

## **EXPRESSION OF INTEREST**

### **For Standardization Of Network Of National Investigation Agency**

This is for general information of the firms/manufacturers of the equipments for Network Standardization of National Investigation Agency. All interested vendors/firms/manufacturers are requested to go thorough the same and submit their suggestions, if any, by 15.07.2024 on e-mail ID- spadmin.nia@gov.in.

2. A hard copy of suggestions may also be sent to the SP(Adm), NIA Hqrs, Opposite CGO Complex, New Delhi-110003.



Supdt. of Police(Adm)  
NIA Hqrs, New Delhi

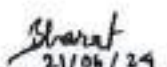


National Investigation Agency  
Government of India  
राष्ट्रीय अन्वेषण अभिकरण  
भारत सरकार

RFP for Standardization of Network of  
National Investigation Agency


## Table of Contents

1.	Introduction .....	3
2.	Project Requirement .....	3
3.	Components .....	5
3.1.	Technical Specification of Layer 3 Core Switch (Qty. 60 Nos.): .....	5
3.2.	Technical Specification of Layer 2 Access Switch (116 Nos.): .....	7
3.3.	Technical Specification of Network Orchestration Platform / SDN Controller (2 Nos.): .....	9
3.4.	Technical Specification of SD-WAN Routers with Firewall Capabilities (Type01-34 Nos. and Type02-04 Nos.) and SD-WAN Controller (02 Nos.): .....	11
3.5.	Technical Specification of AAA (2 Nos.): .....	22
3.6.	Technical Specification of Endpoint Detection and Response (EDR) solution .....	24
4.	Passive Elements: .....	28
5.	License, Support and Warranty: .....	28
6.	Scope of Work .....	29
7.	Instruction to Bidders .....	30
8.	BoQ (Price Bid Format): .....	34

  
21/06/24  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)  
21/06/24

  
(Ashish Choudhary)

## 1. Introduction

NIA intends to setup a scalable, secure network infrastructure for its Data Center (DC), Disaster Recovery Center (DRC) and branch locations powered by latest technology Software Defined Network. The Project for Network Standardization is to setup a unified network infrastructure across 19 locations of NIA (Data Center at NIA HQ, Disaster Recovery Center at NIA Hyderabad BO and other 17 branch locations) i.e. uniform network architecture, network hardware equipment and network security policies across all branches and further scalable to locations/branches added in future.

## 2. Project Requirement

To setup a unified network architecture across 19 locations of NIA (Data Center, Disaster Recovery Center and 17 branch locations). The site locations are as follows:

1. New Delhi - DC
2. Hyderabad - DR
3. Jammu
4. Lucknow
5. Kolkata
6. Guwahati
7. Imphal
8. Ranchi
9. Raipur
10. Chandigarh
11. Mumbai
12. Kochi
13. Chennai
14. Bengaluru
15. Bhopal
16. Patna
17. Ahmedabad
18. Jaipur
19. Bhubaneshwar

Each location will have two physically segregated air-gapped networks i.e. MPLS (Intranet) and Internet.

*Bharat Bhushan* (On Leave) *D. Singh* 1.8 ✓

The management and provisioning of LAN and WAN must use software defined principles with centralized controller in high-availability (DC and DR). A DC-DR network must be designed for Data replication, L2 and L3 extensions etc. The security framework for all end-points protected with a centralized end-point detection & response security solution, security posture checks and authentication with the existing domain controller.

Hence, the project of network standardization will cover the following model and components:

- **Centralized Management Layer at NIA HQ/DC and its High-Availability (HA) at NIA Hyderabad BO/DRC**
  - Centralized WAN Network Control Plane (SDWAN)
  - SDN Controller for network Management & Analytics
  - Centralized Network Access Control/AAA Solution
  - Centralized management for EDR solution
- **Infrastructure at all location**
  - Layer 3/core switches
  - Layer 2 switches
  - SD-WAN router with Firewall capability
  - End-point Detection and Response (EDR) solution

#### **MPLS/Intranet Subnet:**

MPLS connectivity will be terminated on a pair (HA) of SD-WAN routers. The Layer-3 switches and SD-WAN Routers are to be connected in full mesh. The VRF segmentation from the SD-WAN router will be carried to the Layer-3 switches and further into segmented VLANs. For centrally managing all the SD-WAN routers, SD-WAN controller will be installed at NIA HQ Data Center and its HA will be configured at DR Site, NIA Hyderabad BO.

For centrally managing, Layer3 and Layer2 switches in MPLS/Intranet subnet, an SDN Controller will be implemented at NIA HQ and its HA will be installed at DR Site, NIA Hyderabad BO.

#### **Internet Subnet:**

Internet segment at each location will be **air-gapped** from MPLS/Intranet subnet and will have a separate zone for Infrastructure service and user systems. The end points will have EDR Client installed and configured and will be centrally managed at DC or DR. In Internet subnet at Branch offices of NIA, the equipment will not be in High-Availability (HA) mode. This is because the Internet subnet will not be having very critical data of NIA and

 (Bharat Bhushan)  (Amit Nigam) (On leave)  (Prashant V Holkar)  (Dhruv Singhal)  (Ashish Choudhary)

there are several alternatives to make Internet services up in case of any fault in the equipment. Hence, L3-switch and L2-switch will be in non-HA at NIA BOs.

### 3. Components

#### 3.1. Technical Specification of Layer 3 Core Switch (Qty. 60 Nos.):

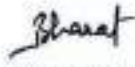
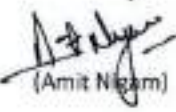
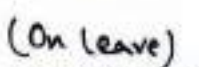


Feature	Specifications
<b>Performance and Architecture</b>	<ol style="list-style-type: none"> <li>1. Should have 24 x 1/10G (12x 10G SFP+ SR optics and 2 x 1G SFP LX, 2 x 1G SFP-SX transceiver modules), 8 x 1G RJ45 Transceiver module and additional ports (with capacity of switching throughput) for both HA connectivity between the core switches and SPAN. All the ports must be Fully populated from day-1.</li> <li>2. Should be able to support MLAG or similar high available architecture</li> <li>3. Support active-active &amp; active-passive mode (HA cables to be included, if dedicated HA Port), VRRP or equivalent.</li> <li>4. Should be a non-blocking switch with minimum 480Gbps of switching throughput.</li> <li>5. Minimum 32 MB packet buffer memory.</li> <li>6. Should have minimum 16 GB RAM and 32 GB flash</li> <li>7. Should have minimum 10K MAC address entries, minimum 4000 VLANs.</li> <li>8. Should support OpenFlow/equivalent for software defined networking, Zero Touch Deployment</li> <li>9. Should support VRF, Q-in-Q on day-1 and have capability to support EVPN + VXLAN if required in future. The switch should provide a mechanism to support group-based micro-segmentation providing the ability to filter traffic between endpoint groups as defined in the central manager.</li> <li>10. Should have 802.1x, TACACS+, RADIUS, sFLOW or equivalent. NTP, Control Plane Policing and DoS attack protection, Dynamic/ Arp Protection, DHCP Relay, DHCP Snooping, Port Security,</li> <li>11. Should support ACLs (L2, L3, L4)</li> <li>12. Should support MAC address change notification</li> <li>13. Support Storm Control (Broadcast, Unicast, Multicast)</li> <li>14. Should support STP, RSTP, MSTP</li> <li>15. Support Link Aggregation, Port and Subnet based VLAN, Dynamic VLAN, Private VLAN, Uplink Failure Detection, BFD, UDLD or Bridge Assurance or equivalent static and</li> </ol>

