NATIONAL INSURANCE CORPORATION
COMPUTER DEPARTMENT

REQUEST FOR PROPOSAL (RFP)

FOR

NETWORK REDESIGN WITH A SPECIAL EMPHASIS ON CYBERSECURITY

&

SOFWARE DEFINED-WIDE AREA NETWORK (SD-WAN)

Author: Systems Analyst, NIC

LAST EDITED: 30/06/2022
ISSUED ON: 01/07/2022

TABLE OF CONTENTS

PURPOSE OF THIS RFP

The National Insurance Corporation is requesting sealed proposals from qualified vendors to assist in the development of a **new design** for the organization's computer network infrastructure and security architecture. The deliverables requested include two main phases; (1) redesign the current data network and implement the approved changes to obtain the most efficient, reliable and secured configuration, with a **special emphasis on Cybersecurity** and (2) design , implement and maintain a Software Defined Wide Area Network (SDWAN).

This RFP outlines the overall objectives and expectations of the contract and will provide NIC with the required information such that NIC can make an informed and prudent decision for the acquisition of the services and products described herein.

A final scope of work will be developed by agreement with the NIC and the proposer. The following acts only as a preliminary scope to generally communicate the expectations of the NIC. The NIC reserves the right to request any additional information, which might be deemed necessary after the completion of this document.

The qualified Vendor will need to ensure the NIC and its users are operating as desired on the Network and will need to work closely with NIC until this is achieved.

BACKGROUND

The National Insurance Corporation((hereinafter referred to as "NIC"), established under the National Insurance Act, is a statutory body of the government of Saint Lucia, that administers Social Security, providing benefits for retirement, sickness, death, maternity, disability, etc. Headquartered in Castries, with 5 satellite offices, NIC is manned by over 100 skilled workers, over the length and breadth of Saint Lucia. Additionally, the NIC either wholly owns or has a majority stake in a number of subsidiaries, namely: National Insurance Property Management Company (NIPRO), St Lucia Mortgage Finance Company(SMFC) and Blue Coral.

The mission of the NIC is:

To ensure that every St. Lucian enjoys social and financial protection and to assist in the development of our nation through the efficient collection of contributions, payment of relevant benefits, prudent management of assets, use of cutting edge technology and a cadre of highly skilled staff.

The vision: of the NIC:

An effective, transparent and financially sound institution which is customer focused, provides social protection to the St. Lucian population and plays a leading role in national development.

PROJECT DESCRIPTION

The National Insurance Corporation(NIC) relies on an efficient, resilient and secured network for the delivery of critical automated services to its clients.

Presently our main office is connected to our sub-offices(branches) through a Metro-Ethernet network.

Our subsidiaries presently operate as standalone networks and are not interconnected to the network of the NIC.

The Computer Department of the NIC, has been given the mandate to redesign and upgrade the existing core IP network and to unify it with all the subsidiaries through the utilization of an SDWAN.

The SDWAN shall be designed to achieve at least 99.99% availability, and it shall not be rendered inoperable for the purpose of routine maintenance, system software upgrades, or hardware additions.

BID EVALUATION

This section describes the guidelines that will be used for analysing and evaluating the various proposals. Although cost of the solution will be an important factor in evaluating the proposals, the need for a competent and high-quality end product is of primary importance. We will put great emphasis on the criteria which follows in evaluating the quality of the system proposed.

The bid will be assessed by NIC's Evaluation Team, which includes independent consultants.

The criteria applied will include, but not necessarily limited to the following:

- Suitability of the Proposed Solution;
- Sites with Similar Installations;
- Financial Viability of the Vendor Company;
- Currency of Technology and Architecture;
- Implementation Approach and Ease of Implementation
- Training Approach and Costs
- Vendor's Experience and Support;
- Cost of Solution;

