LANDBANK

SERVING THE NATION

SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-HOBAC-ITB-GS-20230328-02

PROJECT : **Supply, Delivery and Installation of Multifactor Authentication (MFA) Solution with 50 Hard Tokens and Three (3) Years Maintenance and Support Services**

IMPLEMENTOR : **HOBAC Secretariat Unit**

DATE : **May 25, 2023**

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) The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.

2) The Terms of Reference (Annexes D-1 to D-6), Technical Specifications (Section VII) and Checklist of Bidding Documents [Item No. 12 of Technical Documents and Item No. 14 of Other Documents to Support Compliance with Technical Specifications) have been revised. Please see attached revised Annexes D-1 to D-6, and specific sections of the Bidding Documents.

3) The submission and opening of bids is re-scheduled on **June 2, 2023** at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams.

ATTY. HONORIO T. DIAZ, JR.
Head, HOBAC Secretariat Unit

Technical Specifications

Specifications	Statement of Compliance
	Bidders must state below either "Comply" or "Not Comply" against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered. 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.
Supply, Delivery and Installation of Multifactor Authentication (MFA) Solution with 50 Hard Tokens and Three (3) Years Maintenance and Support Services 1. **Minimum technical specifications and other requirements per attached Revised Terms of Reference (Annexes D-1 to D-6).** 2. The documentary requirements enumerated in Annex D-6 – Vendor Requirements of the Terms of Reference shall be submitted in Eligibility and Technical Component to support the compliance of the Bid to the technical specifications and other requirements. Non-submission of the above documents may result in the post-disqualification of	**Please state here either "Comply" or "Not Comply"**

the bidder.	

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 Components (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.

- **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.

- **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. **Duly filled-out Revised Terms of Reference signed in all pages by the authorized representative/s of the bidder.**

15. Manufacturer's authorization (sample form - Form No. 9) or its equivalent document, confirming that the bidder is authorized to provide the brand being offered and consumables supplied by the manufacturer, including any warranty obligations and after sales support as may be required.

16. Manufacturer's certification that the vendor is authorized reseller/partner for 3 years.

17. Certificate of Employment, Resume/Curriculum Vitae and List of Trainings and Certifications of at least two (2) certified engineers of the solution.

18. Detailed Escalation Procedure and Support including contact numbers and email addresses.

19. List of at least three (3) installed base of similar solution and/or equivalent technology like SSL and IPSEC VPN and FTP in the Philippines, with one (1) Commercial or Universal Philippine Bank with client name, contact person, complete address, contact number and email address.

○ **Post-Qualification Documents/Requirements – <u>[The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:</u>**

20. 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.

21. Latest Income Tax Return filed manually or through EFPS.

22. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
23. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
24. 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).

<u>Financial Component (PDF File)</u>

- ***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.

LANDBANK OF THE PHILIPPINES

TERMS OF REFERENCE

SUPPLY, DELIVERY AND INSTALLATION OF MULTI-FACTOR AUTHENTICATION SOLUTION WITH FIFTY (50) HARD TOKENS & THREE (3) YEARS MAINTENANCE AND SUPPORT SERVICES

Technical Requirements:	**Compliance**
1.0 Multi-Factor Authentication Server (SID Access Appliance)	
The MFA authentication server must be able to support the following type of authenticators: * On-demand authenticator (Short Message System) * Hardware authenticator * Software authenticator	
The MFA authentication server must be available in both software and appliance form.	
The MFA authentication server must come with a RADIUS server with no additional cost.	
The solution must be a leader in the Gartner Magic Quadrant for User Authentication	
The management interface of the RADIUS server must be fully embedded within the same management console as the MFA authentication server to simplify setup and on-going management.	
The MFA authentication server and authenticators must be designed and manufactured by the same company or Original Equipment Manufacturer (OEM) for the same company.	
The MFA authenticators must be built and assembled by the same company.	
The MFA hardware authenticator must be the same brand with LANDBANK's existing authentication server appliance for redundancy.	
The MFA hardware authenticator seed used to generate the One Time Password or OTP must be created and generated only upon an order from a customer. It must not be pre injected in bulk without a genuine customer purchase.	
The MFA authentication server must support Security in Depth (SID) authentication protocol out-of-the-box with no additional customization required.	
The MFA authentication server must support CT-KIP (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.	
The MFA authentication server must provide Business Continuity Option without requiring the use of hardware authenticators for MFA authentication.	
The MFA authentication server must provide a user self-service portal out-of-the-box with no additional cost.	
The user self-service portal must provide the following functions: * Separated from the MFA authentication server to avoid exposing the server and to facilitate the hosting of self-service portal function in the DMZ. * Report a lost or unavailable token. If a user has left his hardware token at home while travelling, for example, an on-demand token code, or set of one-time token codes, is issued to authenticate him temporarily to the network. * Report a permanently lost or damaged token. This is similar to the above, except that an extra workflow can be initiated to disable the user's lost/damaged token and, if necessary, issue a new token to the user. * Forgotten PIN. A token code can be issued to the user to authenticate before a PIN reset is initiated as an extra security precaution. * Grant Emergency Access. In the event a user forgets both login and PIN, emergency access can be granted by asking the user 'life questions' pre-populated from the database.	