*Sharat*

*A. J. Singh (On Leave) - S. Sankar*

*1, 1*

	<p>policy based Routing, BGPv4, ISIS (v4 and v6), OSPF v2 &amp; v3, L3 subinterface.</p> <p>16. Static and policy based Routing, BGPv4, OSPF v1/v2/v3.</p> <p>17. Traffic classification based on MAC Address, Port, Differentiated Service Code Point (DSCP), IP Address, VLAN, Ingress and Egress traffic shaping and policies, Traffic Flows - Filter, mark and limit, Minimum 8 queues per port, Quality of Service (QoS) to provide priority for Audio/Video Traffic (Should support Audio Video bridging from day 1) and VoIP.</p> <p>18. Support IPv4 and IPv6 Multicast, IGMP v3, IGMP Snooping, PIM-SM, SSM and Bidir, IGMP</p> <p>19. Support IEEE standards like 802.3ae, 802.3x, 802.3ad, 802.3ab, 802.1p, 802.1ab</p>
<b>Management</b>	<ol style="list-style-type: none"> <li>1x console port, 1x Out-of-band Copper Ethernet IP based management port, USB port. Console cable and rail kit to be provided along with each switch.</li> <li>Support port mirroring to local and L3 remote destination (GRE Encapsulated).</li> <li>Should also support wireshark/tcpdump locally to capture data plane and control plane packets locally for troubleshooting purposes.</li> <li>Should Support SNMP v3, CLI, SSH v2, SCP/SFTP or equivalent secure copy, TLS 1.3, Ansible/Puppet/Chef/SaltStack, RESTCONF API or their equivalent open APIs/scripting methods.</li> <li>Dual firmware, configuration rollback, hot patching, docker containers for third party application integration like for management</li> <li>IPv6 - Management, Ping and traceroute</li> </ol>
<b>General</b>	<ol style="list-style-type: none"> <li>Should operate at AC -50Hz, 220-240V</li> <li>Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent</li> <li>Should have redundant hot-swappable power supplies</li> <li>Should be 1U/2U Rack Mountable with required accessories for rack mounting.</li> <li>Should have LED indicator for per port status, PSU and Management Status</li> <li>All required licenses as per specification should be quoted on day-1. All licenses should be perpetual in nature or should be quoted with 5 years of subscription on day-1.</li> <li>Switch, Switch OS, switch transceivers and switch manager software should be from same OEM.</li> </ol>

 (Bharat Bhushan)
  (Amit Nigam)
 (On leave)
  (Prashant V Holkar)
  (Dhruv Singhal)
  (Ashish Choudhary)

### 3.2. Technical Specification of Layer 2 Access Switch (116 Nos.):

Feature	Specifications
<p><b>Performance and Architecture</b></p>	<ol style="list-style-type: none"> <li>1. Should have 48 x 10/100/1000 Base-T PoE+ ports (Fully populated) &amp; 4x 10G SFP+ ports supporting both 1GbE &amp; 10GbE speeds (populated with 2x10G SFP+ SR</li> <li>2. Should be able to support MLAG or similar high available architecture,</li> <li>3. Should be a non-blocking switch with minimum 176Gbps of switching throughput</li> <li>4. Should have minimum 1K MAC address entries and 10K IPv4 LPM Routes, 1000 VLANs.</li> <li>5. Should have minimum 4GB RAM and 8GB flash</li> <li>6. Should support latest OpenFlow/equivalent for software defined networking, Zero Touch Deployment</li> <li>7. Should have capability to support EVPN + VXLAN if required in future.</li> <li>8. Should have 802.1x, TACACS+, RADIUS, sFLOW or equivalent, NTP, Control Plane Policing and DoS attack protection, Dynamic/ Arp Protection, DHCP Relay, DHCP Snooping, Port Security,</li> <li>9. Should support ACLs (L2, L3, L4)</li> <li>10. Should support MAC address change notification</li> <li>11. Support Storm Control (Broadcast, Unicast, Multicast)</li> <li>12. Should support STP, PVST+, RSTP, MSTP</li> <li>13. Support Link Aggregation, Port and Subnet based VLAN, Dynamic VLAN, Private VLAN, Uplink Failure Detection, BFD, UDLD or Bridge Assurance or equivalent, static and policy based Routing, BGPv4, ISIS (v4 and v6), OSPF v2 &amp; v3, L3 subinterface.</li> <li>14. Traffic classification based on MAC Address, Port, Differentiated Service Code Point (DSCP), IP Address, VLAN, Ingress and Egress traffic shaping and policies, Traffic Flows - Filter, mark and limit, Minimum 8 queues per port, Quality of Service (QoS) to provide priority for Audio/Video Traffic (support Audio Video bridging from day 1) and VoIP.</li> <li>15. Support IPv4 and IPv6 Multicast, IGMP v3, IGMP Snooping, PIM-SM, SSM and Bidir, IGMP</li> <li>16. Support IEEE standards like 802.3ae, 802.3x, 802.3ad, 802.3ab, 802.1p, 802.1ab</li> <li>17. Capability to integrate using L3 Remote SPAN / Equivalent with Network detection and response (NDR) solutions, if required, in future.</li> </ol>

Sharat At Nya (On Leave) D. Sushil



<p><b>Management</b></p>	<ol style="list-style-type: none"> <li>1. 1x console port, 1x Out-of-band Copper Ethernet IP based management port, USB port. Console cable and rail kit to be provided alongwith each switch.</li> <li>2. Support port mirroring to local and L3 remote destination (GRE Encapsulated)</li> <li>3. Should also support wireshark/tcpdump locally to capture data plane and control plane packets locally for troubleshooting purposes.</li> <li>4. Should Support SNMP v3, CLI, SSH v2, SCP/SFTP or equivalent secure copy, TLS 1.3, Ansible/Puppet/Chef/SaltStack, RESTCONF API or their equivalent open APIs/scripting methods.</li> <li>5. Dual firmware, configuration rollback, hot patching, docker containers for third party application integration like for management</li> <li>6. IPv6 - Management, Ping and traceroute</li> </ol>
<p><b>General</b></p>	<ol style="list-style-type: none"> <li>1. Should operate at AC -50Hz, 220-240V</li> <li>2. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent</li> <li>3. Should have redundant power supplies.</li> <li>4. Should be 1U/2U Rack Mountable with required accessories for rack mounting.</li> <li>5. Should have LED indicator for per port status, PSU and Management Status.</li> <li>6. All required licenses as per specification should be quoted on day-1. All licenses should be perpetual in nature or should be quoted with 5 years of subscription on day-1.</li> <li>7. Switch , Switch OS, switch transceivers and switch manager software should be from same OEM.</li> </ol>

  
(Bharat Bhushan)

  
(Amit Nigam)