PHASE 1 – NETWORK REDESIGN

PRESENT ARCHITECTURE

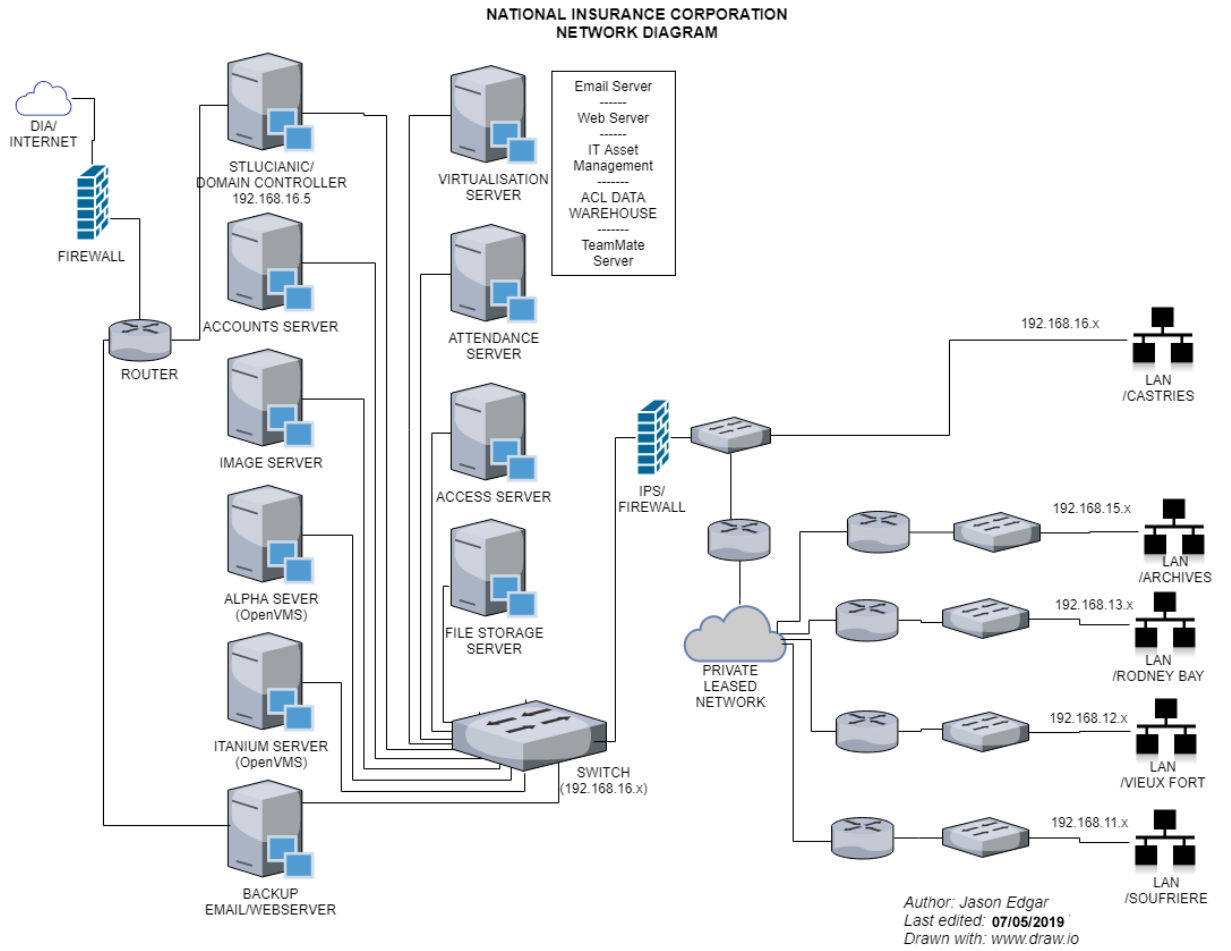

Fig 1: Existing Network Architecture

The current configuration is based on an Internet Protocol version (IPv4) network, interconnecting all departments at the NIC's primary office with other NIC suboffices across the country. Further details of the current architecture can be provided when a successful bidder has been appointed.

SOLUTION REQUIRED

DESIGN

The Network will utilize as much as possible existing network infrastructure such as switches and cabling. Qualified Vendors shall have demonstrated experience in similar successful network design/build projects and be able to provide analysis and recommendations for appropriate technology use within the Network including, but not limited to:

- High Availability Routing and General Route Management
- VLANs and Segmentation
- IP Addressing and Subnetting
- Network Security with a special emphasis on Cybersecurity
- Network Resiliency/Redundancy
- Internet Resiliency/ Redundancy
- Central Monitoring
- Central Management
- Alerting
- Quality of Service(QoS)/Traffic Management
- VPNs
- SNMP
- DHCP

DELIVERABLES

1. **Project Management**

   Vendor shall provide project coordination and management including a project kick-off meeting and weekly meetings with the NIC to monitor the progress of the project.

2. **Gather Required Network Information**

   Vendor shall make on-site visits, accompanied by NIC staff, to the primary office and suboffices to review the existing network, communications system, and devices. The on-site visits shall be used as a fact finding activity to gain an understanding of NIC's current network, use cases, and currently available assets. These visits should also be used to discover security requirements of the Network to incorporate those requirements into the design.

   The analysis of the present network architecture must also determine its suitability for the implementation of an SDWAN and to propose recommendations, if requirements not met.

Vendor shall produce a NIC Network Summary Report detailing the findings.

