S.N.	Page Number	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	NABARD Comments
1	Page 12. Clause-4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Kindly modify this point as follows to allow greater participation - NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform or VMWare ESXI or Microsoft Hyper-V or KVM or as a physical appliance	Refer to Corrigendum
2	Page 51, Clause 14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Features like malware behaviours, malware type, severity, source and destination of attack which is more of NBAD or AV functionalities. NAC ensures that the requred services like AV/FW/AntiMalware, etc. are up and running to ensure endpoint is not comprimised. Additionally, NAC can take required action (block, quarantine or notify) by receiving an alert from SIEM solution. Please rewrite the clause as - **Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, User, Endpoint, etc.** Pls delete - network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	No Change
3	Page 52 , Clause 36-a	a. Ability to run custom scripts and policies	Running custom scripts on endpoints results in undesired end result and can be issue for IT team espacially at remote branches with limited or no local IT support. Please modify as - **Ability to run custom script or policies**	No Change
4	Page 53, Clause 40	The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunnelling (FAST), and EAP-Transport Layer Security (TLS)	EAP FAST is obselete protocol with security vulnerabilities. Please modify as - **The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), and EAP-Transport Layer Security (TLS).**	Refer to Corrigendum
5	Page 53, Clause 41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security Group Access (SGA) tagging is a vendor specific feature hence request you to remove this and change this point to - **Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments and URL redirect**	Refer to Corrigendum
6	Page 54, Clause 49	The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto Remediation.	Recommended option is to use Domain GPO policy as it provides better management and the patches can be installed even before the user login to windows. Auto-remediation through NAC may not be the right approach specifically when the patches/updates are missing in bulk. In such scenarios, it may take significant time to complete the installation of all missing patches which could impact the users activity. Some patch installation requires a reboot of windows machine, if the documents on which user is working are not saved, user will lose his data due to machine reboot performed by auto-remediation. Kindly modify this point as thsi will enabel added flexibility to NABARD IT **The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation.**	Refer to Corrigendum
7	Page 56, Clause 71	Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	Since NAC act as a Radius server, it can directly authenticate the Guest and other users either with locally created accounts or with integration through external directory servers like AD, LDAP, etc. and hence, NAC doesn't require to act as an IDP. Our NAC can act as a Service Provider for SAML 2.0 authentication to allow user authentication with existing third party SAML database server (IDP). Kindly modify this pint as; **Solution must support Security Assertion Markup Language (SAML) 2.0 authentication.**	Refer to Corrigendum
S.N.	**Page Number**	**Clarification point as stated in the tender document**	**Comment/ Suggestion/ Deviation**	**NABARD Comments**
1	Page 12. Clause-4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Our NAC Platform not tested on Nutanix platform. Kindly modify this point as follows - NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform or VMWare ESXI or Microsoft Hyper-V or KVM or Physical appliance	Refer to Corrigendum

2	Page 51, Clause 14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Features/ functionality such as malware behaviours, malware type, severity, source and destination of attack which is more of NBAD or AV functionality. NAC will ensure that requred services like AV/FW/AntiMalware etc. are up and running to ensure endpoint is not comprimised. Additionally, NAC can take required action (block, quarantine or notify) by receiving an alert from SIEM solution. Please modify clause as - **Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, User, Endpoint, etc.** Pls delete - network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	No Change	
3	Page 53, Clause 41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security Group Access (SGA) tagging is a vendor specific feature. Request you to remove this and change this point to - **Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments and URL redirect** and ~~Security Group Access (SGA) tagging.~~	Refer to Corrigendum	
4	Page 54, Clause 49	The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto Remediation.	Windows Patch update can be triggered in multiple ways i.e., through Domain Group Policy, by prompting the user to start required installation or Registry modification, . Recommended approach is using Domain GPO policy as it provides better management and the patches can be installed even before the user login to windows. Auto-remediation through NAC is not be the right approach specifically when the patches/updates are missing in bulk. In such scenarios, it may take significant time to complete the installation of all missing patches which could impact the users activity. also at times patch installation requires a reboot of windows machine. For More flexibility to NABARD kindly modify this point as follows - **The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation**	Refer to Corrigendum	
Sr. No.	**Page No.**	**Clause**	**Existing clause**	**Query**	**NABARD Comments**
4	48	10.3 Annexure –III: Minimum Eligibility Criteria- Experience The Bidder should have supplied and implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI sector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the Bidder should be submitted.	Letter from the OEM on their letter head stating that SI is the authorized partner of OEM and also that the OEM shall support the solution for the entire period. If the Bidder himself is OEM, a self-certification should be submitted.	Is it mandatory for bidder to have minimum experience of 3 customers similar project done ? Out of which 1 customer should be from BFSI segment ? Is it okay if we share our respective OEM work experience of 3 customers instead of bidder ?	Bidders and OEM have to submit 3 POs repsectively.
Sno	**Page No**	**Section No**	**Clarification point as stated in tender document**	**Comment/Suggestion/Deviation**	**NABARD Comments**
1	11	4.2.2 General Requirements	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Aruba Clearpass supports VMWare Vsphere, Microsoft HyperV,KVM on CentOS & Ubuntu. We request you to change the clause to include these Hypervisors.	Refer to Corrigendum
2	50	10.4.1.1	The offered solution should provide comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services for a total of 10,000 network and endpoint devices. (+2000 additional licenses)	Does this 10000 include network devices like routers / switches/wireless controllers etc. If yes what is the total count of such devices?	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder.
3		10.4.1.2	The solution should support health-check / integration of minimum 4000 Desktops.	The total licenses required on day 1 is 10000. This includes 4000 desktops. Will there be any laptops that will also connect and need health check?	Yes
4		10.4.1.3	The solution should support health-check / integration of minimum 1000 Guest Users.	We request you to provide clarity on the authentication mechanism for Guests. Also is health check necessary for Guests devices?	LDAP protocol. And yes, health check up necessary for guests.

5		10.4.1.5	Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access using SPAN or mirror traffic.	As per previous clause 10.4.1.4 , the solution should be a pre admission control solution.Aruba solution is a zero trust solution where we authenticate the user and then grant network access. This is achieved through 802.1x mechanism. we request you to amend the cluase as " **Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access"**	Refer to Corrigendum
6		10.4.1.9	Solution shall use Agent based approach for detection of unauthorised access via network activities analysis from the endpoints	Point no 4 states " The solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution" In line with this approach, 802.1x mechanism ensures that only authenticated users get network access.This access grants them necessary authorisation. An agent installed on the machine only checks for the health status and reports its back to the NAC server. The agent will come into picture only after authentication and authorisation is done. Hence we request you to consider deletion of this clause as it contradicts with the point no 4 stated above.	Refer to Corrigendum
7	51	10.4.1.14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	The functionality specified is that of a security device like NGFW, anti malware solution etc. The NAC can integrate with the security solution so that it receives notitfication of such alerts and takes appropriate action of blocking network access for those endpoints/ devices. NAC solution can only act as a gatekeeper and permit/deny access to the network based on certain policies/events.	No change
8	52	10.4.1.36	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of:		No change
			a. Ability to run custom scripts and policies		
			b. Hardware/Asset Management information	Please help to understand what is meant by asset management information. The NAC solution is not an asset mgmt solution. It can provide with the count of connected devices and their broad categories. We request you consider deletion of this clause.	
			c. Event driven properties for compliance checks		
10		10.4.1.41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security group tagging is proprietery to an OEM. This also creates a dependency on the underlying network infrastructure. Since this contradicts the point 34 which mentions vendor agnostic switch infra, we request you to remove this clause.	Refer to Corrigendum
11		10.4.1.45	The proposed NAC solution should integrate with Firewalls (e.g. Checkpoint, Fortinet, Sonicwall)	The firewalls should be NGFW / user aware firewalls and they should support API integration with the NAC solution.	No change
12		10.4.1.47	The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Please provide clarification as to what is Microsoft Factory server? Is it intended that the NAC solution should integrate with Azure AD environment? Please provide clarity about Factory Server.	Refer to Corrigendum

13		10.4.1.50	Should able to integrate with major leading vendor vulnerability assessment tools & ATD solution, so that Solution should respond rapidly to compromised devices on network to prevent threat propagation & data breaches and quarantine infected endpoints	These vulnerability assessment tools should be capable of API based integration.	No change
14	56	10.4.1.64	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin	The NAC solutions have a fixed number of fields. The dashboard can be customised by choosing from the available fields only. No new fields can be added to the dashboard. The management console is centralised.	No change
15	56	10.4.1.69	Automatic endpoint device provisioning/ installation with approval required option for on boarding	We understand this refers to Bring Your Own device. Please help to understand the count of such devices so as to size the solution accordingly.	The solution should be capable of provisioning. The actual device counts will be shared with selected bidder
Sr.No	**Pg. No**	**Section Number**	**Clarification point as stated in the tender document**	**Comment/ Suggestion/ Deviation**	**NABARD Comments**
1			Other Information	Please provide total Number of L2/L3 devices details , Are all device are managable?	All devices are manageable, actual number shall be shared with the successful bidder
2	11	4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Nutanix support multiple hyperviser (https://www.nutanix.com/info/hypervisor) , Request you to repharse as "NAC Solution to be installed in HA at both DC and DR on the Acropolis/KVM/VMware ESXi/Microsoft Hyper-V Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform"	Refer to Corrigendum
3	11	4.2.12	The Bidder shall engage one Technical Account Manager from OEM for a period of 1 year and an Onsite Engineer for the entire contract period	Request you repharse as "The Bidder shall engage one Technical Account Manager for a period of 1 year and an Onsite Engineer for the entire contract period"	No Change
4	12	4.3.2	The Bidder/ Vendor shall provide training to at-least two batches of NABARD officials for the following each type of training. 4.3.2.1. User Training. 4.3.2.2. System Administration training. 4.3.2.3. Top executive awareness program.	Does this mean training for 6 batches?	These are the topics to be covered. Training in 2 batches.
5	12	4.3.3	Training shall be for a day per batch and it should be at least three days with a batch size as mutually agreed by the Bank and Vendor/Bidder	Is the training for 1 day per batch or 3 days per batch?	3 days per batch
6	14	4.7.6	SLA for Incidents Handling:	How many resources are required onsite? Is the bank expecting 24 x 7 onsite support?	One resource , between 9.00 AM to 5 PM (24x7 call support)
7	15	4.12.1	Power OnSelf Test (POST) will be conducted by Bidder at the site in presence of NABARD officials and /or nominated person. Installation report (IR) should be submitted after complete implementation of systems. NABARD will take over the system on successful completion of above acceptance test.	Point Need to be deleted as this is software based NAC solution deployement and hardware would be provided by bank.	No Change
8	29	8.4.1	50% of Total Cost of Solution (indicated in the final commercial bid) after successful configuration and implementation of the solution at the Data Center of NABARD and DR Site, covering all HO end-point devices.	Request- Please change it as 100% payment against delivery for Cost of Licenses And 100% payment for Implementation cost on sign off.	No Change
9	32	8.10.1	Phase –I Delivery of Licenses and Pilot Implementation (On Nutanix –VM)	NABARD is looking for separate pilot setup? We have to propose additional license for Pilot setup? Please provide total license require for pilot setup.	Refer to Corrigendum