(On leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

### 3.3. Technical Specification of Network Orchestration Platform / SDN Controller (2 Nos.):

Feature	Specifications
<p style="text-align: center;"><b>Architecture</b></p>	<ol style="list-style-type: none"> <li>1. Support Campus fabrics and data center Clos network topology defined using Spine/access, Leaf/Core switches with VXLAN overlay.</li> <li>2. Support workload mobility anywhere in the Data Center and across Data Center sites. Add as many Leaf as needed to achieve desired scale.</li> <li>3. Support various Hypervisor encapsulation including VXLAN and 802.1q natively.</li> <li>4. Support VXLAN Switching/Bridging and VXLAN Routing.</li> <li>5. Support the distributed campus network architecture (as mentioned in this document). It should have the capability to support different hypervisor/ virtual Machine Environments like (ESXi / VmWare vCenter, hyperV / System Center/Nutanix).</li> <li>6. . Should support L2 &amp; L3 extension across DC sites to support failover and failback of the applications.</li> <li>7. Support zero trust policy model /segmentation model for connected systems or hosts in campus/DC to help in protecting against attacks and provide support for stateless/statefull firewall. Should display endpoint connectivity details.</li> <li>8. Support Role based access control and support AAA using Local User authentication, RADIUS, TACACS+ / LDAP / AD, SAML/OAUTH. Communication between switches and controller should be encrypted.</li> <li>9. Should provide micro-segmentation / Macro-segmentation.</li> <li>10. Support SNMP v2/3, streaming telemetry and Netflow/sFlow/IPFIX. Telemetry and flow data from switches which should be available for at least 14 days.</li> <li>11. Support centralized single pane of glass for managing, monitoring and provisioning the entire Leaf-spine fabric, core/access switches within Data Centers &amp; across sites.</li> <li>12. Easily configure, standardize, and manage configuration changes, compliance policies, and firmware deployments to multiple devices in one operation or many operations that can be scheduled for pre-determined times. Should have in-product documentation</li> <li>13. Template-based configuration file creation, back-up and restoration - on an automated, scheduled or ad hoc basis.</li> </ol>

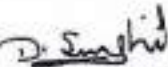
Sharat N. Nijjar (On leave) D. Suresh

	<ul style="list-style-type: none"> <li>14. . configuration change detection, policy-based compliance detection via the compliance feature – pre-deployment configuration verification, compliance policies, bugs and PSIRT visibility, produce audit trails to facilitate troubleshooting.</li> <li>15. Deploy firmware upgrades to devices, or groups of devices, manage user/user group security settings and their functional permissions within the application.</li> <li>16. Support reporting in pdf/html/csv other standard formats. Support event alerts over email.</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>1. The Fabric Manager must be physical appliance based. Fabric management infrastructure should be provisioned in HA mode. Failure of complete SDN controller should not impact production traffic.</li> <li>2. Should be able to support a minimum of 200 Switches from day-1.</li> <li>3. The proposed SDN controller should provide migration to new leaf-spine fabric from same OEM at NIA DC &amp; DR, when required in future.</li> <li>4. Should manage all the Layer3/core and Layer2/access switches in MPLS/Intranet subnet.</li> </ul>
<b>General</b>	<ul style="list-style-type: none"> <li>1. Should provide the latest features and updates and provide new version of SDN controller as on when available.</li> <li>2. Should be provided with 05 years direct OEM TAC support.</li> </ul>

  
(Bharat Bhushan)

  
(Amit Nigam)

(On leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

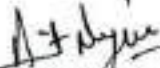
3.4. Technical Specification of SD-WAN Routers with Firewall Capabilities (Type01-34 Nos. and Type02-04 Nos.) and SD-WAN Controller (02 Nos.):

Feature	Specifications
<p><b>SDWAN Functional Requirements for SDWAN Solution across all locations</b></p>	<ol style="list-style-type: none"> <li>1. All components of SDWAN solution should be deployed on premise and maintain zero trust secure relationships among themselves. None of the Organization's Business data should go to the OEM Premises or Cloud under any reason (which includes logging &amp; scanning for Threats). Bidder to submit undertaking/declaration from OEM with the technical bid.</li> <li>2. SDWAN Edge Device should build Control plane with Controllers/orchestrator and Data Plane with peer edge devices and also forwards traffic in encrypted IPSEC tunnels, applies local policy like QoS, ACL etc.</li> <li>3. System should be able to support by separating the control plane from the data plane and from management plane. The Data Plane, Control Plane and management plane should be virtually and logically separate end-to-end. SDWAN solution should provide security to control plane sessions as well as to data plane traffic</li> <li>4. SDWAN solution should support following transports - MPLS, Ethernet, Internet BB, LTE/5G,</li> <li>5. There has to be minimum two factor authentication between Controllers, central and Type 1, Type 2 devices before they established session with each other. Out of two factors, one factor needs to be certificate based (PKI). This PKI functionality should be inbuilt with the solution from Day1</li> <li>6. Solution should not require any pre-shared keys to form IPsec tunnels. Solution should use dynamic crypto keys and it should be possible to refresh keys at periodic interval from Day1</li> <li>7. SDWAN solution should support minimum 100 branch devices.</li> <li>8. SDWAN Solution shall support deployment of any kind of topologies such as full- mesh, hub-spoke and</li> </ol>

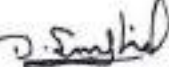
Sharat A.T. Nigam (On Leave) D. Singh M.S.

	<p>partial mesh or any arbitrary topology. It shall be possible to change network topology only by pushing policy from central controller/orchestrator and shall not require device by device configurations</p> <p>9. SDWAN edge device should support end to end logical segmentation of WAN and each LAN networks from Day 1</p> <p>10. SDWAN solution should built on demand IPSEC tunnels automatically between branch-to-branch edge devices</p> <p>11. The proposed SD WAN solution should provide end to end Encryption using industry standard protocol (Minimum AES-GCM-256 or higher).</p> <p>12. SDWAN solution should support underlay reachability with non-SDWAN sites directly from the site through MPLS as well as overlay connectivity with Hub or other edge devices on overlay.</p> <p>13. SDWAN solution should support traffic routing based on longest prefix match</p> <p>14. SDWAN solution should support IPSec connectivity to third party devices from branch (Type 1) and Hub (Type 2) routers</p> <p>15. SDWAN solution should support dual stack IPV4 and IPV6 support on underlay and overlay</p> <p>16. SDWAN solution should support OSPF, BGP, Static routing, policy/performance bases routing. It should support advanced BGP capabilities like Local preference, AS path prepending, IPv4 and IPv6 address families, MED and filtering support with the use of BGP communities</p> <p>17. SDWAN Solution should be capable of upgrading CPE ( ) devices to the latest version and also support rollback of the software version when upgraded to the latest software version, if required. Rollback and Upgrade shall be performed from the central management engine</p> <p>18. Central Management engine should support Customized Role Based Access Control that provides only relevant information to the user based on their roles and privileges. Solution shall provide detailed information of changes done using configurations/templates</p> <p>19. SDWAN solution should support integration using RADIUS/TACACS protocols also should have</p>
--	---

  
(Bharat Bhushan)

  
(Amit Nigam)

(On leave)  
(Prashant V Holkar)

  
(Ohruv Singhal)

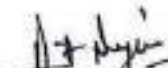
  
(Ashish Choudhary)