3. Develop Conceptual Design

Vendor shall develop a conceptual design of the NIC Network. The design shall be prepared in Microsoft Visio and will show a diagram layout of the Network. The Vendor shall identify and address any potential issues, conflicts, or impacts the project may have on existing network functionality.

4. Recommend Network Management System

Vendor shall provide a comparative and cost analysis of available Network Management System (NMS) software packages. A self-hosted solution is preferred but NIC is open to third-party-hosted solutions. The NMS Comparative Analysis will include a recommendation for the NMS package that best meets the needs of NIC's technical and management teams. The NMS will allow NIC to obtain feedback from systems on their operation and performance and provide alarm notification when problems occur. The NMS will also provide additional tools that include:

- Physical & logical views of the NIC Network
- Performance management reporting
- Fault management
- Configuration management data collection
- Device discovery processes

5. Initial Design Review

Vendor shall meet with NIC to evaluate and validate the proposed design of the NIC Network as detailed in the Network Summary Report and the NIC Network Design Diagram. This meeting will serve to validate the design and discuss recommendations of the Vendor.

Vendor shall provide an Electronic Vendor Datasheet for each piece of equipment proposed.

6. Develop Detailed Design

i. Vendor shall develop a detailed Network design and Network Equipment List to build the NIC Network.

ii. The detail design will include among other plans;
    1. VLAN Segmentation plan
    2. Routing Plan
    3. Traffic Management/Quality of Service(QoS) Plan
    4. Cybersecurity Enhancement Plan

iii. This task will draw upon the comments received during the conceptual design and review tasks to finalize the Network design.

iv. The Detailed Network Equipment List will include the IP Address scheme, a detailed specification of all equipment to be procured, including cabling, installation locations, and estimated prices.

v. A Draft Detailed NIC Network Design and Detailed Network Equipment List will be provided to NIC for their information, review, and comment.

vi. Vendor shall develop a Final Detailed NIC Network Design and Detailed Network Equipment List that addresses any comments from NIC. The Electronic Vendor Datasheet for each piece of equipment proposed shall also be included.

vii. The Cybersecurity Enhancement Plan must address the following requirements:
    - Firewall(Perimeter and Internal Firewall)
    - Endpoint Protection
    - Gateway antivirus/anti-malware
    - Intrusion Prevention and Detection(IPS/IDS)
    - Botnet Prevention
    - Phishing Prevention
    - Command and Control Prevention
    - Deep Packet Inspection
    - Threat(Virus, Spyware, DDoS, Rootkits, etc.) Detection
    - Content(including Social Media) Filtering
    - Security Analytics System
    - Access Control(rights to access all or a portion of the network)
    - Prevent unauthorized devices from connecting to network
    - Audit Logs

viii. Vendor shall provide design drawings including, but not limited to, the following:
    - Drawing – Proposed Logical Network Topology
    - Drawing – Proposed Physical Network Topology including recommendations for spares

- Drawing – Proposed security architecture showing logical firewall boundaries

7. Equipment Procurement, Staging

Vendor shall work with NIC to procure the necessary hardware to build the Network as designed. NIC may choose to purchase the equipment through Vendor, if they are an authorized reseller of legitimate equipment, or through an alternate channel. This task includes:

- Providing the NIC with a Spreadsheet - Proposed Bill of Materials
- An outline of specifications covering products and installation
- Supplying the NIC with the Electronic Vendor Datasheet for each piece of equipment proposed
- Staging and configuration of the equipment
- Registration of equipment with manufacturer for the purposes of warranty and after-warranty support
- Identification and replacement of any defective equipment prior to deployment to the NIC sites

8. **Install and Configure Network Devices**

Vendor shall install and configure the procured NIC Network equipment at each of the NIC sites.

Vendor shall develop NIC Network Record Drawings. The Record Drawings will document the installation of the Network Equipment and reflect any changes made between the Detailed NIC Network Design and implementation. The Record Drawings shall be delivered at the end of the project and must be approved by NIC for this deliverable to be considered complete.

9. Install and Configure Network Management Software

Propose and install and configure selected SNMP monitoring and Central Network Management software.

10. Perform and Support Network Testing

Vendor shall develop a test plan for the NIC Network. Test scripts shall be produced and provided to NIC for testing. The Vendor shall work with the NIC Network Administrator during the testing of the NIC Network, address and resolve technical issues.

Vendor shall record any equipment configuration changes and capture them in the NIC Network Record Drawings / Documents. All revisions to the Record Drawings / Documents shall be approved by NIC.

11. Deliver As-Built Documentation/ Hand-off

All documentation, test plans with results, and drawings must be submitted to NIC and approved.

Documentation shall include an explanation the equipment setup and overview theory of operation for the Network design.

All accounts and credentials shall be transferred to NIC at this time.