10	48	10.3	Financials The Bidder should have a minimum annual turnover of Rs.30.00 crore and should also be in operating profit during the last three financial years, viz., 2017-18, 2018-19 & 2019-20 The Net worth of the Bidder Company should be positive as on 31 March 2020	Please make the following changes as: The Bidder should have a minimum annual turnover of Rs.20.00 crore and should also be in operating profit during the last three financial years, viz., 2017-18, 2018-19 & 2019-20 The Net worth of the Bidder Company should be positive as on 31 March 2020	No Change
11	49	10.3	Technical Support The Bidder/OEM should have 24*7 Technical Assistance Center in India for customer support. The Bidder / OEM should have a Toll Free number facility for call logging within India.	Request to relax the requirement for Toll Free Number. Rephrase as Technical Support "The Bidder/OEM should have 24*7 Technical Assistance Center in India for customer support. The Bidder / OEM should have a contact number facility for call logging within India."	No Change
12	49	10.3	The OEM should possess ISO 27001 series certification	ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties (https://www.iso.org/isoiec-27001-information-security.html) It must be applicable to bidder and not OEM Request you to repharse as " The Bidder should possess ISO 27001 Series certification"	No Change
13	50	10.4.1	2.The solution should support health-check / integration of minimum 4000 Desktops.	As per RFP total license is 10000 , what are the other 6000 devices? Ideally The Solution should capable enough not only for Campus infrastructure but also with Data Center(Virtual or physical) , IOT (Printer/Scanner/IP Phone/IP Camera/ Smart PDU / Smart Rack etc)& cloud for security risk assessment & incident response. IoT (Printer/Scanner/IP Phone/IP camera/Netowrk Device) Risk Assessment : The solution should be able to identify all network devices such as routers, switches,IOT's devices using factory default or Weak/common credentials.Kindly repharse as "The solution should support health-check / integration of minimum 10000 devices."	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder.

14	50	10.4.1	4.The solution should be able to control the user even before IP address is assigned. It should act as a preadmission solution	Ideal NAC approach recommends that pre-connect controls should be implemented only after an initial post-connect deployment to establish device visibility, develop security policies and assess their impacts on users. A gradual transition from post- to pre-connect control can help avoid unnecessary blockage of authorized users due to abrupt introduction of new security policy. Incremental deployment allows security and operations teams the necessary time to identify affected devices, measure operational impacts and adjust policies as necessary before full enforcement begins. Request you to re-pharse as "Solution must support both post-connect & pre-connect addmission controls, NAC control should be implemented only after an initial post-connect deployment to establish device visibility, develop security policies and assess their impacts on users."	No Change
15	50	10.4.1	6.Solution should have the capability of traffic log retention for a period of 1 year.	Traffice log retention for the period of 1 year is Log sever capability & not a NAC Solution Capability. Request you to remove this point or Repharse as "For logs retention for a period of 1 year , Solution should have the capability to forward logs to Syslog/SIEM solution. "	Refer to Corrigendum
16	50	10.4.1	9.Solution shall use Agent based approach for detection of unauthorized access via network activities analysis from the endpoints	Most agent based approaches have a challenge of additional opertational overheads of agent installation and management. NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.The Solution should capable enough not only for Campus infrastructure but also with Data Center(Virtual or physical) , IOT (Printer/Scanner/IP Camera/IP Phone etc) for security risk assessment & incident response.	Refer to Corrigendum
17	51	10.4.1	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Not a functionality of NAC. Request to remove this point. This functionality is provided by IPS/IDS or Network Behaviour Anomaly Detecton solutions.	No Change

18	52	10.4.1	28.The proposed solution must support a managed switch environment having 802.1 x support.	This should be applicable in both managed and unmanaged switch environments." NABARD is having unmanaged switches where switch may not support 802.1x Kindly repharse "The solution should support both 802.1X and Non-802.1X Architecture." The support for Non-802.1X Architecture will allow early integration with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployments. NABARD can then take its own time to upgrade the infrastructure to support 802.1x at its own pace and doesn't make it a deterrent to the NAC deployment.	No Change
19	52	10.4.1	29.The solution must support agent-based deployment and provide complete posture analysis.	Large organization have 30-40% of the devices which will not support agent.It is not a good idea to Completely depend on agent. Request you to remove the point & Add below Points -Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , Printers , Scanners etc. -The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important for NABARD to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.	No Change
20	52	10.4.1	33.The solution should support MAC Address Bypass (used for devices which do not support MAC id) and utilize other available identity of the endpoint to apply the proper rules for access.	Large organization have 30-40% of the devices which will not support 802.1x.It is not a good idea to create a repository of MAC address to whitelist. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. also MAC address repository should be uptodate at any point in time to meet security aspect. Request you to remove the point & Add below Points -Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , Printers , Scanners etc. -The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important for NABARD to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible. -The Solution should capable enough not only for Campus infrastructure but also with Data Centre(Virtual or physical) , IOT & public cloud(Amazon/Azure) for security risk assessment & incident response -The solution should support both 802.1X and Non-802.1X Architecture in single deployment. The support for Non-802.1X Architecture will allow early integration with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployments (there is no option to deploy	No Change

21	52	10.4.1	35.The solution should have a provision to support non- NAC capable hosts (i.e., IP phones, IOT's etc.) based on Mac address or other parameter and it should support exception lists for non-NAC capable hosts.	NABARD may have have 3000-4000 of the devices which will not support 802.1x/Non-NAC capable host.It is not a good idea to create a repository of MAC address to whitelist. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. also MAC address repository should be up to date at any point in time to meet security aspect. Request you to remove the point & Add below Points -Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , Printers , Scanners etc. - IoT (Printer/Scanner/IP Phone/IP camera/Netowrk Device) Risk Assessment : The solution should be able to identify all network devices such as routers, switches,IOT's devices using factory default or Weak/common credentials	No Change
22	53	10.4.1	38.The solution should provide full Terminal Access Controller Access Control System (TACACS)+ capability including enable password, configuration present for different NAD types, TACACS+ proxy etc.	NABARD may already uses PIM or Network device authentication solution. TACACS+ is not a NAC funcationility. Request you to repharse as " The solution should provide full integration Terminal Access Controller Access Control System (TACACS)+ capability."	No Change
23	54	10.4.1	47.The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Seems like a typo it must be Microsoft Active directory server, Is Our under standing is correct? What type of authentication NABARD is looking for IP Priner / IP phone / IP camera / Smart PDU / Data Center Server etc , which may not integrated with Microsoft Active Directory?	Refer to Corrigendum
24	54-55	10.4.1	52.Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal for a specific user for a selected period of time. The report should provide the following detail •Logged in Date and Time •Portal User (who registered the device) •MAC Address •Identity Group •Endpoint Policy •Endpoint Policy ID •NMAP Subnet Scan ID •Device Registration Status	Specific to single OEM . Request you to delete "https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_prof_pol.html"	No Change
25	55	10.4.1	54.The solution should offer a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations. The solution should enable administrators to centrally configure and manage profile, posture, guest, authentication, and authorization services in a single web-based GUI console, simplifying administration by providing consistency in managing all these services.	Kindly repharse as "The solution should offer a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations. The solution should enable administrators to centrally configure and manage profile, posture, guest, authentication, and authorization services in a single web- based / GUI console, simplifying administration by providing consistency in managing all these services. "	No Change
26	56	10.4.1	66.Automatically configure and provision mobile devices such as MAC, iOS, Android, Chromebook etc. enabling them to securely connect to enterprise network.	Need to understand the use case. Is it about allowing BYOD / Guest devices to the network?	No Change

27	56	10.4.1	68. Capable to define the number of devices that can be on-boarded per user and validity period.	Such feature is required only in cases where BYOD devices are allowed to connect to corporate network. As per our understaning of a Banking environment BYOD devices should not be alowed to connect to corporate network. Request to reconsider this point	No Change
28	56	10.4.1	69. Automatic endpoint device provisioning/ installation with approval required option for on boarding	What is the expected use case here? NAC cannot install an endpoint. Are we talking about onboarding of Guest device?	Yes
29	56	10.4.1	71.Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	NABARD is already having Cloud based AD? What is the exact use case NABARD want to achieve via SSO & SAML?	No Change
30	58	10.5	Cost of Technical Account Manager from OEM for a period of One Year after the project goes live (One Day per week Onsite and remaining days remote support)	Request you repharse as "Cost of Technical Account Manager from Bidder for a period of One Year after the project goes live (One Day per week Onsite and remaining days remote support) "	No Change
31	90	2.1.3	Audit Services	The services provided to NABARD as part of this tender would not amount to a managded service provider. Request NABARD to remove this section as no customer data would be stored, retained or processed at the bidders premises or data centres. All software and solution required for this tender are installed at NABARD datacentres	No Change
32			Point need to be added	The solution should support all versions of Windows starting from Windows XP, all versions of OS X starting from OS X 10.8 and major Linux versions (atleast CentOS, Debian, Fedora, Red Hat Enterprise Linux, Open SUSE, SUSE Enterprise, Ubuntu) for complete posture assessment both agent based and agent-less.	Not Accepted
33			Point need to be added	IoT (Printer/Scanner/IP Phone/IP camera/Netowrk Device) Risk Assessment : The solution should be able to identify all network devices such as routers, switches,IOT's devices using factory default or Weak/common credentials	Not Accepted
34			Point need to be added	The solution should support both 802.1X and Non-802.1X Architecture. The support for Non-802.1X Architecture will allow early integration with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployments.". The SBIFMPL can then take its own time to upgrade the infrastructure to support 802.1x at its own pace and doesn't make it a deterrent to the NAC deployment.	Not Accepted

35			Point need to be added	"The NAC solution should detect endpoint state changes (AV disabled, execution of an unauthorized application, etc) and perform auto-remediation e.g. it should detect and disable unauthorized dual-homed endpoints. It should be done on a continuous basis rather than waiting for the next authentication event to happen.". It is important today as the endpoints security posture can change at any split of a second in these times of highly sophisticated targeted attacks. Hence, it is critical to detect endpoint state changes and perform auto-remediation on a continuous basis rather than waiting for the next authentication event to happen.	Not Accepted
36			Point need to be added	The NAC solution should support existing network infrastructure i.e Managed & unmanaged swiches to block or limit the non-complied or rough devices behind that.	Not Accepted
37			Point need to be added	The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.	Not Accepted
38			Point need to be added	The Solution should capable enough not only for Campus infrastructure but also with Data Center(Virtual or physical) , IOT & cloud for security risk assessment & incident response	Not Accepted
39			Point need to be added	The solution should provide complete inventory of all applications, running processes , Services and open ports on an endpoint.	Not Accepted
40			Point need to be added	The proposed solution should support automated remediation system including starting madetory process/Services, killing blacklisted process/Services, setting registry keys, starting antivirus, update anti-virus, starting windows updates and running custom scripts (must be available for Windows, Linux and MAC-OS) Help desk and self-service remediation allowing for load reduction through end user self- support and automatic remediation.	Not Accepted
41			Point need to be added	The proposed NAC solution should provide out-of-the-box IOC, Hash, Malicious files scanning to discover and mitigate threats from infected endpoints. The solution must support at least the following IOC types for IOC scanning: CnC Address (Command and Control URL) , Process (Process Name, Process Hash, Process Hash Type) , File Exists (File Name, File Path) , Mutex (Mutex Name) , Registry Key (Path, Value) , Service (Service name) etc	Not Accepted

