN used for the MIDAS DMVPN.
- The DMVPN router should be reachable through the internet using a public IP. **Network Address Translation (NAT) must not be deployed**.
- Where required, firewalls (Cisco ASA 5506-X/ Meraki) devices will be configured for security purposes only, in addition to the router serving as the outside communication device.
- The new DMVPN devices must be able to establish IPSec tunnels to other DMVPN hub sites and send encrypted traffic through them, to allow the IPSec protocols to and from the DMVPN router's public IP address, using ESP, GRE, IKE (UDP 500) and NAT-T (UDP 4500) protocols.
- The network configuration notes and diagrams will be pulled from the device, submitted and checked against stated compliance lists.
- The new DMVPN configuration must rely on two Cisco technologies: Next Hop Resolution Protocol (NHRP) and multipoint GRE tunnel interfaces. This should not alter the standard-based IPSec VPN tunnel, but allow for a modification of

their configuration such as;

* Protocols to use must be defined (mode, authentication and encryption, message digest algorithm, site authentication).

* The required definition and use of pre-shared secret keys during inter-site collaborations.

* Clearly define and prove that the VPN platform to be used is Dynamic Multipoint VPN.

* Clearly define IP addresses to be used for data exchange over the link.

* Define and set appropriate filter rules on the network devices (firewalls, routers, switches) over the link as required e.g. allow UDP port over 5000 for ISAKMP, allow UDP 4500 traversal, allow IP protocol 50 over ESP, etc

* Implemented protocols and configuration must be submitted in a txt format. This will be copied directly from the device to check for compliance and standards.

* Link testing will be done on a site to site basis e.g. BCP to state office, and state office to HQ.

- The network configuration notes and diagrams will be extracted from the devices, submitted, and checked against above stated compliance lists.

TECHNICAL EVALUATION (100 POINTS)

The evaluation for qualified firms shall be based on the evaluation criteria and point System specified below.

Technical Evaluation Criteria	Points
Company IT service qualification status	
Registered as a core IT service company? (**Yes – Qualified and No - Disqualified**)	
Company national/ international registration status	**10**
I. Provision of relevant registration documents with the Government (CAC, FIRS) (**4 points**). II. Company certifications/ registration with OEMs? (**Total of 6 points @ 3 points each for certification and OEM registration**).	
Proof of competence to configure a DMVPN and overall quality of proposal	**80**
I. List previous experience within the last <u>12 months</u> at configuring/ maintaining a **DMVPN**, preferably for the UN or INGOs (**15 marks for UN and 5 marks for others**). II. Verifiable proof(s) that (i) above has undergone a penetration test within the last <u>36 months</u> (**15 marks**). *<u>Note: IOM will verify all claims</u>* III. Proof of compliance to Next Hop Resolution Protocol (**NHRP**) and Generic Routing Encapsulation (**GRE**) tunnel services (**10 marks**). IV. Scalability of the solution (**5 marks**). V. Proof of a 24hx7 days support (**5 marks**).	

VI. Provision of CVs of 3 staff with a minimum of two years of experience each on VPN setup (**total of 9 points @ 3 points for relevant experience of each staff**). VII. Relevant certification for each staff – preferably in Cisco (**total of 9 points @ 3 points for relevant certification of each staff**). VIII. Technical Support and maintenance Plan (5 points). IX. Quality assurance and Risk Management methodology (**7 points**).	
Training and transfer of knowledge	**10**
I. Provision of a proposed training plan and outline for 10 people on VPN management (**total of 6 points @ 3 points each for plan and outline**). ii. Previous experience with evidence on (i) above? (**4 points if yes and 0 if no**).	
Total	**100**

An offer is declared technically valid and considered for the financial analysis if it obtains a minimum score of **Eighty (80) points**.