	<p>integration with NTP using authentication and secured with access-list.</p> <p>20. Branch (Type 1) and Hub (Type 2) router hardware should be a hardened appliance of OEM running SDWAN firmware on top of it.</p> <p>21. SDWAN solution should identify the application and it should be possible to define policy based on application.</p> <p>22. SDWAN solution should be able to load balance traffic across multiple links based on load balancing algorithms efficiently using all available links. System shall also detect blackouts &amp; brownouts by supporting active-active load balancing and fast session failover</p> <p>23. SDWAN solution should support traffic load balancing across unequal capacity of WAN links</p> <p>24. SDWAN solution should support SLA based application aware routing for various on-prem applications running over IPSEC tunnels to DC/DR</p> <p>25. SDWAN solution should support SLAs based on Latency, Packet drops and Jitter for accessing various on-prem applications over IPSEC tunnels</p> <p>26. Solution should support adaptive FEC and Packet Replication policies. FEC ratio (of loss-recovery packets to data packets) and Packet Replication policies should be tied to dynamic network measurements. When a link is experiencing no loss, FEC and Packet Replication policies should get disabled automatically and there should be no overhead. The proposed SD WAN solution should support Forward error correction and packet duplication for real time applications like Voice and Video and all other non-real time applications.</p> <p>27. In the event of link down the solution shall be able to move traffic to a better link within 1 second.</p> <p>28. SDWAN solution should be able to automatically route LAN traffic on the overlay WAN/IPSEC tunnels without the need of configuring any separate routing protocols running between edge devices.</p> <p>29. SDWAN solution should use protocols to probe the link health end to end and to detect the link SLA (Latency/Drops/Jitter). The protocol should be</p>
--	---

Sharat *[Signature]* (On Leave) D. Suresh *[Signature]*


	<p>DSCP aware so that it can be mapped with MPLS SP QOS offerings if required.</p> <p>30. SDWAN solution should be able to prioritize business critical applications and shall have the capability of prioritizing traffic during congestion</p> <p>31. SD-WAN solution should build dynamic IPSEC tunnels using Asymmetric encryption (DH group) and should generate unique key for each site for better security.</p> <p>32. . SDWAN solution should support IPSEC and configuration of firewall policies using L3/L4 information and inhouse NCFW, Antivirus, URL filtering from day-1 and should not be dependent on third party solution</p> <p>33. SDWAN solution should provide end to end logical segmentations between branch and hub devices</p> <p>34. SDWAN solution should provide minimum 4 tenants or equivalent at branch locations and minimum 8 tenants or equivalent at DC and DR SDWAN Devices.</p> <p>35. SDWAN solution should able to carry multiple segments traffic on single or multiple IPSEC tunnels between branch and hub devices.</p> <p>36. In case of a change in WAN IP Address (Private/Public) at branch locations, SDWAN solution shall detect and rebuild the IPSEC tunnel without manual VPN configurations.</p> <p>37. SDWAN solution should support NAT, PAT, Static NAT on branch locations and DC-DR Encryption devices.</p> <p>38. The solution shall be capable of configuring QoS weights on default applications, critical applications &amp; destination IP based QoS definitions/VLAN based etc.</p> <p>39. SDWAN solution should support granular level of QOS for return traffic from HUB devices towards branches with support of per tunnel QoS so that branch traffic with smaller WAN bandwidth are not over utilized by huge return traffic from hub sites.</p> <p>40. SDWAN solution should support change in QOS parameters on hub locations dynamically with reference to branch interface bandwidth upgrade/downgrade. The solution should also support inbound and outbound QOS.</p>
--	---

  
(Bharat Bhushan)

  
(Amit Nikam)

(On leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

	<p>41. The system should support load balancing on basis of per packet and per session based on application requirements.</p> <p>42. SDWAN solution should support single device with multiple links or multiple links spread across two devices however all WAN links should work in active-active fashion without any additional hardware required at the location.</p> <p>43. SDWAN solution support integration with RADIUS authentication server to authenticate client connected to a port before that client can access any services offered by network</p> <p>44. SDWAN solution should support DHCP Server, DHCP relay, PPPoE, VRRP.</p> <p>45. The proposed SDWAN solution must have visibility of each element with the NMS Suite.</p> <p>46. The proposed SDWAN solution must have capability to support Multicast Features like Multicast forwarding, PIM sparse (rfc 4601), PIM rendezvous point</p> <p>47. The proposed SDWAN solution must support following Device Management Features like Console, SSH and Web for management. Software upgrades through either of CLI, TFTP, Web based using HTTPS or SNMPv3</p> <p>48. The system should support SHA-384 or above authentication algorithms for Data Integrity.</p> <p>49. The system should allow automated, policy driven refresh of the encryption key.</p> <p>50. The system should have Intrusion Prevention System (IPS) at branch locations with the ability to update the IPS signature database centrally from the software defined controller/orchestrator on a need basis or on a periodic basis.</p> <p>51. During the contract period the device should provide no performance degradation with all the features enabled with 100% of WAN link utilization.</p> <p>52. Controller /Management Server /orchestrator must not communicate with any un-authenticated and un-authorized Controller/Management Server.</p> <p>53. The Centralized devices must be capable of termination of backhaul links directly or through an Existing aggregation switch and must be compatible with ISP links</p>
--	--

Sharat      A. D. Dey (On Leave)      D. Suresh      A. S.



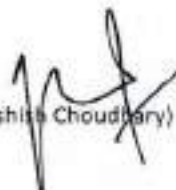
	<p>54. In case the SDWAN encrypted throughput reaches beyond the value of license applied on Day 1 then the overhead traffic must not be dropped by the SDWAN device and continue to function without any disruption to the services.</p> <p>55. The proposed SD WAN solution must support Bandwidth testing on WAN links to check the available bandwidth.</p> <p>56. The proposed SD WAN devices/appliances in the proposed SD WAN solution should be able to interoperate with the existing products of different vendors.</p> <p>57. The proposed SD WAN solution should have dashboard/pre-defined central reports to see Prevented Attacks, Detected Attacks and Attack Trends.</p> <p>58. There has to be authentication mechanism between Controllers/orchestrator and central and branch devices before they established communication with each other. PKI (certificate) based authentication between branch and central concentrator is must.</p> <p>59. USB port and telnet should be disabled by default and console should be password protected.</p> <p>60. The proposed SDWAN solution must co-exist with existing IP/MPLS network and work with vendor / ISP solution.</p> <p>61. The proposed SDWAN solution must support bandwidth multiplexing (ability to bind multiple links) for all platforms on network side i.e. (MPLS and Internet) or (Internet and Internet) or (MPLS and MPLS) lines</p> <p>62. The SDWAN solution should have autonomous control plane, which ensures that the Edge Customer Premises Equipment devices (CPE) continue to operate minimum 7 days (with the last configuration) even if disconnected from the Centralized Management / Orchestrator. Such edge CPE devices should have the capability to be reconfigured by logging in to their GUI/CLI, during exceptional circumstances.</p> <p>63. All SDWAN components must support AAA framework from Day 1</p>
--	--

  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)   
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

