



**SUPPLEMENTAL/BID BULLETIN NO. 2
For LBP-ICTBAC- ITB-GS-20240906-01**

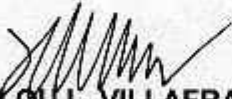
PROJECT: Supply, Delivery, Installation and Configuration of Unified Identity Protection Platform Solution w/ Three (3) Years Support Services

DATE: 28 October 2024

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

1. Response to prospective bidder/s queries/clarifications per attached Annex H.
2. Section VII. Technical Specifications (pages 42-43), Checklist of the Bidding Documents (pages 64-67) and Terms of Reference (Annexes D1-D7) have been revised. Copies of said revised portions of the Bidding Documents are herein attached.
3. The Bidder/s are reminded that the deadline of Bid Submission and Opening is on 06 November 2024 at 10:00 AM. **Late bids will not be accepted.**
4. The bidder/s is/are encouraged to use the Bid Securing Declaration as Bid Security.


SVP MARILOU L. VILAFRANCA
Chairperson, ICT-BAC

SUPPLEMENTAL/BID BULLETIN NO. 2
For LBP-ICTBAC- ITB-GS-20240906-01

PROJECT: Supply, Delivery, Installation and Configuration of Unified Identity Protection Platform Solution w/ Three (3) Years Support Services

DATE: 28 October 2024

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

1. Response to prospective bidder/s queries/clarifications per attached Annex H.
2. Section VII. Technical Specifications (pages 42-43), Checklist of the Bidding Documents (pages 64-67) and Terms of Reference (Annexes D1-D7) have been revised. Copies of said revised portions of the Bidding Documents are herein attached.
3. The Bidder/s are reminded that the deadline of Bid Submission and Opening is on 06 November 2024 at 10:00 AM. **Late bids will not be accepted.**
4. The bidder/s is/are encouraged to use the Bid Securing Declaration as Bid Security.



SVP MARILOU L. VILLAFRANCA
Chairperson, ICT-BAC

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

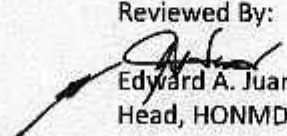
RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS DATE	October 25, 2024
PROJECT IDENTIFICATION NO.	ITB-GS-20240906-01
PROJECT NAME	Supply, Delivery, Installation and Configuration of Unified Identity Protection Platform Solution w/ Three (3) Years Support Services
PROPONENT UNIT/TECHNICAL WORKING GROUP	Head Office Network Management Department (HONMD)

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND /OR SUGGESTIONS	LANDBANK'S RESPONSES
103	The supplier must submit list with Certificate of Satisfactory Performance from at least two (2) installed base of same solution wherein one (1) is a Universal or Commercial Philippine Bank, with client name, contact person, address, telephone number and email address.	Can you relax the requirements for the installed base?	We have updated item 103: The supplier must submit list with Certificate of Satisfactory Performance from at least two (2) installed base of Identity Protection Cybersecurity Solution wherein one (1) is a Universal or Commercial Philippine Bank, with client name, contact person, address, telephone number and email address
	All items under Vendor Requirements	Clarification on the terms "vendor" and "supplier" are often used interchangeably, but they can have slightly different connotations depending on the context.	As for this project, the terms vendor and supplier both pertains to the entity that will supply, deliver, install and configure the solution.

Prepared by:


Bryan Armand C. Cristobal
SITS, HONMD

Reviewed By:


Edward A. Juan
Head, HONMD

Technical Specifications

Specifications	Statement of Compliance
<p>Supply, Delivery, Installation and Configuration of Unified Identity Protection Platform Solution with Three (3) Years Support Services</p> <ol style="list-style-type: none">1. Minimum technical specifications and other requirements per attached Revised Annexes D-1 to D-7.2. The documentary requirements enumerated in Revised Annexes D-6 to D-7 of the Terms of Reference shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements. <p>Non-submission of the above documents may result in the post-disqualification of the bidder.</p>	<p>Bidders must signify their compliance to the Technical Specifications/Terms of Reference by stating below either "Comply" or "Not Comply"</p> <p>Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.</p> <p>Please state here either "Comply" or "Not Comply"</p>