42			Point need to be added	The solution should be able to provide detection for shared directories and non-admin shares.	Not Accepted
43			Point need to be added	The solution should be able to provide detection for shared directories - admin shares	Not Accepted
44	90-91	2.13	Audit Services	Kindly remove all the points related to Audit Services since this is not relevant to the proposed solution.	No Change
45	29	8.4.1	Payment Terms: a) 50% of Total Cost of Solution (indicated in the final commercial bid) after successful configuration and implementation of the solution at the Data Center of NABARD and DR Site, covering all HO end-point devices. b) 40% Total Cost of Solution (indicated in the final commercial bid) after the configuration and implementation of the solution for all end-point devices at all RO/TE Offices. c) Final 10% of Total Cost of Solution (indicated in the final commercial bid) will be paid after 3 months from the date of acceptance of the solution by NABARD.	Request to change:90% of licenses cost on license delivery and activation of licenses. 50% of implementation cost on installation and configuration of the solution. 40% of implementation cost on complete coverage of endpoints. 10% of licenses and implementation cost on acceptance/sigoff.	No Change

Sl.No	Clause No. and Page No.	RFP Term	Clarifications and Amendments sought	NABARD Comments
1	Cl. 4.7.5./ Pg 12	The maximum penalty shall be capped at 10% quarterly charges of AMC	The maximum penalty shall be capped at 5% quarterly charges of AMC	No Change
2	Cl. 8.3.4/ Pg 29	While any increase in the rates of applicable taxes or impact of new taxes imposed by GoI, subsequent to the submission of commercial bid shall be borne by NABARD, any subsequent decrease in the rates of applicable taxes or impact of new taxes shall be passed on to NABARD in its favour. This will remain applicable throughout the contract period.	Any changes in Statutory tax at the time of invoicing to be borne by the customer	No Change
3	Cl. 8.4/ Pg 29	Cost of Licenses & Implementation Cost: a) 50% of Total Cost of Solution (indicated in the final commercial bid) after successful configuration and implementation of the solution at the Data Center of NABARD and DR Site, covering all HO end-point devices. b) 40% Total Cost of Solution (indicated in the final commercial bid) after the configuration and implementation of the solution for all end-point devices at all RO/TE Offices. c) Final 10% of Total Cost of Solution (indicated in the final commercial bid) will be paid after 3 months from the date of acceptance of the solution by NABARD.	Cost of Licenses & Implementation Cost: a) 100% of Cost of Licenses to be paid on delivery of licenses b) 100% of Cost of Implementation including Manpower upon Acceptance c) 100% of Cost of Training upon Training completion	No Change
4	Cl. 8.4/ Pg 30	AMC Cost: a) Quarterly in Arrears, upon receiving Quarterly invoices from the vendors after the start of AMC period.	AMC Cost: a) Quarterly in Advance	No Change

5	Annexure XVI/ Cl 2.11/ Pg 90	If, the Bidder fails to deliver and / or install any or all of the Licenses/ Software's mentioned in the Purchase order (PO), Purchaser shall, levy a penalty of a sum equivalent to 0.5% percent per week or part thereof of the value of purchase order subject to maximum of 10% of the purchase order value of the delayed equipment or unperformed services for that particular location	If, the Bidder fails to deliver and / or install any or all of the Licenses/ Software's mentioned in the Purchase order (PO), Purchaser shall, levy a penalty of a sum equivalent to 0.5% percent per week or part thereof of the value of purchase order subject to maximum of **5%** of the purchase order value of the delayed equipment or unperformed services for that particular location	No Change
6	Cl. 4.9.5 Pg. 15	If the Bidder having been notified fails to remedy the defect(s) within the period specified in Section-4, Purchaser may proceed to take such remedial action as may be necessary, at the Bidder's risk and expense and without prejudice to any other rights, which Purchaser may have against the Bidder under and in accordance with the Contract	We request to delete this clause.	No Change
7	Cl. 5.6.8 Pg. 19	EMD forfeiture	We seek to clarify that the EMD will not be forfeited in the event the parties are unable to sign a mutually agreeable contract.	No Change
8	Cl. 8.1 Pg, 29	Duration of Contract	We submit that any extesnion of the contract shall be on mutually agreed terms.	Yes
9	Cl. 8.3.2 Pg. 29	Once a contract price is arrived at, the same must remain firm and must not be subject to escalation during the performance of the contract due to fluctuation in foreign currency, changes in costs related to the materials and labour or other components or for any other reason.	We submit that any fluctuation in prices due to reasons beyond our control will be mutually agreed upon by both parties.	No Change
10	Cl. 8.4 Pg. 29	Payment Schedule	We request that all payments be made within 30 days from the date of the invoice.	No Change
11	Cl. 8.6.2 Pg. 31	In case of order cancellation, any payments made by the Bank to the vendor (for period for which services are not availed) would necessarily have to be returned to the Bank with interest @ 15% per annum. Further, the vendor would also be required to compensate the Bank for any direct loss incurred by the Bank due to the cancellation of the contract and any additional expenditure to be incurred by the Bank to appoint any other SP. This is after repaying the original amount paid.	We request deletion of imposition of interest. In the event of termination, we shall refund any advance amount paid to us on a pro-rata basis. Further, in the event of non-payment by the purchaser on three consecutive ocassions, we shall have the right to terminate the contract with immediate effect.	No Change
12	Cl. 8.7 Pg. 31	Termination for Default	We submit that prior to termination, we will be provided a cure period of at least 30 days. Further, purchaser shall pay all amounts due and payable to us for all services performed by us till the effective date of termination. Furthermore, we request deletion of clause 8.7.2.	No Change
13	Cl. 9.6 Pg. 34	Compliance with Applicable Laws	We submit that we will indemnify for any regulatory fines/penalties imposed by the relevant authorities on the purchaser due to a direct default on our part to comply with applicable laws.	No Change

14	Cl. 9.7 Pg. 34	Compliance in obtaining approvals/ permissions/ licenses	We submit that we will indemnify for any regulatory fines/penalties imposed by the relevant authorities on the purchaser due to a direct default on our part to comply with applicable laws.	No Change
15	Cl. 9.8.3 Pg. 35	Performance Bank Guarantee may be invoked in case of violation of any of the terms and conditions of this document or in case of deficiency / delay in implementation/services provided by the successful bidder.	We submit that the purchaser shall provide us with a cure period of at least 30 days prior to invoking PBG.	No Change
16	Cl. 9.9 Pg. 35	Forfeiture of performance security	We submit that the purchaser shall provide us with a cure period of at least 30 days prior to invoking PBG.	No Change
17	Cl. 9.10 Pg. 35	Right to Alter Quantities	We seek to clariy that any change in scope, including alteration in quantities, beyond the scope of the RFP shall follow a change request procedure.	No Change
18	Cl. 9.28.1 Pg. 39	The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidders obligation under these general conditions or for which the bidder has assumed responsibilities under the purchase contract including those imposed under any contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the bidder or bidders in connection with the performance of any system covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the purchase contract and to protect the Bank during the tenure of purchase order.	We submit that we will indemnify only for any third party claims brought against the purchaser arising out of: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of bodily injury or death.	No Change
19	Cl. 10 (Annexure XVI) Pg. 94	Vendor liability to meet the SLAs is limited to 20% cost of agreement during the year of warranty period and later the total AMC cost of duration of the AMC period in which the liability event occurred. Vendor will in no event be liable to NABARD for consequential, incidental, special or other indirect damages such as loss of profits herein whether by contract or tort, even if Vendor has knowledge of the likelihood of such damages.	We request deletion of this clause. The capping for SLAs is already provided.	No Change

20	Cl. 15 (Annexure XVI) Pg. 96	Indemnification	We will defend (settle and/or pay damages awarded by the court) the purchaser against any third party claims arising from the following: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of bodily injury or death; c. claims by any third party in respect of any IP infringement; brought against or recovered from purchaser by reasons of any act or omission on our part, our agents or employees in the performance of the contractual obligation.	No Change
21	Pg. 14 - Point 4.7.6	SLA for Help Desk Service	Please provide a Clear scope regarding this, we need to factor financials accordingly	The scope is to the extent of NAC being made live post logging of a ticket.
22	Pg. 48 - 10.3 Annexture III, Point No. 4	Experience: The Bidder Should have supplied & implemented the NAC solution in at least 3 institutions in India of which one should be in BFSI Sector, during last 3 years (i.e. since April 2017). References of top Three Projects (in terms of size of solutions) of the Bidder should be submitted	In case if Bidder is OEM, please allow submission of reference PO's through Partner Organization for the same solution. Also please consider installation report as a proof of project completion (Some customers may not have policy to issue such letters due to their internal policies). Please correct the marking scheme on Pg. no. 25 accordingly	POs from partner organisations shall be accepted in case of Bidder is OEM.
23	Pg. 49, Point No 2 OEM Experience	Experience The OEM should have implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI sector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the OEM should be submitted.	In case if Bidder is OEM, please allow submission of reference PO's through Partner Organization for the same solution. Also please consider installation report as a proof of project completion (Some customers may not have policy to issue such letters due to their internal policies) Please correct the marking scheme on Pg. no. 25 accordingly	No Change
24	Pg. 12 - Point 4.3	Training Services	is it one batch for 3 days training and 2nd batch for 3 days? Whereas page no 58 reflects "Cost of Imparting Training for 5 personnel for 5 days on NAC Solution " Please get it corrected , accordingly financials needs to be taken care of.	Refer to Corrigendum
25		NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Need clarity on the OS procurement, VM procurement and deployment.This is pre-requisite requirment and needs clarity so that NAC solution deployment will not have any challenges if these points are already taken care of.	NABARD shall create the necessary VM based on requirements submitted the vendor
26		Licenses and Pilot for DC Mumbai and DR faridabad to be compeleted within 4 weeks of PO.	Request to change to 8 weeks from PO	No Change
27		Locations refer to HO, Regional office and training establishiments	Need location final list to avoid challenges as the statement is open ended statement in the RFP.	Not applicable
28	Page 11, 4.2.2 General Requirements	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Aruba Clearpass supports VMWare Vsphere, Microsoft HyperV,KVM on CentOS & Ubuntu. We request you to change the clause to include these Hypervisors.	No Change
29	Page 50, Clause10.4.1.1	The offered solution should provide comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services for a total of 10,000 network and endpoint devices. (+2000 additional licenses)	Does this 10000 include network devices like routers / switches/wireless controllers etc. If yes what is the total count of such devices?	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder.