	<p>64. The solution must support TCP optimization for mitigating the effects of link quality degradation like high latency or packet drops.</p> <p>65. All SDWAN router devices must support Netflow Verison 9 or later from Day 1.</p> <p>66. All SDWAN router devices must support all standard BGP attributes for incoming and outgoing direction from Day 1.</p> <p>67. All SDWAN components must support management ACL, Banner, interface description on all live interfaces (Min 40 Characters) from Day1</p> <p>68. All SDWAN router devices must support WAN interface parameters to check link quality from Day1</p> <p>69. All SDWAN router devices must support way to prevent dropping fragmented packets, clearing interface and ACL counters without reboot from Day1.</p> <p>70. The solution must also support load sharing based on IP addresses/network subnets/application categories across all locations.</p> <p>71. All the devices provided in the solution must be capable of integration with NMS using SNMPv3 protocol and should be able to generate common reports like link/device performance, Asset details, SLA reports from branch SDWAN device using SNMPv3.</p> <p>72. All devices part of this solution should be able to integrate with SIEM, SOAR using SYSLOG.</p> <p>73. All SDWAN router devices should support traffic blocking using access lists, MGMT access restriction, critical email/SMS alerts for major events, clearing of interface counters.</p> <p>74. The solution should support inverse wildcard mask.</p> <p>75. All SDWAN router devices supplied as part of the solution should support mechanism to check various interface counters for link Utilization/Speed etc. which are required to troubleshoot WAN links.</p> <p>76. All SDWAN devices supplied as part of this solution should support to add interface descriptions on all used interfaces which can be fetched using SNMPv3 in NMS software</p> <p>77. All SDWAN router devices should be capable of supporting BGP protocol with password and should also support standard BGP attributes</p>
--	---

Sharet Lt. Major (On Leave) D. Singh In I

	<p>78. The proposed SD WAN solution should allow automated, time based, and policy driven refresh of the encryption key per virtual private network.</p> <p>79. The proposed SD WAN solution should continuously check the link flaps, if the link is not stable then put the link in monitor state, once the link is stable for time then start sending traffic on that link with QoS features/ bandwidth shaping.</p> <p>80. All SD-WAN router devices should be having multi core CPU and at-least 8192 MB Memory from Day1.</p> <p>81. The proposed SD-WAN solution should be able to load balance across multiple WAN links from Day1. The WAN links would consist any combination of the following links - MPLS Primary Link, MPLS Secondary Link, etc.,</p> <p>82. The proposed branch SD-WAN devices should be able to work as a standalone layer 3 routing device from Day1.</p> <p>83. The proposed SD-WAN solution should be able to create dashboard for the monitoring all links, all appliances. The solution should also support link utilization, availability, SLA report generation, loss/latency report etc. The data retention period for the same would be minimum 3 months.</p> <p>84. The proposed SD-WAN solution, the software defined controller/orchestrator must be able to monitor, and report top applications by usage across all branch locations. In the proposed SD-WAN solution, the software defined controller must be able to monitor, and report at-least top 20 applications by usage. The retention period for the same should be for at-least 3 months.</p> <p>85. In the proposed SD-WAN solution, the administration should be able to drill down these reports for troubleshooting. For e.g., application accessed by specific host along with bandwidth consumed during defined amount of time.</p> <p>86. The proposed SD-WAN solution must support partial software upgrade feature which allows the network administrator to selectively upgrade the software on sites in the network without needing to upgrade all sites simultaneously.</p>
--	---

  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)   
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

	<p>87. The SD-WAN should support DDoS mitigation functionality and protect DDOS attack like UDP Flood, Ping of Death etc.</p> <p>88. The SD-WAN solution should have same management console (single pane of glass) for SD-WAN and Security monitoring/Configuration.</p> <p>89. The system architecture should allow to use the most preferred link based upon Link characteristics (Latency, Jitter, Packet loss, MOS score) for critical applications as defined in policy.</p> <p>90. SD-WAN should have common criteria (at least EAL4) certificate or equivalent and FIPS-140-2.</p> <p>91. Should have IPv6 logo certification or USGv6 or equivalent TEC certification.</p>
<p><b>SD-WAN Branch Device (Type 01)</b> <b>(For 17 locations)</b></p>	<p>1. Appliance should have 4x1GE RJ45 Slots, 2x10G(SFP+ SR), 2x1GE SFP (SX) slots and 2x1G SFP(LX). Appliance should have free slots to accommodate additional interface like RJ45, SFP &amp; SFP+ (All transceiver should be populated from day one)</p> <p>2. Type 1 devices should support minimum 4 tenants or equivalent. Each tenant or equivalent should be administered individually. It should support minimum 4 tenants or equivalent with separate management and role-based access. It should possible to create different overlay topology per tenants or equivalent.</p> <p>3. Appliance should support at least 10,000 IP routes.</p> <p>4. The Router must support minimum 1000 Branch to Branch IPsec tunnel.</p> <p>5. Type 1 devices should have RJ45/Micro USB console port</p> <p>6. Type 1 devices should be capable to terminating total BW of 200 Mbps with all SDWAN features enabled (Stateful + NGFW + URL Filtering) from day-1.</p> <p>7. The Proposed solution should have 100000 layer 4 concurrent sessions.</p> <p>8. The Proposed solution should have 25,000 Layer 4 new sessions per second or higher.</p> <p>9. The Proposed solution should have minimum 200 Mbps of VPN throughput or higher</p> <p>10. The Next Generation Firewall in Type 1 devices should support the following security features:</p>

*Bharat* *A. S. Nigam* (On leave) *D. Smith* *M. S.*

	<ul style="list-style-type: none"> <li>a. Application Based Access Control</li> <li>b. URL Filtering Based on Category and Reputation</li> <li>c. SSL Inspection</li> <li>d. IP Filtering Based on Geo-Location and Reputation</li> <li>e. DNS Filtering Based on Query Match, Category and Reputation</li> <li>f. File Filtering Based on Application, File Type, Size and Reputation</li> <li>g. Users and Groups</li> </ul> <p>11. Type 1 devices should be configured in HA.</p>
<p><b>SD-WAN Hub Device (Type-02) (For DC and DR )</b></p>	<ul style="list-style-type: none"> <li>1. Appliance should have 4x1GE RJ45 Slots, 2x10G(SFP+ SR), 2x1GE SFP (SX) slots and 2x1G SFP(LX). Appliance should have free slots to accommodate additional interface like RJ45, SFP &amp; SFP+ (All transceiver should be populated from day one)</li> <li>2. Type 2 devices should support minimum 8 tenants or equivalent. Each tenant or equivalent should be administered individually. It should support minimum 8 tenants or equivalent with separate management and role-based access. It should possible to create different overlay topology per tenants or equivalent.</li> <li>3. Appliance should support at least 10000 IP routes.</li> <li>4. The Router must support minimum 2000 Branch to Branch IPsec tunnel to support full mesh/partial mesh topology.</li> <li>5. Type 2 devices should have RJ45/Micro USB console port</li> <li>6. Type 2 devices should be capable to terminating total BW of 1 Gbps with all SDWAN features enabled (Stateful + NGFW + URL Filtering + IPS) from day-1.</li> <li>7. The Proposed solution should have 200,000 layer 4 concurrent sessions.</li> <li>8. The Proposed solution should have 50,000 Layer 4 new sessions per second or higher.</li> <li>9. The Proposed solution should have minimum 1 Gbps of VPN throughput or higher</li> <li>10. The Next Generation Firewall in Type 2 devices should support the following security features: <ul style="list-style-type: none"> <li>a. Application Based Access Control</li> </ul> </li> </ul>

  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)   
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

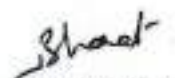
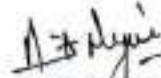
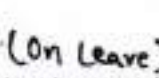
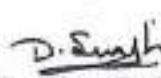