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position

Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Component (PDF File)

- **The Eligibility and Technical Component shall contain documents sequentially arranged as follows:**

- **Eligibility Documents – Class “A”**

Legal Eligibility Documents

1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);

Technical Eligibility Documents

2. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).
3. Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).
4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar to the contract to be bid within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

Financial Eligibility Documents

5. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

6. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.
- o **Eligibility Documents – Class "B"**
7. Duly signed valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.
 8. For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos, Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
 9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.
- o **Technical Documents**
10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
 11. Section VI – Schedule of Requirements with signature of bidder's authorized representative.
 12. Section VII – Revised Specifications with response on compliance and signature of bidder's authorized representative.
 13. Duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

Note: During the opening of the first bid envelopes (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary "pass/fail" criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.

- **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**
 14. **Revised Terms of Reference** duly signed in all pages by the authorized representative/s of the bidder.
 15. **Manufacturer's authorization** or any equivalent document confirming that the bidder is authorized to provide the product/brand being offered and consumables supplied by the manufacturer, including any warranty obligations and after sales support as may be required (sample form - Form No.9).
 16. **Securities and Exchange Commission (SEC) Registration** as proof that the bidder has at least ten (10) years of experience in the IT Industry.
 17. **Detailed Escalation Procedure and Support** including contact numbers and email addresses.
 18. **Certificate of Employment, Resume/Curriculum Vitae and List of Trainings and Seminars attended** (including Cyber Security related seminars) of at least three (3) local Information Technology engineers with at least three (3) years work experience in Cyber Security Solutions.
 19. **Certificate of Employment and Resume/Curriculum Vitae** of a dedicated Project Manager employed with the bidder with at least three (3) years work experience and handled at least one (1) Commercial or Universal bank and one (1) non-bank client.
 20. **List of at least two (2) installed base of similar cybersecurity solution in the Philippines, with one (1) Commercial or Universal Philippine Bank, with client name, contact person, complete address, contact number and email address supported with Certificate of Satisfactory Performance.**
 21. **Business Continuity Plan (BCP)** that are related to the Bank, and List of updated Technical Support Unit including name, contact number, and email address.
- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**
 22. **Business Tax Returns** per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.
 23. **Latest Income Tax Return** filed manually or through EFPS.

24. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
25. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
26. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

Financial Component (PDF File)

- ***The Financial Component shall contain documents sequentially arranged as follows:***
 1. Duly filled out Bid Form signed by the Bidder's authorized representative (sample form - Form No.1).
 2. Duly filled out Schedule of Prices signed by the Bidder's authorized representative (sample form - Form No.2).
 3. Duly filled out Bill of Quantities Form signed by the bidder's authorized representative (Annex E)

Note: The forms attached to the Bidding Documents may be reproduced or reformatted provided the information required in the original forms and other requirements like signatures, if applicable, are complied with in the submittal.

TERMS OF REFERENCE

Unified Identity Protection Platform Solution with Three (3) Years Support Services