30	Page 50, Clause10.4.1.2	The solution should support health-check / integration of minimum 4000 Desktops.	The total licenses required on day 1 is 10000. This includes 4000 desktops. Will there be any laptops that will also connect and need health check?	Yes, Laptops are included and requires Health Check
31	Page 50, Clause10.4.1.3	The solution should support health-check / integration of minimum 1000 Guest Users.	We request you to provide clarity on the authentication mechanism for Guests. Also is health check necessary for Guests devices?	LDAP protocol. And yes, health check up necessary for guests.
32	Page 50, Clause10.4.1.5	Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access using SPAN or mirror traffic.	As per previous clause 10.4.1.4 , the solution should be a pre admission control solution.Aruba solution is a zero trust solution where we authenticate the user and then grant network access. This is achieved through 802.1x mechanism. we request you to amend the cluase as " **Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access"**	Refer to Corrigendum
33	Page 50, Clause10.4.1.9	Solution shall use Agent based approach for detection of unauthorised access via network activities analysis from the endpoints	Point no 4 states " The solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution" In line with this approach, 802.1x mechanism ensures that only authenticated users get network access.This access grants them necessary authorisation. An agent installed on the machine only checks for the health status and reports its back to the NAC server. The agent will come into picture only after authentication and authorisation is done. Hence we request you to consider deletion of this clause as it contradicts with the point no 4 stated above.	Refer to Corrigendum
34	Page 51, Clause10.4.1.14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	The functionality specified is that of a security device like NGFW, anti malware solution etc. The NAC can integrate with the security solution so that it receives notitfication of such alerts and takes appropriate action of blocking network access for those endpoints/ devices. NAC solution can only act as a gatekeeper and permit/deny access to the network based on certain policies/events.	No Change
35	Page 52, Clause10.4.1.36	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of:		No Change
36	Page 52, Clause10.4.1.36	a. Ability to run custom scripts and policies		
37	Page 52, Clause10.4.1.36	b. Hardware/Asset Management information	Please help to understand what is meant by asset management information. The NAC solution is not an asset mgmt solution. It can provide with the count of connected devices and their broad categories. We request you consider deletion of this clause.	
38	Page 52, Clause10.4.1.36	c. Event driven properties for compliance checks		
39	Page 52, Clause10.4.1.41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security group tagging is proprietery to an OEM. This also creates a dependency on the underlying network infrastructure. Since this contradicts the point 34 which mentions vendor agnostic switch infra, we request you to remove this clause.	Refer to Corrigendum
40	Page 52, Clause10.4.1.45	The proposed NAC solution should integrate with Firewalls (e.g. Checkpoint, Fortinet, Sonicwall)	The firewalls should be NGFW / user aware firewalls and they should support API integration with the NAC solution.	No Change

41	Page 52, Clause10.4.1.47	The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Please provide clarification as to what is Microsoft Factory server? Is it intended that the NAC solution should integrate with Azure AD environment? Please provide clarity about Factory Server.	Refer to Corrigendum
42	Page 52, Clause10.4.1.50	Should able to integrate with major leading vendor vulnerability assessment tools & ATD solution, so that Solution should respond rapidly to compromised devices on network to prevent threat propagation & data breaches and quarantine infected endpoints	These vulnerability assessment tools should be capable of API based integration.	No Change
43	Page 56, Clause10.4.1.64	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin	The NAC solutions have a fixed number of fields. The dashboard can be customised by choosing from the available fields only. No new fields can be added to the dashboard. The management console is centralised.	No Change
44	Page 56, Clause10.4.1.69	Automatic endpoint device provisioning/ installation with approval required option for on boarding	We understand this refers to Bring Your Own device. Please help to understand the count of such devices so as to size the solution accordingly.	The solution should be capable of provisioning. The actual device counts will be shared with selected bidder
S.N.	**Page Number**	**Clarification point as stated in the tender document**	**Comment/ Suggestion/ Deviation**	**NABARD Comments**
1	Page 12. Clause-4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Kindly modify this point as follows to allow greater participation - NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform or VMWare ESXI or Microsoft Hyper-V or KVM or as a physical appliance	Refer to Corrigendum
2	Page 51, Clause 14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Features like malware behaviours, malware type, severity, source and destination of attack which is more of NBAD or AV functionalities. NAC ensures that the requred services like AV/FW/AntiMalware, etc. are up and running to ensure endpoint is not comprimised. Additionally, NAC can take required action (block, quarantine or notify) by receiving an alert from SIEM solution. Please rewrite the clause as - **Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, User, Endpoint, etc.** Pls delete - network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	No Change
3	Page 52 , Clause 36-a	a. Ability to run custom scripts and policies	Running custom scripts on endpoints results in undesired end result and can be issue for IT team espacially at remote branches with limited or no local IT support. Please modify as - **Ability to run custom script or policies**	No Change
4	Page 53, Clause 40	The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunnelling (FAST), and EAP-Transport Layer Security (TLS).	EAP FAST is obselete protocol with security vulnerabilities. Please modify as - **The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), and EAP-Transport Layer Security (TLS).**	Refer to Corrigendum

5	Page 53, Clause 41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security Group Access (SGA) tagging is a vendor specific feature hence request you to remove this and change this point to - **Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments and URL redirect**	Refer to Corrigendum	
6	Page 54, Clause 49	The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto-Remediation.	Recommended option is to use Domain GPO policy as it provides better management and the patches can be installed even before the user login to windows. Auto-remediation through NAC may not be the right approach specifically when the patches/updates are missing in bulk. In such scenarios, it may take significant time to complete the installation of all missing patches which could impact the users activity. Some patch installation requires a reboot of windows machine, if the documents on which user is working are not saved, user will lose his data due to machine reboot performed by auto-remediation. Kindly modify this point as thsi will enabel added flexibility to NABARD IT **The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation.**	Refer to Corrigendum	
7	Page 56, Clause 71	Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	Since NAC act as a Radius server, it can directly authenticate the Guest and other users either with locally created accounts or with integration through external directory servers like AD, LDAP, etc. and hence, NAC doesn't require to act as an IDP. Our NAC can act as a Service Provider for SAML 2.0 authentication to allow user authentication with existing third party SAML database server (IDP). Kindly modify this pint as; **Solution must support Security Assertion Markup Language (SAML) 2.0 authentication.**	Refer to Corrigendum	
	Page 48, Annexure 3.2	Financials The Bidder should have a minimum annual turnover of Rs.30.00 crore and should also be in operating profit during the last three financial years, viz., 2017-18, 2018-19 & 2019-20 The Net worth of the Bidder Company should be positive as on 31st mach2020	As per MSME, NSIC and DPIIT norms, MSME/Startup is exempted from any prior experience. Attached necessary document for the same. OR Moditfy the clasue as The bidder should have Average annual turnover of Rs 30 CR for the last 3 financial years	No Change	
	Page 48, Annexure 3.3	Experience The Bidder should have supplied and implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI sector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the Bidder should be submitted.	As per MSME, NSIC and DPIIT norms, MSME/Startup is exempted from any prior experience. Attached necessary document for the same. OR Modify the clause as The bidder/ OEM must have implemented NAC solution in atleast 2 institutions in india of which one should be in BFSI sector during the last 5 years. OR The bidder must have implemented solution in atleast 2 institutions in India of which one should be in BFSI during last 5 years	No Change	

Sno	Page No	Section No	Clarification point as stated in tender document	Comment/Suggestion/Deviation	NABARD Comments
1	48	10.3 ELIGIBILITY	The Bidder should have supplied and implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI sector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the Bidder should be submitted.	The Bidder should have supplied and implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI /GOVT/PULIC 7 FINANCIAL INSTITUTEsector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the Bidder should be submitted.	No Change

2	25	7.10.1- Bidders past Experience	The bidder and OEM must have implemented NAC Solution in at least 3 institutions in India of which one should be in BFSI sector during last three years. 15* Marks for submitted project will be allotted as below: a. Project with less than 10,000 endpoints 2 (per project) -	The bidder and OEM must have implemented NAC Solution in at least 3 institutions in India of which one should be in BFSI /GOVT/PULIC 7 FINANCIAL INSTITUTEsector during last three years. 15* Marks for submitted project will be allotted as below: a. Project with less than 1500 endpoints 2 (per project)	No Change
1	11	4.2.2 General Requirements	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Aruba Clearpass supports VMWare Vsphere, Microsoft HyperV,KVM on CentOS & Ubuntu. We request you to change the clause to include these Hypervisors.	Refer to Corrigendum
2	50	10.4.1.1	The offered solution should provide comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services for a total of 10,000 network and endpoint devices. (+2000 additional licenses)	Does this 10000 include network devices like routers / switches/wireless controllers etc. If yes what is the total count of such devices?	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder.
3		10.4.1.2	The solution should support health-check / integration of minimum 4000 Desktops.	The total licenses required on day 1 is 10000. This includes 4000 desktops. Will there be any laptops that will also connect and need health check?	Yes
4		10.4.1.3	The solution should support health-check / integration of minimum 1000 Guest Users.	We request you to provide clarity on the authentication mechanism for Guests. Also is health check necessary for Guests devices?	Yes
5		10.4.1.5	Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access using SPAN or mirror traffic.	As per previous clause 10.4.1.4 , the solution should be a pre admission control solution.Aruba solution is a zero trust solution where we authenticate the user and then grant network access. This is achieved through 802.1x mechanism. we request you to amend the cluase as " Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access"	Refer to Corrigendum
6		10.4.1.9	Solution shall use Agent based approach for detection of unauthorised access via network activities analysis from the endpoints	Point no 4 states " The solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution" In line with this approach, 802.1x mechanism ensures that only authenticated users get network access.This access grants them necessary authorisation. An agent installed on the machine only checks for the health status and reports its back to the NAC server. The agent will come into picture only after authentication and authorisation is done. Hence we request you to consider deletion of this clause as it contradicts with the point no 4 stated above.	Refer to Corrigendum