	<ul style="list-style-type: none"> <li>b. URL Filtering Based on Category and Reputation</li> <li>c. SSL Inspection</li> <li>d. IP Filtering Based on Geo-Location and Reputation</li> <li>e. DNS Filtering Based on Query Match, Category and Reputation</li> <li>f. File Filtering Based on Application, File Type, Size and Reputation</li> <li>g. Users and Groups</li> </ul> <p>11. Type 2 devices should be configured in HA.</p>
<p><b>SD-WAN Controller for Management and Monitoring (For DC and DR)</b></p>	<ul style="list-style-type: none"> <li>1. SDWAN solution should support email or SMS based alarm to notify the administrators when Link Flaps at the remote branch location, ISP link quality degrade (high latency, high packet drops, etc), Link utilization along with threshold, CPU, Memory and Disk Utilization of the Branch Device. The notifications generated by the software defined network controller/orchestrator should have capability to be forwarded as email or SMS.</li> <li>2. SDWAN Controller / management solution must be a separate hardware appliances. Management appliance must have 4 x GE RJ45, 2 x SFP ports and must be capable to manage 100 SDWAN devices without any additional hardware/License and must be provided in HA</li> <li>3. SDWAN solution should be open and programmable through REST APIs.</li> <li>4. SDWAN solution management engine dashboard should provide dashboard for security, VPN management and configuration of SDWAN fabric as well as integrations with cloud providers and cloud security providers.</li> <li>5. Solution should provide various reports like link availability, device uptime, inventory, device health, bandwidth usage, report. Reports need to be provided daily, weekly, monthly as per requirement in excel/pdf format.</li> <li>6. SDWAN Solution management engine should provide the near real time and historical health status of all the location devices on the dashboard for CPU &amp; memory utilization, link utilization and performance, application utilization etc.</li> </ul>

Sharat A. Nigam (On Leave) D. S. U. A. S.

	<p>7. SDWAN solution should have capabilities to provide analytical information for Application performance, Bandwidth usage, traffic distribution across sites, tunnels and links, Availability information of links and devices along with top users and flows.</p> <p>8. SDWAN solution should support onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device.</p> <p>9. In the proposed SD WAN solution, the system should provide a mechanism to monitor the performance for Links based on latency, jitter, packet loss and MOS Score.</p> <p>10. SD-WAN controller should have the capability for exporting the configuration backup of all associated SD-WAN devices and restoring the configuration.</p>
--	---

### 3.5. Technical Specification of AAA (2 Nos.):

Feature	Specifications
<b>Architecture</b>	<ol style="list-style-type: none"> <li>Should be an appliance based (Hardware / Virtual / Software). In case of Virtual / Software based solution, all the required and supporting hardware, OS and software with the licenses must be supplied.</li> <li>Support minimum of 2500 concurrent end points / users licenses (with posture check)</li> <li>Should be able to integrate with all makes and type of manageable network (Wired and Wireless) devices, which are capable of supporting open standards-based protocols required for NAC operation. Support for 802.1X, MAC, Web HTTPS authentication and authorization.</li> <li>Support multi-factor (including token) Authentication Support.</li> <li>AAA framework must allow for the complete Authentication and Authorization sources from databases (like AD/LDAP/RADIUS/TACACS). Support built-in database for user credential management.</li> <li>Solution must have support for Windows NAP allowing health and posture checks on Windows endpoints without the need to install an agent. Identity-Based Policies</li> </ol>

 (Bharat Bhushan)
  (Amit Nigam)
 (On Leave)
  (Prashant V Holkar)
  (Dhruv Singhal)
  (Ashish Choudhary)

	<p>through Integration with Active Directory. Must be able to join multiple Active Directory domains to facilitate authentication</p> <ol style="list-style-type: none"> <li>7. Should be able to integrate with devices such as firewall and switch to isolate and quarantine / in-depth device assessments of an user/system</li> <li>8. Support transparent network authentication Via Single Sign-On.</li> <li>9. Support port bouncing, VLAN steering and sending custom messages.</li> <li>10. Should support device profiling. Able to gather detailed identity and access information with OS and device fingerprinting for iOS, Android, Windows, Linux and more.</li> <li>11. Should be able to perform posture check for end points (Windows &amp; macOS, Linux) for OS health for parameters like Registry Keys, allowed process, AV or Firewall Enabled etc.</li> <li>12. Detect and authenticate (like MAC based) device with IP address without the need for a client application on endpoint for devices like VoIP phones, printers, wireless devices, machinery, cameras, sensors etc.</li> <li>13. Support event logging of device access and activity time stamp.</li> <li>14. Support device search functionality by attributes such as user name, OS type, IP &amp; MAC address, System Name</li> <li>15. Support automated onboarding and self-registration of all IP end points.</li> <li>16. Support automated context-based policy provisioning of network services for mobile devices. Granular policy enforcement. Policy model should support incorporation of several contextual elements including identity, endpoint health, device, authentication method &amp; types, and conditions such as location, time, day, etc.</li> <li>17. Must provide capability to bind together the username, IP address and MAC address, and physical port of each endpoint for forensic analysis</li> <li>18. Support RADIUS IETF attributes and VSA, enforcement of dACLs, VLAN, post health check application install etc.</li> <li>19. REST/SOAP/XML APIs for integration.</li> <li>20. Ability to perform caching of MAC address post guest authentication.</li> <li>21. Support protocol / Framework - RADIUS Dynamic Authorization, TACACS+, RadSec, EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS), PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD), TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP), EAP-TLS, PAP, CHAP, MSCHAPv1, MSCHAPv2,</li> </ol>
--	--

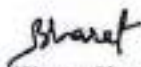
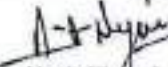
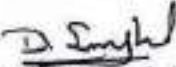
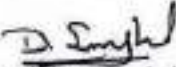

Sharat *[Signature]* (On leave) D. Smith M B



	<p>EAP-MD5, OAuth2, WPA3, Windows machine authentication, SMB v2/v3, Online Certificate Status Protocol (OCSP), SNMP generic MIB, Common Event Format (CEF), Log Event Extended Format (LEEF)</p> <p>22. Polling of an Active Directory Domain Controller and SSO Portal based authentication with tracking widgets to reduce the need for repeated authentications and Monitoring of RADIUS Accounting Start records.</p> <p>23. Support of built-in certificate authority. Certificate management for enterprise VPN deployment and 802.1X.</p>
<b>Management</b>	<p>1. Centralized GUI Management with dashboard with policy configuration templates, reporting and troubleshooting tools.</p> <p>2. Must provide role-based network access control and visibility in single pane of glass for the entire infrastructure spread across multiple Network Locations / Zones.</p> <p>3. Built-in guest management and device/user onboarding.</p>
<b>General</b>	<p>1. Hardware supplied should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent.</p> <p>2. Hardware supplied should be rack mountable with required accessories for rack mounting.</p>

### 3.6. Technical Specification of Endpoint Detection and Response (EDR) solution

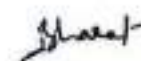
<b>Requirement of EDR Licenses</b>	EDR licenses are required for 1500 end-points (Desktop & Laptops) with subscription of 05 Years. EDR solution is required for both Internet and Intranet Subnet. All the features of EDR mentioned in this RFP should be available in both internet and intranet subnet. The distribution of the licenses for internet and intranet systems will be conveyed at the time of actual deployment.
<b>Hosting Environment / Deployment Option</b>	On Premises
<b>Prevention Features</b>	<ol style="list-style-type: none"> <li>1. Protection from exploitation of specific application</li> <li>2. Prevent privilege escalation</li> <li>3. Prevent process hollowing attacks</li> <li>4. Protect from Encrypting File System attacks</li> <li>5. Protection from malicious webpages</li> </ol>