Item No.	General Requirements
1	Extend modern identity security to any sensitive resources: Solution architecture needs to have end-to-end identity protection coverage without modifying servers and applications, deploying proxies in your network, or installing agents on your machines. This includes homegrown applications, legacy systems, admin command line access tools, file systems and databases, IT infrastructure and industrial systems. 1000 Software licenses.
2	Service account and privileged access protection: Protect highly privileged users and service accounts without the need to rotate passwords. Solution is required to automate discovery, monitoring and enforcement of adaptive access policies on these accounts, blocking any attempt to leverage them for malicious access.
3	Identity-based Zero Trust: Enforce identity-based Zero Trust access policies with a least-privilege approach by continuously analyzing the full context of users' access activity, from initial login through every resource within the hybrid network.
4	Lateral movement protection: Block lateral movement attacks and automated malware propagation in real time, by enforcing adaptive MFA protection on remote administration and access tools (RDP, SSH, PsExec, PowerShell, WMI, etc.).
5	Hybrid IAM consolidation: Consolidate the Identity Protection across your entire network, on-prem and cloud environments on your cloud IAM of choice (Azure AD, Okta, Ping, etc.), to enable unified visibility and security controls from a single console, including for assets that couldn't be migrated into your cloud IAM before.
6	Unified risk-based authentication: Leverage an AI-based risk engine to analyze access requests of users and service accounts across all networks, on-prem and cloud resources to detect identity-based attacks across your hybrid environment, and block them with adaptive access policies, while reducing disruption to the workforce.
7	Visibility and threat hunting: Gain a detailed view of every access event to all resources in your on-prem and multi-cloud environments to address security weak spots, detect malicious activity and conduct forensic investigations
Technical Requirements	
8	The proposed solution shall support distributed architecture which multiple nodes can be deployed geographically to receive authentication traffic from Identity Stores, while all nodes will be connected to a single administrative component.
9	The proposed solution shall support High Availability for nodes component. In the event one node is not fully functional, the Identity Store should be able to re-route authentication traffic to another available node seamlessly
10	All communication between administrative component and nodes must be secured.
11	Nodes shall be configured to continue processing authentications and enforcing verification independently, should the administrative component become unavailable
12	The proposed solution must not send out sensitive customer data outside. All sensitive customer data must be stored on-premise.
13	The proposed solution must be deployed within organization premises, which can be either virtual environment (VMware or Hyper-V) or cloud-based (AWS or Azure)
14	The proposed solution shall support fail-open scenario in the event all components are not available. User authentication traffic must not be disrupted but will only have one (1) factor authentication
15	In addition, the proposed solution shall support fail-close scenario as well if required.

16	The proposed solution shall support a "breakglass" option to de-activate all configured access policies without interrupting protected systems or applications
17	The proposed solution shall provide a holistic authentication platform which monitors user access across all systems and environments without agents, proxies or local configurations
18	The proposed solution shall seamlessly enforce verification on access to any sensitive system or device, across all corporate networks, cloud environments, or hybrid
19	When protecting sensitive resources, the proposed solution must not require deploying software agents or inline proxies and without integrations with individual systems. No modification is required on target systems or servers.
20	The proposed solution must not have any access to any password when analyzing authentication traffic.
21	The proposed solution shall support multiple Identity Stores such as Microsoft Active Directory and AzureAD.
22	The proposed solution shall support authentication through RADIUS protocol and verification of user credential with Microsoft Active Directory.
23	In addition, the proposed solution shall also support second-factor authentication for RADIUS request (Skip first-factor authentication (for example, username/password) and directly perform the second factor).
24	The proposed solution shall support an integration with Active Directory Federation Services (ADFS) through SAML and WS-Fed protocol so administrator can configure a policy based on the federated applications the user is trying to access
25	The proposed solution support evaluating authentication requests from applications federated with PingFed and OKTA
26	The proposed solution shall support mobile phone apps (IOS and Android) as a token. The proposed solution shall also support desktop notification such as Google Chrome extension and FIDO2 token as an option.
27	The proposed solution shall support time-based OTP as an alternative verification token option in which push notification cannot be used.
28	The proposed solution shall support native desktop notification on Windows and Mac systems. The notification can be triggered from internal network and does not rely on Internet access.
29	The proposed solution shall support customized look and feel for the needs of organization, including logos, wording and window location.
30	The proposed solution shall support monitoring authentication traffic from multiple domains without any agent or proxy or key
31	The proposed solution shall support monitoring authentication traffic from VPN and Firewall without any agent or proxy
32	The proposed solution shall support protection for Windows Logon when computer is online or offline
33	The proposed solution shall support protection for Windows Logon not only for personal use computers, but also for non-personal use computers such as stateless servers (launch a new and clean instance on each reboot).
34	The proposed solution shall support multi-factor enrollment and authentication capabilities for users who are authenticating using Azure AD without any agent or proxy
35	The proposed solution shall provide information such as servers, applications, and assets within multiple protected Identity sources, as well as the number of users and how they are authenticated. The information is useful to show which applications are heavily used and by how many users