PHASE 2 – SDWAN

GEOGRAPHICALLY DISTRIBUTED LOCATION OF OFFICES

An SD-WAN is required to connect 9 remote sites. The following table provides locations of these sites.

SITE	DESCRIPTION	LOCATION
SITE A	Main office	Castries, St. Lucia
SITE B	Sub office	Vieux Fort, St. Lucia
SITE C	Sub office	Soufriere, St. Lucia
SITE D	Sub office	Gros Islet, St. Lucia
SITE E	Archives Department	Castries, St. Lucia
SITE F	NIPRO	Castries, St. Lucia
SITE G	BlueCoral	Castries, St. Lucia
SITE H	SMFC	Castries, St. Lucia
SITE I	Cloud Network Services	Cloud

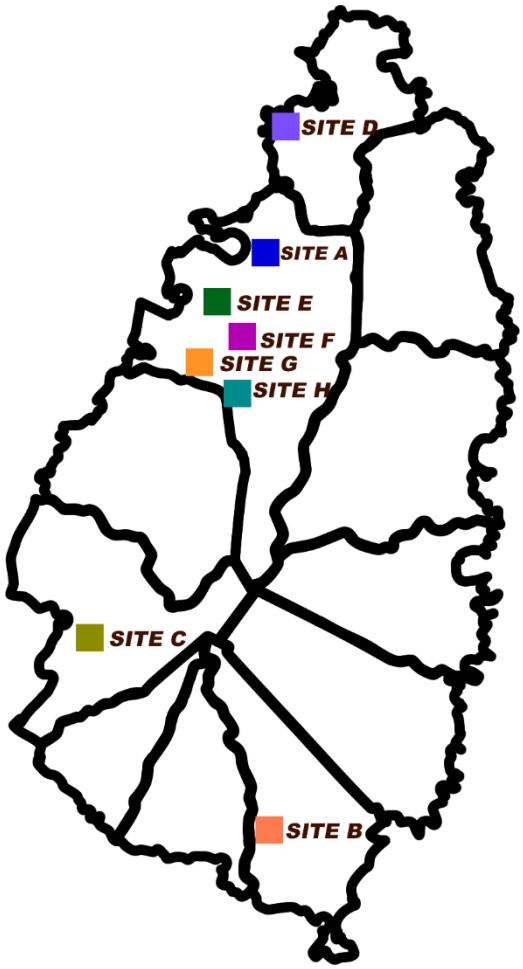

Fig 2. Map of Saint Lucia – Geographic Locations of sites

CUSTOMER PREMISES EQUIPMENT

In addition to the office sites, the SD-WAN solution must identify and provide as necessary Customer Premises Equipment (CPE) which will allow employees of the NIC and its subsidiaries to join the main network from home or other remote location.

The CPE can be physical or virtual as is required.