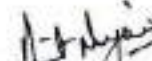
 (Bharat Bhushan)
  (Amit Nigam)
 (On Leave)
  (Prashant V Holkar)
  (Dhruv Singhal)
  (Ashish Choudhary)

	<ol style="list-style-type: none"> <li>6. Protection from malicious IP and domains</li> <li>7. HIPS/Exploit Prevention - Application Control Threat Intelligence</li> </ol>
<b>Reducing Attack Surface Features</b>	<ol style="list-style-type: none"> <li>1. Block all applications from creating child processes</li> <li>2. Block execution of potentially obfuscated scripts</li> <li>3. Block Win32 API calls from Office macro</li> <li>4. Block applications from creating executable content</li> <li>5. Block against loading</li> <li>6. DLL files from untrusted folders</li> <li>7. Block applications from injecting code into other processes</li> <li>8. Block JavaScript or VBScript from launching downloaded executable content,</li> <li>9. Block executable content from email client and webmail</li> <li>10. Block executable files from running unless they meet a prevalence, age, or trusted list criterion,</li> <li>11. Use advanced protection against ransomware</li> <li>12. Block process creations originating from PSEXEC and WMI commands</li> <li>13. Block untrusted and unsigned processes that run from USB</li> <li>14. Block applications from creating child processes</li> <li>15. Block Adobe Reader from creating child processes</li> <li>16. Block persistence through WMI event subscription</li> </ol>
<b>Network Protection Features</b>	<ol style="list-style-type: none"> <li>1. Protection across browsers, scripts, shells, Protection from malicious SMB, Psexec, WMI injections from other devices in the network.</li> </ol>
<b>Malware Protection (AV) Features</b>	<ol style="list-style-type: none"> <li>1. Blended Threats/Malware Protection</li> <li>2. Automated Malware and Threat Removal</li> <li>3. Suspicious email attachments scanning</li> <li>4. Enhanced remediation capabilities</li> <li>5. Global Threat Intelligence with Reputation Source configuration capability</li> <li>6. Advanced Protection against file less attack methods.</li> <li>7. Memory Protection</li> <li>8. Root cause analysis/Threat cases for the malware incidents</li> <li>9. Advance machine learning and AI based malware protection</li> </ol>
<b>Device Control Features</b>	<ol style="list-style-type: none"> <li>1. Block Specific Devices</li> <li>2. Allow specific devices</li> <li>3. Monitor files written to USB devices</li> <li>4. Disallow execution of Unsigned/Untrusted files from USB</li> <li>5. Custom detection and response of device control Automatic Threat detection on USB mount</li> </ol>
<b>Threat Detection Features</b>	<ol style="list-style-type: none"> <li>1. Comprehensive detection of Advanced Kernel Exploitation and In Memory Attack - Kernel sensors,</li> <li>2. Pre-written SQL queries for IT operations</li> </ol>

Shrest  
 D. Singh (On leave) → D. Smith in S.

	<ol style="list-style-type: none"> <li>3. Solution should have the ability to create Forensic Snapshots and perform detailed analysis on demand</li> <li>4. Threat analysis/correlation of 3 months data.</li> <li>5. Historical Search</li> <li>6. Real time search</li> <li>7. On demand data collection to capture active processes and network connections</li> <li>8. Lists applications in the startup section of the registry and their reputation scores</li> </ol>
<b>Automatic Investigation Features</b>	<ol style="list-style-type: none"> <li>1. Automatic AI-Guided Intelligent alert correlation and analysis with no manual intervention</li> <li>2. Recommendations on threat mitigations for approvals like kill process</li> <li>3. Machine isolation etc</li> <li>4. Suspicious event detection and prioritization,</li> <li>5. Reduced time to mitigate</li> <li>6. Automatically gather</li> <li>7. Summarize and visualize evidence</li> <li>8. Different views for different users</li> </ol>
<b>Threat Remediation Features</b>	<ol style="list-style-type: none"> <li>1. Automatically applies surgical remediation &amp; containment steps to reduce risk</li> <li>2. Ability to remediate completely in memory attacks - due to our presence in Kernel</li> </ol>
<b>File Level Actions Features</b>	<ol style="list-style-type: none"> <li>1. Block</li> <li>2. Quarantine</li> <li>3. Allow</li> <li>4. Collect</li> <li>5. Restore</li> </ol>
<b>System Level Actions</b>	<ol style="list-style-type: none"> <li>1. Isolate Machine</li> <li>2. Run AV</li> <li>3. Collect Investigation Package</li> <li>4. Kill Process</li> <li>5. Stop Service</li> <li>6. De-register DLLs</li> </ol>
<b>Advanced Threat Hunting Features</b>	<ol style="list-style-type: none"> <li>1. Hunting for IOCs and IOAs</li> <li>2. Shows a process tree of currently running processes</li> <li>3. Lists the activity history of a process</li> <li>4. Hunt for specific Application behaviors like process creations etc.</li> <li>5. Hunt for User behavior like web browsing, Application usage</li> <li>6. file creation</li> <li>7. Hunt for registry creation and modifications</li> <li>8. Hunt for Logon events and activities</li> <li>9. Hunt for command lines and PowerShell activities</li> <li>10. Hunt for Network info and events</li> </ol>
<b>Threat Experts Features</b>	<ol style="list-style-type: none"> <li>1. Targeted attack notification</li> <li>2. Collaborate with experts</li> <li>3. on demand (Paid service)</li> </ol>

  
(Bharat Bhushan)

  
(Amit Nikam)

(On leave)   
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

<b>Integrated Security and Insights Features</b>	<ol style="list-style-type: none"><li>1. Identify threat campaigns prior to an attack</li><li>2. Machine Learning analysis to determine security posture against attacks</li></ol>
<b>EDR Management</b>	<ol style="list-style-type: none"><li>1. EDR Manager should be an appliance based (Hardware / Virtual / Software). In case of Virtual / Software based solution, all the required and supporting hardware must be supplied.</li><li>2. Separate EDR Management Servers are required for Intranet and Internet as there is an airgap between these two networks. The EDR Management servers are deployed in HA mode with primary in DC and secondary in DR</li></ol>

*Shant*

*A. D. Singh (On leave) -> Smital A. S*

#### 4. Passive Elements:

Item	Quantity (in Nos.)
Multimode Fiber Patch Cables (3 Meters) Nos.	400
Single Mode Fiber Patch Cables (5 Meters) Nos.	50
Cat 6 Patch Cables (5 Meters) Nos.	50
Cat6 Patch Cable (1 Meter) – For Patch panel to Switch Connectivity	1500

#### 5. License, Support and Warranty:

1. 24X7 support with 4 hrs. response time. For Hardware replacement (RMA) should be dispatched within NBD
2. Telephonic, e-mail/chat support with call logging (single point of Contact) mechanism must be provided on 24x7x365 basis by OEM. Also, must provide escalation matrix.
3. The bidder must provide 5 years comprehensive OEM warranty with the following:
  - a. Subscription of all software, Firmware and associated Licenses (of all features) and effective from day one.
  - b. Warranty for all the supplied Hardware and software.
  - c. Bidder must ensure that all features of the proposed solution is functional without requirement of any additional procurements of Hardware, Software, Subscriptions and Licenses from day one. Any components/ accessories to meet the solution, should be included in the quote. Bidder must supply the items missed/ short shipped at no additional cost.
  - d. All hardware, software replacements and delivery must be taken care by the bidder with no financial implications to NIA.
  - e. Online upgradation of firmware/software/patches as and when required.
  - f. The Total solution must come with the latest and updated version (Hardware, Software, and Firmware) available at no extra cost.