36	The proposed solution shall provide a tool to collect information about Domain Controllers capacity in the network and to configure Domain Controllers to forward authentication traffic to proposed solution.
37	The tool provided shall provide detailed Domain Controllers information such as latency between Domain Controllers, performance for a set number of time, number of NTLM authentications per time, DC architecture, etc.
38	The proposed solution shall support API which allow a service to verify user's identity thereby protecting sensitive corporate resources from unauthorized access
39	The proposed solution shall support API to interact with the solution system such as get information, set configuration, input risk information, etc.
40	The proposed solution shall be able to discover, monitor, and protect service accounts
41	The proposed solution shall be able to visualize how the service accounts have been used in organization
42	The proposed solution shall be able to give notifications when a service account is used out from the allowed policy.
43	The proposed solution shall be able to prevent service account from being misused
44	The proposed solution shall be able to give warning notifications when a service account is used for interactive logins.
45	The proposed solution shall support a zero-trust policy in air-gapped network. The integration shall support second factor authentication using FIDO2 certified tokens such as YubiKey device.
46	The proposed solution shall enforce adaptive AI-driven Multi-Factors Authentication for access verification in the organization without agents, proxies or local configurations.
47	The proposed solution shall constantly calculate risks associated with each user, device, resource, etc. using combination methods: a. AI Engine – profile user's/device's/resource's normal authentication pattern and look for deviation b. Know Threats – identity-based attack patterns c. External Inputs
48	The proposed solution shall have a report which has valuable insights about risks discovered over a selected period of time.
System Administration Requirements	
49	The proposed solution shall be provided in a hardened virtual appliance. No additional Operating Systems or Database is required.
50	The proposed solution shall provide a secure Web Portal for Administrator to configure and manage
51	The proposed solution shall support admin security roles using Domain Group identity. Segregation roles are supported for admin and viewer. Access to each page must be able to be customized per role
52	The proposed solution shall support logon using domain credential with verification access to Admin Console Web Portal.
53	The proposed solution shall support SAML-based Single Sign On access to Admin Console Web Portal.
54	The proposed solution shall support customized company name and company logo displayed in management console and token apps

55	<p>The proposed solution shall provide an intuitive Dashboard which contains (not limited to):</p> <ul style="list-style-type: none"> a. Number of users and devices monitored by the system b. Authentication request progress and how it was handled c. Authentication by protocol d. System status e. Total services and total servers monitored f. Number of active users g. Number of active resources
56	<p>The proposed solution shall provide a full audit of every authentication activity in organization. The data displayed can be filtered by one more filters such as (not limited to):</p> <ul style="list-style-type: none"> a. User b. Device Name c. Server d. Date and Time e. Action f. Domain Controller g. Executed Policy h. IP Address i. MFA Response j. Protocol k. Result l. Risk m. Service
57	<p>The proposed solution shall provide a comprehensive yet simple page to display deeper knowledge on organization's security posture such as:</p> <ul style="list-style-type: none"> a. Active Directory Statistics information. b. Information on specific user or resource c. Inventory information such as number of Registered Domains, Security Groups, Servers, Organizational Units, Users, Services d. Users information such as number of Domain Admins, Privileged Users, Password Never Expire, Shadow Admins, Old Password, Shared Users, Admins with SPN e. Servers and Devices information such as number of Shared Devices, Suspected Service Account, Old Operating System, Stale Device f. Risk Statistics information such as Top Risk Users and Resources, Top Connected Users and Resources, Top Active Users and Resources, Number of Authentication Requests monitored, Number of Authentication by Protocol, Daily Trend for Active Account and Resources
58	<p>The proposed solution shall provide a tool for Administrator to investigate suspicious activity by a user or device in the network. The proposed solution shall also provide a detailed timeline and graphical representation of a user's or device's authentication actions over the past week</p>
59	<p>The proposed solution shall provide a capability for organization to identify risks based on their unique needs, such as special naming conventions for different resources and user types, or various compliance requirements</p>
60	<p>The proposed solution shall be able to provide a full audit of every authentication activity and highlight potential identity risks detected</p>
61	<p>The proposed solution shall provide monitoring capabilities to display:</p> <ul style="list-style-type: none"> a. Current system status b. Current component status, number of Domain Controller connected per component, sync details, date and time of most recent AD sync and logs c. Number of authentication attempts per second per protocol
62	<p>The proposed solution shall provide a built-in capability to initialize network traffic capture for advanced troubleshooting purpose</p>