PRESENT ARCHITECTURE

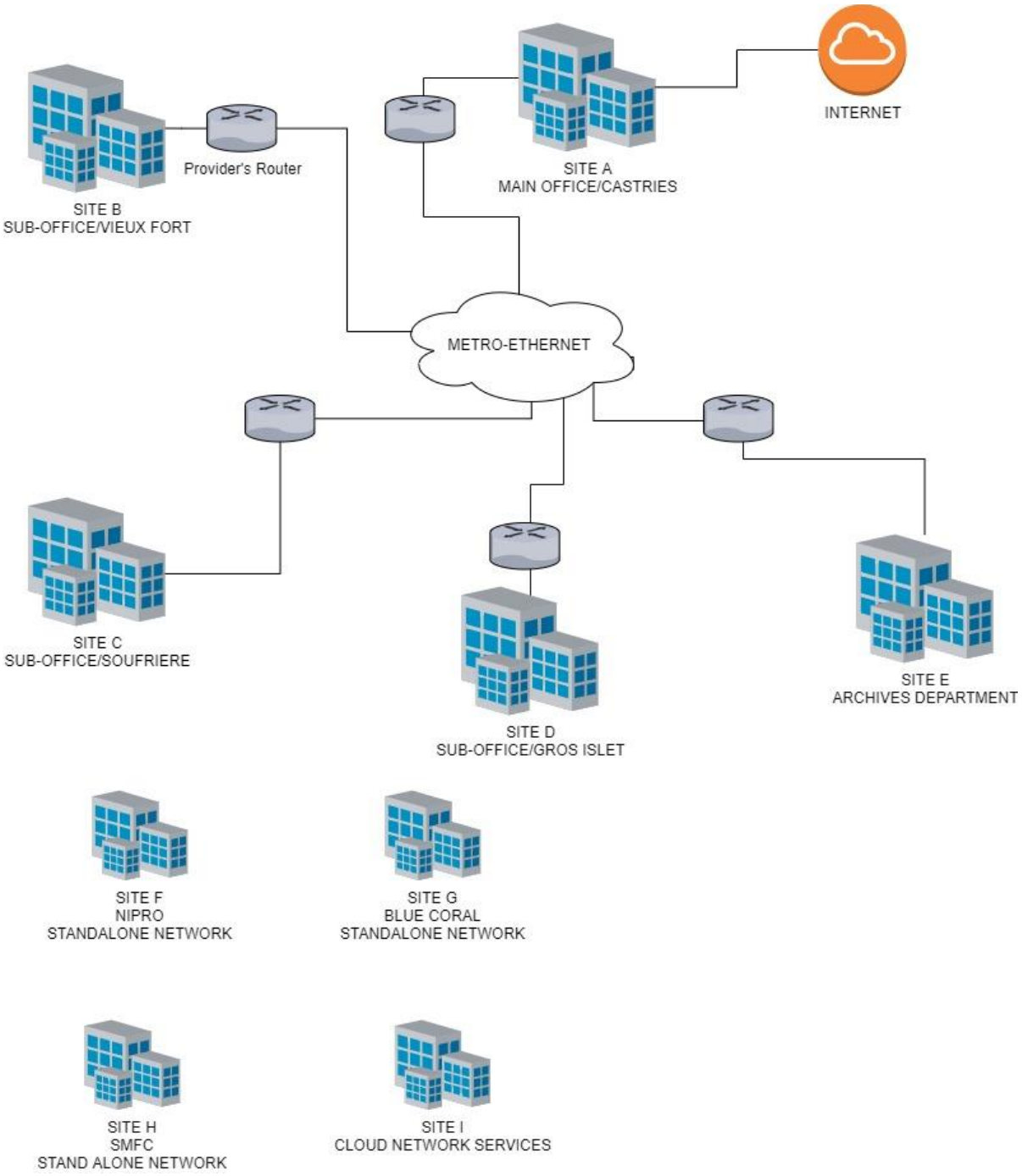

Fig 3: Present WAN Architecture

Presently, the core business services are hosted in the Main Office in Castries. The sub-offices' sites are connected to this main office through a Metro-Ethernet IP network provided by telecommunications company Cable and Wireless. Internet connectivity at the main office is through a cable broadband connection. All sub-offices receive Internet from the main office through the Metro-E network.

The subsidiaries each have their own Cable broadband connection.

SOLUTION REQUIRED

A co-managed or fully managed (by the NIC) Secure, IP-based Virtual Overlay Network Software Defined-Wide Area Network (SD-WAN) to connect all of NIC's sub-offices and subsidiaries to the Main office using a variety of WAN network technologies currently available in Saint Lucia.