  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)   
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

- g. All the devices should support automatic patch updates like IPS signature updates, Antivirus signature updates and patch updates must be provided by OEM.
4. The seller warrants that the goods supplied under the contract conform to technical specifications prescribed and shall perform according to the said technical specifications.

## 6. Scope of Work

The bidder is expected to do following but not limited to:

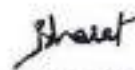
1. Requirement Study, Propose and Deploy.
2. Supply, Implementation, Training, Warranty & Support.
3. Bidder is responsible to supply and install the required items across 19 NIA Offices as per the requirement of NIA. The actual branch-wise distribution count of the items will be conveyed at the time of implementation.
4. Ensure that all aspects of installation, de-installation, integration, configuration, re-configuration, Customization (as per solution requirement), enhancements, updates, upgrades, bug fixes, problem analysis, and performance analysis for the proposed solution.
5. The bidder/OEM should ensure smooth and complete integration of proposed equipment and ensure inter-compatibility of all the sub systems and components comprising the total solution. For proper integration following should be ensured by bidder:
  - a. Layer3/core Switches, Layer2/Access switches and SDN controller should be from same OEM.
  - b. Complete SD-WAN solution should be from single OEM i.e. SD-WAN Type-01 routers, Type-02 routers and SD-WAN controller should be from same OEM
6. Documentation of the implementation and operation process.
7. All power sockets/fixtures at the installation site are Indian type.
8. Bidder need to provide all required Hardware and Software for implementation of proposed solution without proposing any additional cost to NIA.
9. Provide technical training for all the components of the proposed solution (05 days onsite training) and do knowledge transfer to the NIA team (10 members).

*Sharat*      *A. Singh* (On leave)      *D. Sankh*      *N. B.*

## 7. Instruction to Bidders

1. All the necessary documents supporting the specifications (mention in section) must be provided along with the bid. Bidder must submit detailed (like Document / URL References with Page No. / Text highlighted, screenshots (if required)) technical compliance statement.
2. The vendor must list detailed bill of materials for all the items and sub-items offered along with part numbers. Any item given as complied and not listed in bill of material is liable to be treated as non-compliant.
3. Pre-Qualification Criteria:

Sl#	Specific Qualification Criteria	Document/ Information to be submitted with proposal	Compliance (Yes/No/NA)
1	The Bidder must be incorporated and registered in India under the Indian Companies Act 1956/2013 LLP Act 2008 / Partnership Act 1932 & subsequent amendments thereto and shall have been operating for the last five years as on 31st March 2023 (including name change/ impact of mergers or acquisitions).	Valid documentary proof of: <ol style="list-style-type: none"> <li>i. Certificate of incorporation / Certificate of Commencement</li> <li>ii. Certificate consequent to change of name if applicable.</li> <li>iii. Copy of Memorandum of Association (if applicable) (In addition, the Bidder shall also submit last 5 Audited balance sheets)</li> </ol>	

  
(Bharat Bhushan)

  
(Amit Nigam)

 (On Leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

Sl#	Specific Qualification Criteria	Document/ Information to be submitted with proposal	Compliance (Yes/No/NA)
2	The Bidder must have a registered number of: • GST Registration. • Income Tax / PAN / TAN.	i. Certificate of GST registration. ii. Copy of PAN / TAN / Income tax number.	
3	The Bidder must have positive net worth during the last three financial years (i.e., 2021-22, 2022-23 & 2023- 24).  Bidder should have an average Annual turnover of minimum INR 10 Crores in the last 3 financial years. For the purpose of this criterion, the annual turnover of only the bidding entity will be considered.	Audited Balance Sheets for last 3 financial years, i.e., 2021-22, 2022- 23& 2023-24 where financial turnover is segregated. Every sheet shall be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for last 3 financial years.	
4	The Bidder must have executed at least 3 SD-WAN/SDN/ Network Design & implementation projects during last 3 years at premier Govt Indian institutions or other govt PSU organizations or reputed organization in India. (03 years of past Experience).	Copy of Letter of Award (LOA)/ Purchase Order (PO)/ Work Order (WO)/ Contract/ Agreement, containing Scope of Work (SOW) and Order Value or Certification of Acceptance for ongoing projects/ Completion certificate for	

Sharat [Signature] (On Leave) → [Signature] M J.

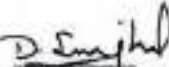


Sl#	Specific Qualification Criteria	Document/ Information to be submitted with proposal	Compliance (Yes/No/NA)
	At least one of the projects should be across 10+ branches/locations.	completed projects by client or Certificate by the Company Secretary of the Bidder indicating the scope of work, in case of projects are under non-disclosure agreement and confidentiality. The WO/ letter shall be in the name of the Bidder and clearly mention the scope of work.	
9	The Bidder shall submit certification for ISO 9001	The bidder should have valid ISO 9001 certification. Please attach a copy of the certificate.	
10	Bidder shall provide valid OEM Authorization Certificates for all the products quoted as well as certify that the proposed product is not declared end of sale.	Copy of MAF certificate for all solution proposed as part of Bid.	
12	The Bidder must not be blacklisted by Central /State Government Ministry/ Department/ PSU/ Government Company. Bidder	Self-certification duly signed by authorized signatory on Bidder's firm letter head.	

  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)

  
(Ashish Choudhary)

SI#	Specific Qualification Criteria	Document/ Information to be submitted with proposal	Compliance (Yes/No/NA)
	also must not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry / Department/ PSU/ Government Company		

*Bharat*      *A. J. Singh* - (On Leave)      *D. S. Singh*      *1. 8*

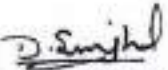
8.BoQ (Price Bid Format):

S.No.	Items	Qty	Units	GST@	Total Amount in INR & Words
1	Layer 3 Core Switch	60	Nos.		
2	Layer 2 Access Switch	116	Nos.		
3	Network Orchestration Platform / SDN Controller	02	Nos.		
4	SD-WAN Type-01	34	Nos.		
5	SD-WAN Type-02	04	Nos.		
6	SD-WAN Controller	02	Nos.		
7	AAA	02	Nos.		
8	End Point Detection and Response (EDR) solution	1500	users.		
9	Multimode Fiber Patch Cables (3 Meters) Nos.	400	Nos.		
10	Single Mode Fiber Patch Cables (5 Meters) Nos.	50	Nos.		
11	Cat 6 Patch Cables (5 Meters) Nos.	50	Nos.		
12	Cat6 Patch Cable (1 Meter) - For Patch panel to Switch Connectivity	1500	Nos.		
13	Technical Training	05	Days		
14	Installation, commissioning and Testing	-	-		
	<b>Total</b>				

  
21/06/24  
(Bharat Bhushan)

  
(Amit Nigam)

(On Leave)  
(Prashant V Holkar)

  
(Dhruv Singhal)  
21/6/24

  
(Ashish Choudhary)