63	The proposed solution shall provide a notification and event affecting the system. This view is especially useful when making configuration changes. The system administrator can quickly and easily check that updates have the desired effect on the system.
64	The proposed solution shall be upgraded from one administrative component regardless how many nodes deployed. The upgrade shall be done through a secure tunnel.
65	The proposed solution shall support sending log information to an external syslog server using CEF format
66	The proposed solution support for the use of external storage for persistent data (such as authentication logs).
67	The proposed solution shall support SNMP monitoring
68	The proposed solution shall provide a mechanism to add users and manage their verification tokens by: a. Provide customizable enrollment email for unpaired users to do self-enrollment b. Allow or deny access to users who have not completed the device pairing process c. Display information on paired users, pending-paired users, and excluded users
69	The proposed solution shall support user pairing with external email address (email address which are not in organization's email domain). This is especially useful for third party vendors such as contractors and partners who do not have an email address within an organization. The external users must have a domain user record with organization's Active Directory for verification.
70	The proposed solution shall support upgrading specific node only to minimize operation downtime during upgrade
71	The proposed solution shall provide a notification when a connectivity between components is lost
72	The proposed solution shall be able to generate a periodic custom reports of log records and send them to email recipients
	Access Policy Requirements
73	The proposed solution shall provide rules or policies to manage authentication requests based on the defined parameters such as protocol, user, group, device, resource, risk level, etc.
74	The proposed solution shall have a default rule to allow authentication requests
75	The proposed solution shall support managing multiple authentication protocols such as Kerberos, NTLM, LDAP, LDAPS, RADIUS
76	The proposed solution shall support the Require MFA Timeframe which control the frequency for MFA requests to be sent to the user, whether with every authentication request, or less frequently
77	The proposed solution shall support other verification methods such as FIDO2, Microsoft Authenticator, Okta Verify, Duo Mobile, RSA Approve, Ping Identity, HYPR.
78	The proposed solution shall support customized prompt message for user to know the context of incoming verification request
79	The proposed solution shall provide desktop notifications to notify users of pending step-up authentication. This is useful when adding verification to applications with non-configurable user interface such as hypervisors, PowerShell commands, or 3rd party applications.
80	The proposed solution shall support responding to authentication request with either Allow or Block or Trigger MFA option.
81	The proposed solution shall support responding to authentication request based on certain authentication risk level.