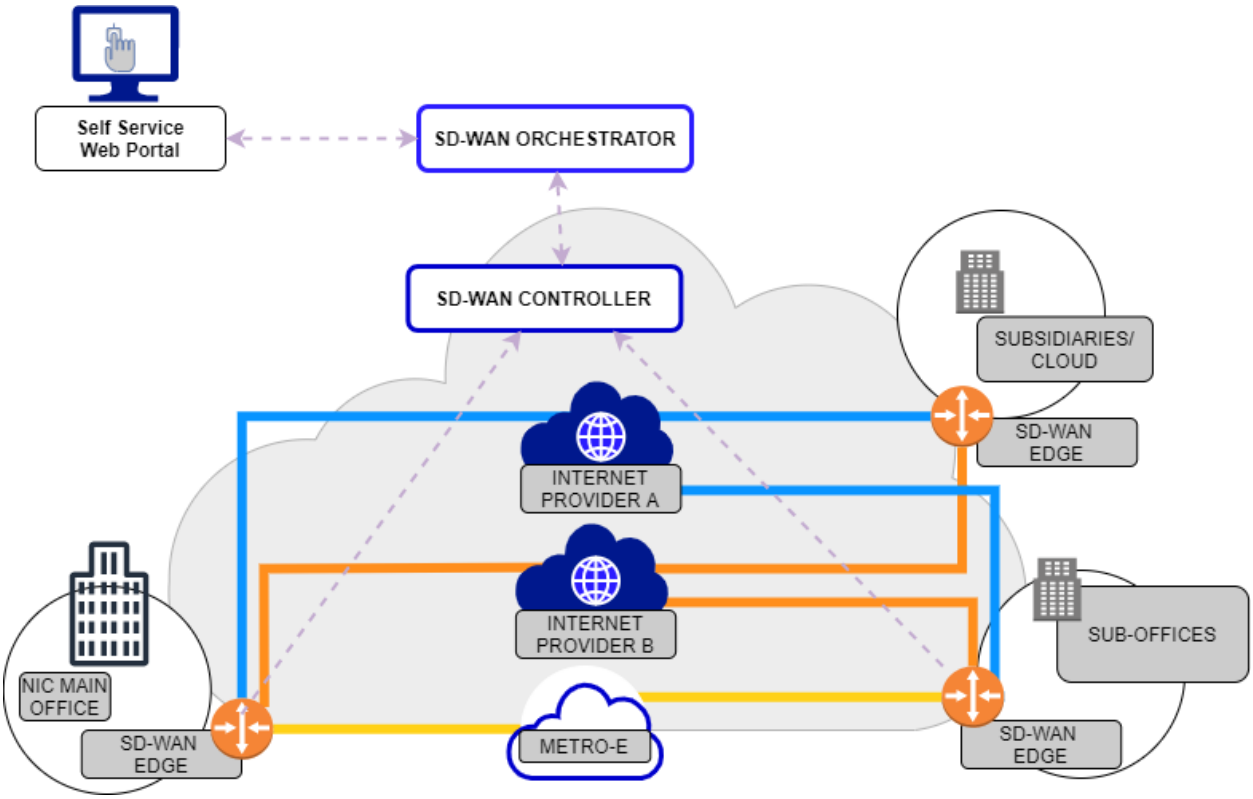

Fig 4: High-Level SD-WAN Architecture of Required SD-WAN (*Thick colored lines represent SDWAN tunnel virtual connection(TVC))*

)

Note: This diagram is for conceptualisation (reference) and illustrative purposes mainly. The proposal by the bidder does not necessarily have to match the architecture depicted in the diagram but the features and functions offered should be customised to meet as closely as possible the requirements as stated in the entire RFP.

MINIMUM FEATURE REQUIREMENTS

1. High Availability between the Main office and all other sites listed in Table 1

2. Scalability of the solution should be ensured through proper provisioning. Edge devices must have the required number of ports and throughput to facilitate the efficient transfer of business traffic. The system must also be scalable enough to allow the connection of additional sites if necessary.

3. Successful bidder has to provide all components as part of the solution to implement the project successfully.

TECHNICAL REQUIREMENTS

1. **ANALYSIS OF PRESENT NETWORK**

   An analysis of the present network architecture is required to determine its suitability for an SD-WAN. The analysis conducted in Phase 1, during the re-design of the core network, should be used for this purpose.

2. **IMPLEMENTATION OF RECOMMENDATIONS**

   Implement approved recommendations from analysis of network.

3. **SECURE, IP-BASED VIRTUAL OVERLAY NETWORK**

   The proposed SD-WAN must provide a secure, IP-based virtual overlay network using virtual tunnels over the Internet, Metro-Ethernet or other IP transport network.

4. **TRANSPORT-INDEPENDENCE OF THE UNDERLAY NETWORK**

   The proposed SD-WAN must support various data transport(underlay) networks, including:

   - Metro-Ethernet
   - Cable/Fibre Broadband
   - 4G/LTE Mobile broadband
   - DIA
   - Satellite-based transport
   - Hybrid-WAN
   - VPN

   Data transport networks may be provided by different networks.

5. **HIGH AVAILABILITY AND RESILIENCY:** The SD-WAN must support packet forwarding over multiple WANs at each site so as to provide transport diversity and increase overall availability of connectivity.

6. **APPLICATION-DRIVEN PACKET FORWARDING:** application optimisation shall be configured by the vendor for all the locations controlled centrally. The SD-WAN must be able to distinguish data flows by the application they support. For example, high priority packets originating from core business applications can be routed over Metro-E, while general web browsing is routed over cable broadband.

7. **POLICY-BASED PACKET FORWARDING:** the proposed SD-WAN must be able to apply customized networking policies to different types of packet flows. This means users can choose their desired quality-of-service, security, and/or business policy and their traffic will then flow over the best-matching transport underlay and overlay.

8. **QUALITY-OF-SERVICE (QOS) ASSURANCE:** the SD-WAN must measure QoS in real time, ensuring that core business (accounting, benefits, voice, video-conference calling, etc.) network traffic is given priority over other types of traffic (social media, bulk downloads,

television streaming, etc.). The QoS should be configurable through whatever network manager the vendor provides.

9. **ENCRYPTION:** The SD-WAN solution shall offer encryption between SD-WAN Edges.

10. **SERVICE AUTOMATION VIA CENTRALIZED MANAGEMENT, CONTROL AND ORCHESTRATION**:

The SD-WAN must support:

- Centralised management
- Real time network monitoring
- Real time administration and access levels based on roles (e.g., service provider, network administrator, network user)
- Zero-touch provisioning: Customer Premises Equipment attached to SD-WAN can retrieve its configuration and policies without needing to send a service provider installer to the site.