7	51	10.4.1.14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	The functionality specified is that of a security device like NGFW, anti malware solution etc. The NAC can integrate with the security solution so that it receives notitfication of such alerts and takes appropriate action of blocking network access for those endpoints/ devices. NAC solution can only act as a gatekeeper and permit/deny access to the network based on certain policies/events.	No Change
8	52	10.4.1.36	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of:		No Change
			a. Ability to run custom scripts and policies		
			b. Hardware/Asset Management information	Please help to understand what is meant by asset management information. The NAC solution is not an asset mgmt solution. It can provide with the count of connected devices and their broad categories. We request you consider deletion of this clause.	
			c. Event driven properties for compliance checks		
10		10.4.1.41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security group tagging is proprietery to an OEM. This also creates a dependency on the underlying network infrastructure. Since this contradicts the point 34 which mentions vendor agnostic switch infra, we request you to remove this clause.	Refer to Corrigendum
11		10.4.1.45	The proposed NAC solution should integrate with Firewalls (e.g. Checkpoint, Fortinet, Sonicwall)	The firewalls should be NGFW / user aware firewalls and they should support API integration with the NAC solution.	No Change
12		10.4.1.47	The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Please provide clarification as to what is Microsoft Factory server? Is it intended that the NAC solution should integrate with Azure AD environment? Please provide clarity about Factory Server.	Refer to Corrigendum
13		10.4.1.50	Should able to integrate with major leading vendor vulnerability assessment tools & ATD solution, so that Solution should respond rapidly to compromised devices on network to prevent threat propagation & data breaches and quarantine infected endpoints	These vulnerability assessment tools should be capable of API based integration.	No Change
14	56	10.4.1.64	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin	The NAC solutions have a fixed number of fields. The dashboard can be customised by choosing from the available fields only. No new fields can be added to the dashboard. The management console is centralised.	No Change
15	56	10.4.1.69	Automatic endpoint device provisioning/ installation with approval required option for on boarding	We understand this refers to Bring Your Own device. Please help to understand the count of such devices so as to size the solution accordingly.	The solution should be capable of provisioning. The actual device counts will be shared with selected bidder
Reference	**Page No**	**Clause No**	**Existing Clause**	**Query / Proposed Change**	**NABARD Remarks**
8 Special T&C	29	8.1.2	The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the bidder at more favorable terms in case such terms are offered in the industry at the time of extension of contract	Request to Clause to be deleted	No change

8 Special T&C	29	8.4	Payment Schedule	8.4.1a)~~50%~~ 80% of Total Cost of Solution (indicated in the final commercial bid) after successful configuration and implementation of the solution at the Data Center of NABARD and DR Site, covering all HO end-point devices b)~~40%~~ 10% Total Cost of Solution (indicated in the final commercial bid) after the configuration and implementation of the solution for all end-point devices at all RO/TE Offices. c) Final 10% of Total Cost of Solution (indicated in the final commercial bid) will be paid after 3 months from the date of acceptance of the solution by NABARD. or against 10% PBG Submission. 8.4.7)Deduction of Income Tax, ~~Goods and Services Tax~~ and other applicable statutory duties would be as per the extant laws.	No change
8 Special T&C	31	8.6.2	In case of order cancellation, any payments made by the Bank to the vendor (for period for which services are not availed) would necessarily have to be returned to the Bank with interest @ 15% per annum. Further, the vendor would also be required to compensate the Bank for any direct loss incurred by the Bank due to the cancellation of the contract and any additional expenditure to be incurred by the Bank to appoint any other SP. This is after repaying the original amount paid.	Clause to be modified as under;(Risk Purchase) In the event Bank terminates the Contract in whole or in part, Bank may upon provision of an opportunity of being heard and cure the breach wthin 30 days cure period, procure, upon such terms and in such manner, as it deems appropriate, systems or services similar to those undelivered and the vendor shall be liable to Bank for ~~differential cost~~ maximum upto 5% of the differential costs for ~~any excess costs for~~ such similar systems or services which are undelivered. However, the vendor shall continue the performance of the contract to the extent not terminated. also the bank shall not invoke this clause for the services that are already performed and bank has paid or in the process of making payment for the same.	No change
8 Special T&C	31	8.7.1	Termination for default;	30 days cure prior to be provided to the bidder in rder to cure the breach.	No change
8 Special T&C	31	8.7.2	In the event Bank terminates the Contract in whole or in part, Bank may procure, upon such terms and in such manner, as it deems appropriate, systems or services similar to those undelivered and the vendor shall be liable to Bank for any excess costs for such similar systems or services. However, the vendor shall continue the performance of the contract to the extent not terminated.	Clause to be modified as under;(Risk Purchase) In the event Bank terminates the Contract in whole or in part, Bank may upon provision of an opportunity of being heard and cure the breach wthin 30 days cure perod, procure, upon such terms and in such manner, as it deems appropriate, systems or services similar to those undelivered and the vendor shall be liable to Bank for differential cost maximum upto 5% of ~~any excess costs for~~ such similar systems or services which are undelivered. However, the vendor shall continue the performance of the contract to the extent not terminated. also the bank shall not invoke this clause for the services that are already performed and bank has paid or in the process of making payment for the same.	No change

8 Special T&C	35	9.8.3	Performance Bank Guarantee may be invoked in case of violation of any of the terms and conditions of this document or in case of deficiency / delay in implementation/services provided by the successful bidder.	Clause t be modified as under; Performance Bank Guarantee may be invoked post mutual discussion and agreement between the parties in case of violation of any of the terms and conditions of this document or in case of deficiency / delay in implementation/services provided by the successful bidder and the bidder does not remedy such defaut or breach within 30 days of notice from the bank	No Change
8 General T&C	35	9.9	The Bank shall be at liberty to set off/adjust the proceeds of the performance guarantee towards the loss, if any, sustained due to the supplier's failure to complete its obligations under the contract. This is without prejudice to the Bank's right to proceed against the Supplier in the event of the security being not enough to fully cover the loss/damage.	The Bank shall be at liberty to set off/adjust the proceeds of the performance guarantee towards the actual, direct and proven loss, if any, sustained due to the supplier's failure to complete its obligations under the contract. This is without prejudice to the Bank's right to proceed against the Supplier in the event of the security being not enough to fully cover the actual, direct and proven loss/damage.	No change
8 General T&C	38	9.23	Limitation of Liability; Vendor's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for 1. IP Infringement indemnity 2. Bodily injury (including Death) and damage to real property and tangible property caused by vendor's gross negligence. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase orders placed by bank on the vendor that gave rise to claim, under this tender. Vendor shall not be liable for any indirect, consequential, incidental or special damages under the agreement/ purchase order.	Clause to be modified as under; Vendor's aggregate liability under the contract shall be limited to a maximum of the contract value. ~~This limit shall not apply to third party claims for~~ ~~1. IP Infringement indemnity~~ ~~2. Bodily injury (including Death) and damage to real property and tangible property caused by vendor's gross negligence. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase orders placed by bank on the vendor that gave rise to claim, under this tender~~. Vendor shall not be liable for any indirect, consequential, incidental or special damages under the agreement/ purchase order.	No change

8 General T&C	39	9.28	Indemnity; 9.28.1 The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidders obligation under these general conditions or for which the bidder has assumed responsibilities under the purchase contract including those imposed under any contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the bidder or bidders in connection with the performance of any system covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the purchase contract and to protect the Bank during the tenure of purchase order. 9.28.2 Where any patent, trade mark, registered design, copyrights and/ or intellectual property rights vest in a third party, the bidder shall be liablefor settling with such third party and paying any license fee, royalty and/ or compensation thereon. 9.28.3 In the event of any third party raising claim or bringing action against the Bank including but not limited to action for injunction in connection with any rights affecting the machine supplied by the bidder covered under the purchase contract or the use thereof, the bidder agrees and undertakes to defend and / or to assist the Bank in defending at the bidders cost against such third party's claim and / or actions and against any law suits of any kind	Indemnity (Clause to be modified as under); 9.28.1 The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from ~~all~~ actual, direct and proven liabilities, claims, costs, expenses, taxes and assessments including penalties, punitive damages, resonable attorney's fees and court costs which are or may be required to be paid by reasons of gross negligence and or wilful miconduct of the bidder ~~any breach of the bidders obligation~~ under these general conditions or ~~for which the bidder has assumed responsibilities under the purchase contract including those imposed under any contract~~, or breach of any local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the bidder or bidders in connection with the performance of any system covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the purchase contract and to protect the Bank during the tenure of purchase order. 9.28.2 Where any patent, trade mark, registered design, copyrights and/ or intellectual property rights vest in a third party, the bidder shall be liablefor settling with such third party and paying any license fee, royalty and/ or compensation thereon. 9.28.3 In the event of any third party raising claim or	No change
8 General T&C	40	9.29	Force Majeure	Please add below clause ; Neither party shall be liable for any penalty/damages for delay in performance or non performance of its obligations under this RFP/Agreement due to the event of force Majeure events.	No change
8 General T&C	40	9.30.3	The Bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator or the umpire, as the case may be, is obtained.	Clause to be modifie as under; The Bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator or the umpire, as the case may be, is obtained. likewise, the bank shall be liable to pay to the bidder for the services rendered	No change
SLA	90	2.11	Penalties	Line to be added:The maximum penalties under all clauses would be capped at 10% of the Purchase Order value. c)The purchaser may without prejudice to its right to effect recovery by any other method, deduct the amount of penalty from any money belonging to the bidder it its hands ~~(which includes the purchaser's right to claim such amount against bidder's Bank Guarantee)~~ or which may become due to the Bidder under this contract. This clause will not apply in cases where such amount has already been claimed against Bidder's bank guarantee.	No change

SLA	94	10	Limitation of Liability on SLA breaches; Vendor liability to meet the SLAs is limited to 20% cost of agreement during the year of warranty period and later the total AMC cost of duration of the AMC period in which the liability event occurred. Vendor will in no event be liable to NABARD for consequential, incidental, special or other indirect damages such as loss of profits herein whether by contract or tort, even if Vendor has knowledge of the likelihood of such damages.	Limitation of Liability on SLA breaches; Clause to be modified as under Vendor liability to meet the SLAs is limited to 10 ~~20~~% cost of agreement during the year of warranty period and later the total AMC cost of the perticular year ~~duration~~ of the AMC period in which the liability event perticularly occurred. Vendor will in no event be liable to NABARD for consequential, incidental, special or other indirect damages such as loss of profits herein whether by contract or tort, even if Vendor has knowledge of the likelihood of such damages. However, this Liability on SLA Breaches shall be subject to overall cap on limitation of liability mentioned in clause 9.23 under GCC.	No change
SLA	96	15	Indemnity; The Vendor shall, at his own expense, defend and indemnify Bank against any third party claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its (Vendors') employees or agents or by any other third party resulting from or by any action, omission, or operation conducted by or on behalf of the Vendor and against any and all claims by employees, workmen, contractors, sub-contractors, Vendors, agent(s), employed/ engaged otherwise working for the Vendor, in respect of any and all claims under the Labour Laws including wages, salaries, remuneration, compensation or like. The Vendor shall indemnify, protect and save Bank and hold Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings. (Including reasonable attorney fees), relating to or resulting directly or indirectly from: i. an act or omission of the Vendor, its employees or its agents in the performance of the services provided by this agreement, ii. breach of any of the terms of this Tender or breach of any representation or warranty by the Vendor, iii. Use of the deliverables and or services provided by the Vendor. iv. Infringement of any patent, trademarks, copyrights etc., or such other statutory infringements in respect of all components provided to fulfil the scope of this project. The Vendor shall further indemnify Bank against any loss or damage to Bank's premises or property, Bank's data, loss of life, etc., due to the acts of the Vendor's employees or representatives.	Clause to be modified as under-Indemnity; The Vendor shall, at his own expense, defend and indemnify Bank against any third party claims in respect of any actual, direct and proven damages or compensation payable in consequences of any accident or injury sustained or suffered by its (Vendors') employees or agents or by any other third party resulting from or by any gossly negligent action, wilful omission, or wrongful operation conducted by or on behalf of the Vendor and against ~~any and all~~ actual, direct and proven claims by employees, workmen, contractors, sub- contractors, Vendors, agent(s), employed/ engaged otherwise working for the Vendor, in respect of ~~any and all~~ actual, direct and proven claims under the Labour Laws including wages, salaries, remuneration, compensation or like. The Vendor shall indemnify, protect and save Bank and hold Bank harmless from and against all actual, direct and proven claims, losses, costs, damages, expenses, action suits and other proceedings. (Including reasonable attorney fees), relating to or resulting directly ~~or indirectly~~ from: i. an grossly negligent act or wilful omission of the Vendor, its employees or its agents in the performance of the services provided by this agreement, ii. ~~breach of any of the terms of this Tender or~~ breach of any representation or warranty by the Vendor, iii. Use of the deliverables and or services provided by	No change