82	The proposed solution shall support responding to authentication request based on specific risk indicators such as suspected lateral movement, request using weak encryption method, etc
83	The proposed solution shall support to exclude specific device from a policy.
84	The proposed solution shall support triggering verification request based on the user trying to authenticate and the policy configuration. In addition, verification trigger can also be based on specific devices, specific resources, or both
85	The proposed solution shall support a configuration which determines the behaviour for unpaired users at both system level and policy level. The action can be either allow access or block access.
86	The proposed solution shall support setting policy by order or precedence
87	The proposed solution shall support policy grouping to group policies together, to reduce the number of verification requests, while not compromising on security
88	The proposed solution shall support creation of an authentication policy directly from a log entry in the Logs Table.
89	The proposed solution shall display policy usage statistics
90	The proposed solution shall support duplicating an existing policy to provide the basis for a new policy
91	The proposed solution shall be able to configure policy time which administrator can set the time periods in which a policy will be active
Enterprise Integration Requirements	
92	The proposed solution shall be able to integrate with leading security technology vendor, such as Check Point and Palo Alto Networks, to trigger step-up authentication for any suspicious user without requiring modifications to endpoints and servers
93	The proposed solution shall be able to integrate with SIEM solutions such as QRadar, Arcsight, Splunk, etc. using CEF format syslog
94	The proposed solution shall be able to integrate with Privileged Access Management (PAM) solution without any agent or configuration changes required on PAM solution. a. Enforce MFA protection on privileged accounts, regardless of access method, authentication protocol, or resource type b. Provide end-to-end coverage of your privileged service accounts with risk-based policies that cannot be protected with vaulting and password rotation, providing the same security level as human users
95	The proposed solution shall be able to integrate with Azure Active Directory (AD) to trigger a sign-in authentication with Azure SSO.
96	The proposed solution shall be able to collect sign-in information from an Azure Active Directory (AD) tenant. The information is used to enhance risk estimation for protected users, to provide a more accurate risk estimation, based on user activity both in Azure and on-prem.
97	The proposed solution shall be able to integrate with AzureAD to bridge authentication requests from identity sources to Azure AD for SSO. With this, organization can use all native Azure AD sign-in options, including push, SMS, phone calls, number matching, FIDO2, OTP, and more for onprem AD
Vendor Requirements	
98	Securities and Exchange Commission (SEC) Registration as proof that the bidder has at least ten (10) years of existence in the IT industry.

99	The vendor must be an authorized reseller of the brand being offered. Manufacturer's authorization or equivalent document confirming that the bidder is authorized to provide the brand being offered, including any warranty obligations and after sales support as may be required.
100	The vendor must have at least three (3) local Information Technology (IT) support engineers to support the installations, configurations and 24x7 uptime services within the warranty period. Must submit Certificate of Employment and Resume/Curriculum Vitae and Training/Seminar Certificates showing at least three (3) years work experience in handling the same product/services being procured or work experience in Cyber Security solutions.
101	The vendor must have a dedicated Project Manager (PM) to oversee the project. Certificate of Employment and Resume/Curriculum Vitae of the dedicated PM must be provided, showing at least three (3) years work experience and handled at least one (1) Commercial or Universal bank and one (1) non-bank client.
102	The vendor must have a local helpdesk to provide 24x7 technical assistance. Must provide detailed escalation procedure and support including contract number and email addresses.
103	The supplier must submit list with Certificate of Satisfactory Performance from at least two (2) installed base of Identity Protection Cybersecurity Solution wherein one (1) is a Universal or Commercial Philippine Bank, with client name, contact person, address, telephone number and email address.
104	The bidder must submit documents e.g. Business Continuity Plan (BCP) that are related to the Bank, and List of Updated Technical Support Unit (include name, contact number, and email address, etc.)
105	The winning bidder must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank internal audit and external audit such as Bangko Sentral ng Pilipinas (BSP), Commission on Audit (COA), etc.
106	Payment shall be made through direct credit to the vendor's deposit account with LANDBANK. The vendor is required to maintain a deposit account with LANDBANK's Cash Department or any of its Branches. The following documentary requirements for payment shall be submitted by the vendor: <ul style="list-style-type: none"> • Sales Invoice / Billing Statement / Statement of Account • Delivery Receipt with printed name and signature of LANDBANK employee who received the delivery and actual date of receipt of items
	Warranty
107	Three (3) year warranty on software. Warranty shall cover any reconfiguration after successful implementation.
	Support Services
108	Support services shall cover all software updates, patches and upgrades within the three (3) year support period.
	Delivery and Installation
109	Delivery, installation and configuration period: Must be completed within 90 calendar days after receipt of NTP.

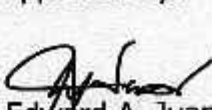
Prepared by:


Bryan Armand C. Cristobal
SITS, HONMD

Checked by:


Marvin A. Matanguihan
ITO, NOD

Approved by:


Edward A. Juan
Head, NOD