11. **WAN OPTIMISATION**

The SD-WAN must utilize a compilation of different network data functions, such as, data deduplication, data compression, data caching, forward error correction and protocol spoofing to increase WAN bandwidth and improve QoS performance.

12. **SECURITY FEATURES**

The edge device must have the following basic firewall features:

- IPS and IDS
- URL filtering
- Malware detection
- DDOS protection

13. **ADDITIONAL REQUIREMENTS**

The approved vendor will work jointly with the technical team of the NIC to recommend and develop any additional requirements as is required to improve performance, capacity and ensure the successful completion of this project.

PILOT TEST

A vendor responding to this RFP be required to setup a pilot test between the main office and two (2) other sites (as proof of) and to demonstrate the relative capacity of their proposed solution to meet the requirements as stated in this RFP.

The vendor will provide well-defined testing criteria for purposes of evaluating the relative performance of the proposed solution.

OPERATION AND MAINTENANCE SERVICES

i. Should have onsite support, that is, the vendor must make support personal available to come to the site when needed for first 6 months after the implementation of the project for Working Days (Monday to Friday) in working Hours (8AM to 5PM). Facilities to raise tickets during the aforementioned hours should be provided. Thereafter, there should be 24 X 7 facilities to raise tickets and customer support when required.

ii. Escalation matrix along with contact details to be provided within 15 days of commissioning the SD-WAN.

iii. Should inform NIC about planned events and service outages through alert, if solution is co-managed.

iv. Should provide online performance monitoring reporting to NIC indicating bandwidth utilization, network latency, packet loss, jitter, link availability parameters as per SLA (Service Level Agreement). Provision for triggering emails/SMSes on alerts should also be provided.

INSTRUCTIONS TO VENDORS

Note: The term VENDOR used throughout this RFP is defined as the company or contractor responding to this RFP, and who is offering to provide services and products. It is not meant to mean a product vendor such as “Cisco”.

Vendor responses should be complete and concise. All responses should include, at a minimum, the following response sections organized and submitted in the following order:

1. Vendor Qualifications to Provide Deliverables – The Respondent should provide detailed information to their qualifications to provide the required services, products and deliverables. Should the respondent be providing only some of the products and deliverables, AND is collaborating or subcontracting with additional vendors to provide all services, then this should be fully explained in the response.

2. Identified Responsible Individual – Please provide the name and detailed contact information of the person responsible for contracting with your company. Also provide the name and contact information of the person responsible for work performance under this solicitation.

3. Specific Deliverables – Complete all forms as provided below by adding the name of the vendor\contractor company who will be providing the services and products.

4. Cost Proposal and Budget

The cost of the products and services is an important and heavily weighted evaluation factor in determining which proposal will best meet the needs of NIC. The respondent shall provide costing information in the form of an itemized budget for all deliverable.

5. Respondents should provide a complete work plan.

6. Respondents should provide a complete timeline and schedule for the delivery of services and products. Anticipated timelines should commence with awarding of the contract and include all anticipated installation timeframes and projected dates for completion.

7. Contractor will work with the NIC to procure all materials and supplies necessary to provide the required services and products. Respondents should provide a materials list and price, by line item, for all supplies and materials. Pricing should be incorporated into the master proposal budget.

8. Please include a sample of your vendor contract or contracts that would be required for NIC to execute for the required product and services. Include a description of any payment or financing options.

9. Copy of business license, trade licenses and certifications, as appropriate

11.Include a description of all warranties and their source.

VENDOR AGREEMENT AND CERTIFICATION

By signing below, the vendor representative expressly certifies and warrants that all information that has been provided in this RFP response is accurate. The individual further acknowledges that all services and products described in this RFP response are immediately available and warrants that the vendor is able to deliver, install and complete all expected services within the required timeframes.

Furthermore, if it appears or becomes known that information provided in this RFP response is not true, or there are products or services that NIC has been assured it would receive but do not exist, or there will be additional charges not included in the proposal, then NIC reserves the right to terminate all discussions, negotiations, and/or implementation with an immediate and full refund of any fees paid by NIC.

All signatories to this document agree and warrant that they have made no changes or altered this RFP in any way, and are authorized to make all commitments set forth in this RFP response. Representatives signing below also agree that all responses to this RFP, and any documentation submitted, may be referenced in any final purchase agreement or contract between NIC and the vendor as an addendum and become legally binding.