			clause to be added as under	Below clause to be added : In the event of delay in installation or commissioning of equipment supplied by the Service Provider, or delay in submission of documents required under the RFP / Agreement / PO, or delay in issuance of the acceptance certificates by the Client, due to reasons beyond the reasonable control of the Service Provider, including but not limited to site not being ready, or force majeure situations, government orders and notifications, government ordered lockdown, epidemics and pandemics etc., the Client shall make immediate payment and not withhold payment of fees for the Products supplied and / or services already rendered, on this account. In such cases the Service Provider shall raise the invoice to the extent of the value of goods delivered and/or quantum of work performed and the Client shall make payment thereof. Further, it shall be the obligation of the Service Provider to perform all the unperformed / partially performed work and submit all the necessary documents in terms of the RFP / Agreement / PO as soon as practicably possible upon normalization of the situation	Not Accepted
			clause to be added as under	termination right for the bidder to be added as under; In the event of default or material breach by HPCL, and HPCL does not cure the breach within 30 days from the ate of receipt notice of such breach from the Vendor/Bidder, the Vendor/Bidder shall have right to terminate the contract with immidiate effect.	
Experienc e	48	4. Experience	The Bidder should have supplied and implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI sector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the Bidder should be submitted.	The Bidder / OEM should have supplied and implemented the NAC solution in at least in 3 institutions in India of which one should be in BFSI sector, during last three years (i.e. Since April 2017). References of top three project (in terms of size of the solution) of the Bidder / OEM should be submitted.	No change
SLA	88	2.7.3 SLA Table	<99.9% to >=98.00%, Penalty 2% <98.00% to >=96.00% Penalty 5% < 96.00% Penalty 10%	Please change it to <99.9% to >=98.00%, Penalty 1% <98.00% to >=96.00% Penalty 3% < 96.00% Penalty 5%	No Change
	50	10.4.1.1	The offered solution should provide comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services for a total of 10,000 network and endpoint devices. (+2000 additional licenses)	Does this 10000 include network devices like routers / switches/wireless controllers etc. If yes what is the total count of such devices?	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder.
		10.4.1.2	The solution should support health-check / integration of minimum 4000 Desktops.	The total licenses required on day 1 is 10000. This includes 4000 desktops. Will there be any laptops that will also connect and need health check?	Yes

		10.4.1.3	The solution should support health-check / integration of minimum 1000 Guest Users.	We request you to provide clarity on the authentication mechanism for Guests. Also is health check necessary for Guests devices?	LDAP protocol. And yes, health check up necessary for guests.
		10.4.1.5	Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access using SPAN or mirror traffic.	As per previous clause 10.4.1.4 , the solution should be a pre admission control solution.Aruba solution is a zero trust solution where we authenticate the user and then grant network access. This is achieved through 802.1x mechanism. we request you to amend the cluase as " **Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access"**	Refer to Corrigendum
		10.4.1.9	Solution shall use Agent based approach for detection of unauthorised access via network activities analysis from the endpoints	Point no 4 states " The solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution" In line with this approach, 802.1x mechanism ensures that only authenticated users get network access.This access grants them necessary authorisation. An agent installed on the machine only checks for the health status and reports its back to the NAC server. The agent will come into picture only after authentication and authorisation is done. Hence we request you to consider deletion of this clause as it contradicts with the point no 4 stated above.	Refer to Corrigendum
	51	10.4.1.14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	The functionality specified is that of a security device like NGFW, anti malware solution etc. The NAC can integrate with the security solution so that it receives notitfication of such alerts and takes appropriate action of blocking network access for those endpoints/ devices. NAC solution can only act as a gatekeeper and permit/deny access to the network based on certain policies/events.	No Change
	52	10.4.1.36	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of:		No change
			a. Ability to run custom scripts and policies		
			b. Hardware/Asset Management information	Please help to understand what is meant by asset management information. The NAC solution is not an asset mgmt solution. It can provide with the count of connected devices and their broad categories. We request you consider deletion of this clause.	
			c. Event driven properties for compliance checks		
		10.4.1.41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security group tagging is proprietery to an OEM. This also creates a dependency on the underlying network infrastructure. Since this contradicts the point 34 which mentions vendor agnostic switch infra, we request you to remove this clause.	Refer to Corrigendum
		10.4.1.45	The proposed NAC solution should integrate with Firewalls (e.g. Checkpoint, Fortinet, Sonicwall)	The firewalls should be NGFW / user aware firewalls and they should support API integration with the NAC solution.	No change

		10.4.1.47	The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Please provide clarification as to what is Microsoft Factory server? Is it intended that the NAC solution should integrate with Azure AD environment? Please provide clarity about Factory Server.	Refer to Corrigendum
		10.4.1.50	Should able to integrate with major leading vendor vulnerability assessment tools & ATD solution, so that Solution should respond rapidly to compromised devices on network to prevent threat propagation & data breaches and quarantine infected endpoints	These vulnerability assessment tools should be capable of API based integration.	No change
	56	10.4.1.64	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin	The NAC solutions have a fixed number of fields. The dashboard can be customised by choosing from the available fields only. No new fields can be added to the dashboard. The management console is centralised.	No change
	56	10.4.1.69	Automatic endpoint device provisioning/ installation with approval required option for on boarding	We understand this refers to Bring Your Own device. Please help to understand the count of such devices so as to size the solution accordingly.	The solution should be capable of provisioning. The actual device counts will be shared with selected bidder
	12	Clause- 4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Kindly modify this point as follows to allow greater participation - NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform or VMWare ESXI or Microsoft Hyper-V or KVM or as a physical appliance	Refer to Corrigendum
	51	Clause 14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Features like malware behaviours, malware type, severity, source and destination of attack which is more of NBAD or AV functionalities. NAC ensures that the requred services like AV/FW/AntiMalware, etc. are up and running to ensure endpoint is not comprimised. Additionally, NAC can take required action (block, quarantine or notify) by receiving an alert from SIEM solution. Please rewrite the clause as - **Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, User, Endpoint, etc.** Pls delete - network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Refer to Corrigendum
	52	Clause 36-a	a. Ability to run custom scripts and policies	Running custom scripts on endpoints results in undesired end result and can be issue for IT team espacially at remote branches with limited or no local IT support. Please modify as - **Ability to run custom script or policies**	No change
	53	Page 53, Clause 40	The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunnelling (FAST), and EAP-Transport Layer Security (TLS).	EAP FAST is obselete protocol with security vulnerabilities. Please modify as - **The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), and EAP-Transport Layer Security (TLS).**	No change

	53	Page 53, Clause 41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security Group Access (SGA) tagging is a vendor specific feature hence request you to remove this and change this point to - **Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments and URL redirect**	Refer to Corrigendum
	54	Page 54, Clause 49	The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto-Remediation.	Recommended option is to use Domain GPO policy as it provides better management and the patches can be installed even before the user login to windows. Auto-remediation through NAC may not be the right approach specifically when the patches/updates are missing in bulk. In such scenarios, it may take significant time to complete the installation of all missing patches which could impact the users activity. Some patch installation requires a reboot of windows machine, if the documents on which user is working are not saved, user will lose his data due to machine reboot performed by auto-remediation. Kindly modify this point as thsi will enabel added flexibility to NABARD IT **The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation.**	Refer to Corrigendum
	56	Page 56, Clause 71	Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	Since NAC act as a Radius server, it can directly authenticate the Guest and other users either with locally created accounts or with integration through external directory servers like AD, LDAP, etc. and hence, NAC doesn't require to act as an IDP. Our NAC can act as a Service Provider for SAML 2.0 authentication to allow user authentication with existing third party SAML database server (IDP). Kindly modify this pint as; **Solution must support Security Assertion Markup Language (SAML) 2.0 authentication.**	Refer to Corrigendum

S.N.	Page Number	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	NABARD Comments
1	Page 51, Clause 14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Functionality like malware behaviours, malware type, severity, source and destination of attack which is more of NBAD or AV functionality. NAC ensures that requred services like AV/FW/AntiMalware etc. are up and running to ensure endpoint is not comprimised. Additionally, NAC can take required action (block, quarantine or notify) by receiving an alert from SIEM solution. Please modify clause as - **Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, User, Endpoint, etc.** Pls delete - network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	No Change

2	Page 53, Clause 41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security Group Access (SGA) tagging is a vendor specific feature. Request you to remove this and change this point to - **Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments and URL redirect** and ~~Security Group Access (SGA) tagging.~~	Refer to Corrigendum
3	Page 54, Clause 49	The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto-Remediation.	Windows Patch update can be triggered in multiple ways i.e., through Domain Group Policy, through Registry modification, by prompting the user to start the required installation or through NAC agent. The recommended option is to use Domain GPO policy as it provides better management and the patches can be installed even before the user login to windows. Auto-remediation through NAC may not be the right approach specifically when the patches/updates are missing in bulk. In such scenarios, it may take significant time to complete the installation of all missing patches which could impact the users activity. Some patch installation requires a reboot of windows machine, if the documents on which user is working are not saved, user will lose his data due to machine reboot performed by auto-remediation. Hence the better option is to either use Domain Group Policy or to give flexibility to the user to perform patch update as per his/her convenience. For More flexibility kindly modify this point as follows - **The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation.**	Refer to Corrigendum
4	Page 56, Clause 71	Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	As a Enterprise NAC we have inbuilt Radius server, hence we able to directly authenticate the Guest and other users either with locally created accounts or with integration through external directory servers like AD, LDAP, etc. and hence, NAC doesn't require to act as an IDP. Pulse Secure NAC can act as a Service Provider for SAML 2.0 authentication to allow user authentication with existing third party SAML database server (IDP). Kindly modify this point as; **Solution must support Security Assertion Markup Language (SAML) 2.0 authentication.**	Refer to Corrigendum

Sno	Page No	Section No	Clarification point as stated in tender document	Comment/Suggestion/Deviation	NABARD Comments
1	11	4.2.2 General Requirements	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Aruba Clearpass supports VMWare Vsphere, Microsoft HyperV,KVM on CentOS & Ubuntu. We request you to change the clause to include these Hypervisors.	Not Accepted
2	50	10.4.1.1	The offered solution should provide comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services for a total of 10,000 network and endpoint devices. (+2000 additional licenses)	Does this 10000 include network devices like routers / switches/wireless controllers etc. If yes what is the total count of such devices?	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder.
3		10.4.1.2	The solution should support health-check / integration of minimum 4000 Desktops.	The total licenses required on day 1 is 10000. This includes 4000 desktops. Will there be any laptops that will also connect and need health check?	Yes

4		10.4.1.3	The solution should support health-check / integration of minimum 1000 Guest Users.	We request you to provide clarity on the authentication mechanism for Guests. Also is health check necessary for Guests devices?	Yes
5		10.4.1.5	Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access using SPAN or mirror traffic.	As per previous clause 10.4.1.4 , the solution should be a pre admission control solution.Aruba solution is a zero trust solution where we authenticate the user and then grant network access. This is achieved through 802.1x mechanism. we request you to amend the cluase as " **Solution shall monitor, detect, alert, report and provide remediation, recommendation for any unauthorized access"**	Refer to Corrigendum
6		10.4.1.9	Solution shall use Agent based approach for detection of unauthorised access via network activities analysis from the endpoints	Point no 4 states " The solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution" In line with this approach, 802.1x mechanism ensures that only authenticated users get network access.This access grants them necessary authorisation. An agent installed on the machine only checks for the health status and reports its back to the NAC server. The agent will come into picture only after authentication and authorisation is done. Hence we request you to consider deletion of this clause as it contradicts with the point no 4 stated above.	Refer to Corrigendum
7	51	10.4.1.14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	The functionality specified is that of a security device like NGFW, anti malware solution etc. The NAC can integrate with the security solution so that it receives notitfication of such alerts and takes appropriate action of blocking network access for those endpoints/ devices. NAC solution can only act as a gatekeeper and permit/deny access to the network based on certain policies/events.	No Change
8	52	10.4.1.36	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of:		No Change
			a. Ability to run custom scripts and policies		
			b. Hardware/Asset Management information	Please help to understand what is meant by asset management information. The NAC solution is not an asset mgmt solution. It can provide with the count of connected devices and their broad categories. We request you consider deletion of this clause.	
			c. Event driven properties for compliance checks		
10		10.4.1.41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security group tagging is proprietery to an OEM. This also creates a dependency on the underlying network infrastructure. Since this contradicts the point 34 which mentions vendor agnostic switch infra, we request you to remove this clause.	Refer to Corrigendum
11		10.4.1.45	The proposed NAC solution should integrate with Firewalls (e.g. Checkpoint, Fortinet, Sonicwall)	The firewalls should be NGFW / user aware firewalls and they should support API integration with the NAC solution.	No Change

12		10.4.1.47	The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Please provide clarification as to what is Microsoft Factory server? Is it intended that the NAC solution should integrate with Azure AD environment? Please provide clarity about Factory Server.	Refer to Corrigendum
13		10.4.1.50	Should able to integrate with major leading vendor vulnerability assessment tools & ATD solution, so that Solution should respond rapidly to compromised devices on network to prevent threat propagation & data breaches and quarantine infected endpoints	These vulnerability assessment tools should be capable of API based integration.	No Change
14	56	10.4.1.64	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin	The NAC solutions have a fixed number of fields. The dashboard can be customised by choosing from the available fields only. No new fields can be added to the dashboard. The management console is centralised.	No Change
15	56	10.4.1.69	Automatic endpoint device provisioning/ installation with approval required option for on boarding	We understand this refers to Bring Your Own device. Please help to understand the count of such devices so as to size the solution accordingly.	The solution should be capable of provisioning. The actual device counts will be shared with selected bidder
S.N.	Page Number	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	NABARD Comments	
1	Page 12. Clause- 4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Kindly modify this point as follows to allow greater participation - NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform or VMWare ESXI or Microsoft Hyper-V or KVM or as a physical appliance	Refer to Corrigendum	
2	Page 15, 4.13. Obsolescence	The vendor will ensure that the stipulated Support and maintenance facilities on the hardware / software will be available for a minimum period of 6 years. The proposed product should not be under “End of Sale” for the next six years or till the end of warranty/Support period , whichever is later and should not be under “ End of Support” for the next 3 years after the warranty period. The vendor will constantly update the Bank on new technologies that could prove cost effective.	Request NABARD to consider the " End of Support " period for the contact period and " End of sale " period for maximim 6 months/ 1 Year from the bid submission date.	No Change	
3	Page 15 4.10.1	Delivery of licenses and pilot implementation of the NAC solution component will be at DC-Mumbai & DR-Faridabad within 4 (four) weeks from the date of release of PO.	Request you to Change as " Delivery of licenses and pilot implementation of the NAC solution component will be at DC-Mumbai & DR-Faridabad within **8 (Eight)** weeks from the date of release of PO.	No Change	

4	Page 25 , 7.10 Bidders past Experience	7.10 Bidders past Experience The bidder and OEM must have implemented NAC Solution in at least 3 institutions in India of which one should be in BFSI sector during last three years. **Marks for submitted project will be allotted as below:** **a. Project with less than 10,000 endpoints--2 (per project)** **b. Project with more than 10,000 and less than 14,000 endpoints--3(per project)** **c. Project with more than 14,000 endpoints--5(per project)** Maximum Marks-15 marks	Request Bank to Consider the Bidder /OEM Experience for this overall technical Scoring	No Change
5	Page 30 (Special conditions)	8.6 Termination of Contract In case of order cancellation, any payments made by the Bank to the vendor (for period for which services are not availed) would necessarily have to be returned to the Bank with interest @ 15% per annum.	We propose the below change in RFP clause: In case of order cancellation, any payments made by the Bank to the vendor (for period for which services are not availed) would necessarily have to be returned to the Bank	No Change
6	Page 48 , 10.3 Annexure –III: Minimum Eligibility Criteria	**Financials** The Bidder should have a minimum annual turnover of Rs.30.00 crore and should also be in operating profit during the last three financial years, viz., 2017-18, 2018-19 & 2019-20 The Net worth of the Bidder Company should be positive as on 31 March 2020 **Documents to be submitted** Audit Balance Sheets of last three FY viz. 2017-18, 2018-19 & 2019-20.	Request NABARD to accept the Provisional Balance Sheet for FY 2019-20 since the Auditing yet to complete for this FY.	No Change
7	Page 51, Clause 14	Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	Request you to change as - **Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, User, Endpoint, etc.** Pls delete - network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack which is more of NBAD or AV functionalities	No Change
8	Page 52 , Clause 36-a	a. Ability to run custom scripts and policies	**Request you to change as - Ability to run custom script or policies**	No Change
9	Page 53, Clause 40	The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunnelling (FAST), and EAP-Transport Layer Security (TLS).	EAP FAST protocol has security vulnerabilities. Please modify as - **The solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), and EAP-Transport Layer Security (TLS).**	Refer to Corrigendum

10	Page 53, Clause 41	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	Security Group Access (SGA) tagging is a vendor specific feature hence request you to remove this and change this point to - **Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments and URL redirect**	Refer to Corrigendum	
11	Page 54, Clause 49	The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto-Remediation.	Request you to change as - **The proposed solution must able to integrate with Endpoint Patch management such as WSUS for Auto or Manual Remediation.**	Refer to Corrigendum	
12	Page 56, Clause 71	Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	Since NAC act as a Radius server, it can directly authenticate the Guest and other users either with locally created accounts or with integration through external directory servers like AD, LDAP, etc. and hence, NAC doesn't require to act as an IDP. Our NAC can act as a Service Provider for SAML 2.0 authentication to allow user authentication with existing third party SAML database server (IDP). Kindly modify this point as; **Solution must support Security Assertion Markup Language (SAML) 2.0 authentication.**	Refer to Corrigendum	
13	Page 74 (Non disclosure Agreement	Obligation of confidentiality contemplated under this Agreement shall continue to be binding and applicable without limit in point in time.	We propose the below change in RFP clause: Obligation of confidentiality contemplated under this Agreement shall continue to be binding till successful completion of the purpose	No Change	
14	Page 96	15. Indemnification "The Vendor shall, at his own expense, defend and indemnify Bank against any third party claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its (Vendors') employees or agents or by any other third party resulting from or by any action, omission, or operation conducted by or on behalf of the Vendor and against any and all claims by employees, workmen, contractors, sub- contractors, Vendors, agent(s), employed/ engaged otherwise working for the Vendor, in respect of any and all claims under the Labour Laws including wages, salaries, remuneration, compensation or like.	We propose the below clause: The Vendor shall, at his own expense, defend and indemnify Bank against any claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its (Vendors') employees or agents resulting from or by any action, omission, or operation conducted by or on behalf of the Vendor and against any and all claims by employees, workmen, contractors, sub- contractors, Vendors, agent(s), employed/ engaged otherwise working for the Vendor, in respect of any and all claims under the Labour Laws including wages, salaries, remuneration, compensation or like.	No Change	
15	Page 97	15. Indemnification The Vendor shall further indemnify Bank against any loss or damage to Bank's premises or property, Bank's data, loss of life, etc., due to the acts of the Vendor's employees or representatives.	We propose the below change in RFP clause: The Vendor shall further indemnify Bank against any loss or damage to Bank's premises or property, loss of life, etc., due to the acts of the Vendor's employees or representatives.	No Change	
Sr.No	**Pg. No**	**Section Number**	**Clarification point as stated in the tender document**	**Comment/ Suggestion/ Deviation**	**NABARD Comments**
1			Other Information	Please provide total Number of L2/L3 devices details , Are all device are managable?	Will be shared with Selected bidder

2	11	4.2.2	NAC Solution to be installed in HA at both DC and DR on the Acropolis Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform	Nutanix support multiple hyperviser (https://www.nutanix.com/info/hypervisor) , Request you to repharse as "NAC Solution to be installed in HA at both DC and DR on the Acropolis/KVM/VMware ESXi/Microsoft Hyper-V Hypervisor created Virtual Machine running RHEL (version N-1) as the Operating System on the Nutanix HCI Platform"	Refer to Corrigendum
3	11	4.2.12	The Bidder shall engage one Technical Account Manager from OEM for a period of 1 year and an Onsite Engineer for the entire contract period	Request you repharse as "The Bidder shall engage one Technical Account Manager for a period of 1 year and an Onsite Engineer for the entire contract period"	No Change
4	15	4.12.1	Power OnSelf Test (POST) will be conducted by Bidder at the site in presence of NABARD officials and /or nominated person. Installation report (IR) should be submitted after complete implementation of systems. NABARD will take over the system on successful completion of above acceptance test.	Point Need to be deleted as this is software based NAC solution deployement	No Change
5	32	8.10.1	Phase –I Delivery of Licenses and Pilot Implementation (On Nutanix –VM)	NABARD is looking for separate pilot setup? We have to propose additional license for Pilot setup? Please provide total license require for pilot setup.	Refer to Corrigendum
6	49		The OEM should possess ISO 27001 series certification	ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties (https://www.iso.org/isoiec-27001-information-security.html) It must be applicable to bidder and not OEM Request you to repharse as " The Bidder should possess ISO 27001 Series certification"	No Change
7	50	10.4.1	2.The solution should support health-check / integration of minimum 4000 Desktops.	As per RFP total license is 10000 , what are the other 6000 devices? Ideally The Solution should capable enough not only for Campus infrastructure but also with Data Center(Virtual or physical) , IOT (Printer/Scanner/IP Phone/IP Camera/ Smart PDU / Smart Rack etc)& cloud for security risk assessment & incident response. IoT (Printer/Scanner/IP Phone/IP camera/Netowrk Device) Risk Assessment : The solution should be able to identify all network devices such as routers, switches,IOT's devices using factory default or Weak/common credentials.Kindly repharse as "The solution should support health-check / integration of minimum 10000 devices."	Approx. 6000 Desktops, 2000 Laptops, 1000 Network Devices (Switches, Routers, Firewall, etc.), and 1000 Printers, Scanners and other endpoints. Actual count will be shared with the selected bidder. No change in clause