Our response is for the following services and products described in the NIC RFP dated July 01, 2022. Please complete the following:

Company _____

Name of Company

_____ **Date:** _____

Signature

_____

Printed Name and Title

Address: _____

_____

Telephone Number: _____

EVALUATION AND SUBMISSION INSTRUCTIONS

NIC will convene a selection group to review the proposals received in response to this RFP. During this review process, additional information may be required of the respondent\vendor and some respondents may be invited to NIC in order to clarify any responses and further discuss the vendor's offer. All contact and any questions between respondent and NIC should be routed through the NIC point of contact (contact information below). NIC expects completion of the evaluation process and identifying its contractor choice for the required services and products within a 3 months' time frame.

Responses will be evaluated based on price and experience.

All responses should be sent to the Point of Contact by the date indicated in the schedule section of this RFP.

Proposals should be provided in both electronic and hardcopy formats by the Due Date. Please place three (3) copies of your RFP in a sealed envelope and clearly label in the lower left corner "Proposal for SD-WAN"

Late proposals will not be accepted.

Thank you for your interest in the National Insurance Corporation.

SCHEDULE

The following schedule applies to the bidding process:

	Activity	**Date**
1	Publication of RFP	Jul 01, 2022
2	Written confirmation of bidders' intent to bid	Jul 21, 2022
3	Deadline for submitting questions in writing	Jul 28, 2022
4	Written responses to all bidders (latest date)	Aug 7, 2022
5	**Proposals Due**	**Aug 14, 2022 – (4:30pm GMT-4)**

NIC Point of Contact:

Aloysius Burke
Manager
Computer Department
National Insurance Corporation
Francis Compton Building
Castries, Saint Lucia

E-mail: aburke@stlucianic.org
Telephone: (758)452-2808

APPENDIX A – REQUIREMENTS CHECKLIST

	Requirement	**NIC Rank**	**Vendor Response**	**Vendor Comment**
	Assessment of Existing Network	H		
	Identify defective equipment	M		
	Detailed Network Design	H		
	Network Segmentation Plan	H		
	Routing Plan	H		
	IP Address Scheme	H		
	Drawing - Proposed Logical Network Topology	H		
	Drawing - Proposed Physical Network Topology	M		
	Drawing - Proposed security architecture	H		
	Traffic Management/ Quality of Service(QoS) Plan	H		
	A procurement list of all network equipment/ services required to be purchased	H		
	Cybersecurity Enhancement Plan	H		
	Specification/ Datasheet for equipment proposed	M		
	Staging and configuration of equipment	H		

	Configure SNMP Traps	H		
	Configure Central Network Management Software	H		
	Registration of equipment with manufacturer	M		
	Develop Test Plan	H		
	Perform Network Testing	H		
	Conduct an analysis of the present network architecture to determine its suitability for the implementation of an SDWAN and to propose recommendations, if requirements not met.	H		
	Implement approved recommendations from analysis of network	H		
	The proposed SD-WAN must provide a secure, IP-based virtual overlay network using virtual tunnels over the Internet, Metro-Ethernet or other IP transport network.	H		
	The proposed SD-WAN must provide a secure, IP-based virtual overlay network using virtual tunnels over the Internet, Metro-Ethernet or other IP transport network.	H		
	Supports various SD-WAN data transport(underlay)	H		

	networks, DIA, METRO-E, LTE, Cable Broadband, etc.			
	Proposed SD-WAN solution must support packet forwarding over multiple WANs at each site so as to provide transport diversity and increase overall availability of connectivity	H		
	The proposed SD-WAN must be able to apply customized networking policies to different types of packet flows. This means users can choose their desired quality-of-service, security, and/or business policy and their traffic will then flow over the best-matching transport underlay and overlay.	H		
	Provides real-time QoS measurements to ensure that core business (accounting, benefits, voice, video-conference calling, etc.) network traffic is given priority over other types of traffic (social media, bulk downloads, television streaming, etc.).	H		
	Shall offer encryption between SD-WAN Edge	H		
	Provides centralised management	H		
	Provides real time network monitoring	H		

	Provides real time administration and access levels based on roles	H		
	Provides zero-touch provisioning: customer Premises Equipment attached to SD-WAN can retrieve its configuration and policies without needing to send a service provider installer to the site.	M		
	Provides in-built data-deduplication mechanisms	L		
	Provides in-built data compression mechanisms	M		
	Provides in-built data caching mechanism	L		
	Provides forward error correction and protocol spoofing mechanism	H		
	Provides IPS/IDS capabilities	M		
	Provides URL-filtering capabilities	M		
	Provides Malware detection capabilities	M		
	Provides DDOS protection capabilities	H		

Rating: L – Low Priority, M – Medium, H – High

Vendor Response: A- Available, NA – Not Available, C – Available with customisation