8	50	10.4.1	4.The solution should be able to control the user even before IP address is assigned. It should act as a preadmission solution	Ideal NAC approach recommends that pre-connect controls should be implemented only after an initial post-connect deployment to establish device visibility, develop security policies and assess their impacts on users. A gradual transition from post- to pre-connect control can help avoid unnecessary blockage of authorized users due to abrupt introduction of new security policy. Incremental deployment allows security and operations teams the necessary time to identify affected devices, measure operational impacts and adjust policies as necessary before full enforcement begins. Request you to re-pharse as "Solution must support both post-connect & pre-connect addmission controls, NAC control should be implemented only after an initial post-connect deployment to establish device visibility, develop security policies and assess their impacts on users."	No Change
9	50	10.4.1	6.Solution should have the capability of traffic log retention for a period of 1 year.	Traffice log retention for the period of 1 year is Log sever capability & not a NAC Solution Capability. Request you to remove this point or Repharse as "For logs retention for a period of 1 year , Solution should have the capability to forward logs to Syslog/SIEM solution. "	Refer to Corrigendum
10	50	10.4.1	9.Solution shall use Agent based approach for detection of unauthorized access via network activities analysis from the endpoints	The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.The Solution should capable enough not only for Campus infrastructure but also with Data Center(Virtual or physical) , IOT (Printer/Scanner/IP Camera/IP Phone etc) for security risk assessment & incident response	Refer to Corrigendum
11	50	10.4.1	14. Solution shall provide forensic evidence on any unauthorized access activity within the network as follows: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack	packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack are not NAC capability , Request you to delete this clause.	No Change

12	52	10.4.1	28.The proposed solution must support a managed switch environment having 802.1 x support.	As per RFP clause Page no 55 point no 59 "The solution should be capable of being bypassed in the event of any failure of the solution. This should be applicable in both managed and unmanaged switch environments." NABARD is having unmanaged switches where switch may not support 802.1x Kindly repharse "The solution should support both 802.1X and Non-802.1X Architecture." The support for Non-802.1X Architecture will allow early integration with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployments. NABARD can then take its own time to upgrade the infrastructure to support 802.1x at its own pace and doesn't make it a deterrent to the NAC deployment.	No Change
13	52	10.4.1	29.The solution must support agent-based deployment and provide complete posture analysis.	Large organization have 30-40% of the devices which will not support agent.It is not a good idea to Completely depend on agent. Request you to remove the point & Add below Points -Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , Printers , Scanners etc. -The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important for NABARD to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.	No Change

14	52	10.4.1	33.The solution should support MAC Address Bypass (used for devices which do not support MAC id) and utilize other available identity of the endpoint to apply the proper rules for access.	Large organization have 30-40% of the devices which will not support 802.1x.It is not a good idea to create a repository of MAC address to whitelist. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. also MAC address repository should be uptodate at any point in time to meet security aspect. Request you to remove the point & Add below Points -Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , Printers , Scanners etc. -The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important for NABARD to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible. -The Solution should capable enough not only for Campus infrastructure but also with Data Centre(Virtual or physical) , IOT & public cloud(Amazon/Azure) for security risk assessment & incident response -The solution should support both 802.1X and Non-802.1X Architecture in single deployment. The support for Non-802.1X Architecture will allow early integration with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployments (there is no option to deploy	No Change
15	52	10.4.1	35.The solution should have a provision to support non- NAC capable hosts (i.e., IP phones, IOT's etc.) based on Mac address or other parameter and it should support exception lists for non-NAC capable hosts.	NABARD may have have 3000-4000 of the devices which will not support 802.1x/Non-NAC capable host.It is not a good idea to create a repository of MAC address to whitelist. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. also MAC address repository should be uptodate at any point in time to meet security aspect. Request you to remove the point & Add below Points -Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera , Printers , Scanners etc. - IoT (Printer/Scanner/IP Phone/IP camera/Netowrk Device) Risk Assessment : The solution should be able to identify all network devices such as routers, switches,IOT's devices using factory default or Weak/common credentials	No Change
16	53	10.4.1	38.The solution should provide full Terminal Access Controller Access Control System (TACACS)+ capability including enable password, configuration present for different NAD types, TACACS+ proxy etc.	NABARD may already uses PIM or Network device authentication solution. TACACS+ is not a NAC funcationility. Request you to repharse as " The solution should provide full integration Terminal Access Controller Access Control System (TACACS)+ capability."	No Change

17	54	10.4.1	47.The proposed NAC solution should support, verify authentication and integrate with Microsoft Factory server.	Typo error it must be Microsoft Active directory server, Our under standing is correct? What type of authentication NABARD is looking for IP Priner / IP phone / IP camera / Smart PDU / Data Center Server etc , which must be not integrated with Microsoft Active Directory?	Refer to Corrigendum
18	54-55	10.4.1	52.Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal for a specific user for a selected period of time. The report should provide the following detail •Logged in Date and Time •Portal User (who registered the device) •MAC Address •Identity Group •Endpoint Policy •Endpoint Policy ID •NMAP Subnet Scan ID •Device Registration Status	Specific to single OEM . Request you to delete "https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_prof_pol.html"	Refer to Corrigendum
19	55	10.4.1	54.The solution should offer a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations. The solution should enable administrators to centrally configure and manage profile, posture, guest, authentication, and authorization services in a single web-based GUI console, simplifying administration by providing consistency in managing all these services.	Kindly repharse as "The solution should offer a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations. The solution should enable administrators to centrally configure and manage profile, posture, guest, authentication, and authorization services in a single web- based / GUI console, simplifying administration by providing consistency in managing all these services. "	No Change
20	56	10.4.1	66.Automatically configure and provision mobile devices such as MAC, iOS, Android, Chromebook etc. enabling them to securely connect to enterprise network.	Specific to single OEM . Request you to delete Refer Pae 1 (https://www.arubanetworks.com/assets/ds/DS_ClearPass_Onboard.pdf)	No Change
21	56	10.4.1	68. Capable to define the number of devices that can be on-boarded per user and validity period.	Specific to single OEM . Request you to delete Refer Pae 2 (https://www.arubanetworks.com/assets/ds/DS_ClearPass_Onboard.pdf)	No Change
22	56	10.4.1	69. Automatic endpoint device provisioning/ installation with approval required option for on boarding	Specific to single OEM . Request you to delete (https://www.arubanetworks.com/assets/ds/DS_ClearPass_Onboard.pdf)	The solution should be capable of provisioning. The actual device counts will be shared with selected bidder
23	56	10.4.1	71.Solution must support Security Assertion Markup Language (SAML) 2.0 identity provider which allows seamless single sign on (SSO) to the cloud or on premises applications along with AD integration	NABARD is already having Cloud based AD? What is the exact use case NABARD want to achieve via SSO & SAML?	Refer to Corrigendum
24	58	11	Cost of Technical Account Manager from OEM for a period of One Year after the project goes live (One Day per week Onsite and remaining days remote support)	Request you repharse as "Cost of Technical Account Manager from Bidder for a period of One Year after the project goes live (One Day per week Onsite and remaining days remote support) "	No Change
25			Point need to be added (Mandatory)	The solution should support all versions of Windows starting from Windows XP, all versions of OS X starting from OS X 10.8 and major Linux versions (atleast CentOS, Debian, Fedora, Red Hat Enterprise Linux, Open SUSE, SUSE Enterprise, Ubuntu) for complete posture assessment both agent based and agent-less.	Not Accepted

26			Point need to be added (Mandatory)	IoT (Printer/Scanner/IP Phone/IP camera/Netowrk Device) Risk Assessment : The solution should be able to identify all network devices such as routers, switches,IOT's devices using factory default or Weak/common credentials	Not Accepted
27			Point need to be added (Mandatory)	The solution should support both 802.1X and Non-802.1X Architecture. The support for Non-802.1X Architecture will allow early integration with existing network infrastructure without the need of any hardware and software upgrades required for 802.1X deployments.". The SBIFMPL can then take its own time to upgrade the infrastructure to support 802.1x at its own pace and doesn't make it a deterrent to the NAC deployment.	Not Accepted
28			Point need to be added	"The NAC solution should detect endpoint state changes (AV disabled, execution of an unauthorized application, etc) and perform auto-remediation e.g. it should detect and disable unauthorized dual-homed endpoints. It should be done on a continuous basis rather than waiting for the next authentication event to happen.". It is important today as the endpoints security posture can change at any split of a second in these times of highly sophisticated targeted attacks. Hence, it is critical to detect endpoint state changes and perform auto-remediation on a continuous basis rather than waiting for the next authentication event to happen.	Not Accepted
29			Point need to be added (Mandatory)	The NAC solution should support existing network infrastructure i.e Managed & unmanaged swiches to block or limit the non-complied or rough devices behind that.	Not Accepted
30			Point need to be added (Mandatory)	The NAC solution should support agentless , agent based & dissolvable agent mode to achieve all feature & functionality mentioned in the RFP. It is important to have all the option & help for faster deployment & flexibility to choose the option as require based on type of devices where agent option is not feasible.	Not Accepted
31			Point need to be added	The Solution should capable enough not only for Campus infrastructure but also with Data Center(Virtual or physical) , IOT & cloud for security risk assessment & incident response	Not Accepted
32			Point need to be added	The solution should provide complete inventory of all applications, running processes , Services and open ports on an endpoint.	Not Accepted

33			Point need to be added	The proposed solution should support automated remediation system including starting madetory process/Services, killing blacklisted process/Services, setting registry keys, starting antivirus, update anti-virus, starting windows updates and running custom scripts (must be available for Windows, Linux and MAC-OS) Help desk and self-service remediation allowing for load reduction through end user self- support and automatic remediation.	Not Accepted
34			Point need to be added	The proposed NAC solution should provide out-of-the-box IOC, Hash, Malicious files scanning to discover and mitigate threats from infected endpoints. The solution must support at least the following IOC types for IOC scanning: CnC Address (Command and Control URL) , Process (Process Name, Process Hash, Process Hash Type) , File Exists (File Name, File Path) , Mutex (Mutex Name) , Registry Key (Path, Value) , Service (Service name) etc	Not Accepted
35			Point need to be added	The solution should be able to provide detection for shared directories and non-admin shares.	Not Accepted
36			Point need to be added	The solution should be able to provide detection for shared directories - admin shares	Not Accepted