Annex

Revised. D-1

* Request a replacement token. * Test a token.	
* Workflow provisioning for the creation of productivity saving processes that speed deployment scenarios and ease the work load of IT staff.	
The MFA authentication server must support the use of an external LDAP directory without making changes to the data schema. The following external LDAP directory must be supported: * Authentication Manager internal database * Oracle Directory Server Enterprise Edition 11G * Microsoft Active Directory	
The administration user interface of the MFA authentication server must be web-based and the communication channel must be encrypted.	
The solution must provide Microsoft Management Console Snap-in.	
The MFA authentication server must provide delegated multi-level administration capability. It must enable granular administrative access control down to a user/group and policy level.	
The MFA authentication solution must be able to integrate with over 350 certified third-party applications out-of-the-box with no customization required.	
The MFA authentication server must be able to support software authenticators for the following platforms: **1. Smartphones** **a. iPhone IOS Devices** **b. Android Phones, including Huawei** **c. Windows Mobile devices** 2. Laptops and Desktops a. Microsoft Windows b. Mac OS X 3. Web Browsers a. SID Toolbar b. SID Software Token for Web SDK 4. Mobile SDK a. iOS b. Android	
The MFA authentication server must provide API function calls usable by customized applications that require MFA authentication integration. The API function calls should be able available for Java and C# programming language.	
The MFA authentication server must support 15 replicas when necessary.	
The MFA authentication server must provide load balancing capabilities for authentication request across all of the authentication servers including replicas.	
The MFA authentication server must support propriety protocol based on strong cryptographic algorithms based on AES.	
The MFA authentication server must be a leader in the Gartner's User Authentication Quadrant.	
The MFA authentication server must protect authentication password stored in the server using SHA-256.	
Sensitive data at rest stored in the database must be encrypted with AES and SHA cryptographic algorithms.	
Trust between primary and secondary servers must be secured by 2 way SSL channel.	

2.0 Authenticators (50 units)	
2.1 Hardware Authenticator	
The hardware authenticator must come with lifetime warranty and free replacement during the lifetime.	
The hardware authenticator must be water resistant.	
The hardware authenticator must not be made and assembled in China.	
The hardware authenticator must conform to the following standards: * Tamper evidence: ISO 13491-1; ISO DIS 13491-2:2005 * Product safety standards: RoHS, WEEE, CE, cRoHS * Regulatory standards: FCC Part 15 Class A and Class B, EN55022 Class A and Class B	
The hardware authenticator must be able to operate normally within -15C to 60C operating temperature.	
The hardware authenticator must provide fix battery lifespan options as follows: * 2 years * 3 years * 4 years * 5 years	
The OTP (One-Time Password) generated by the token must: * be random and not in running sequence * be automatically replaced by another random number every thirty or sixty seconds without having the need to press any buttons. * not be allowed to be used more than once * expire and becomes invalid after 30 or 60 seconds	
The OTP must be generated based on AES 128-bit ECB mode.	
The hardware authenticator must become unusable when being tampered or forced open.	
The LCD display of the hardware authenticator must provide countdown bars on the left of the display signalling when the code on the token will change to a different number.	
There must be a flashing dot on the bottom right of the display indicating that the token is functioning.	
When the hardware authenticator is going to expire within the next month, a small numerical three must be displayed above the flashing dot.	
When the token actually expires, the token must provide the following indication: * Numbers on the display disappear * The tiny three remains to indicate that the token has expired.	
The back of the token must contains certain token specific information such as the date of expiration, and the serial number of the token – engraved, printed and in bar code format.	
2.2 Software Authenticator	
Software authenticator must support the following platforms out-of-the-box with no customization required: **1. Smartphones** **a. iPhone IOS Devices** **b. Android Phones, including Huawei** **c. Windows Mobile devices** 2. Laptops and Desktops a. Microsoft Windows b. Mac OS X	

Revised Annex D-3

3. Web Browsers a. SID Toolbar b. SID Software Token for Web SDK 4. Mobile SDK a. iOS b. Android	
Software authenticator must support the industry leading Security in Depth (SID) authentication protocol.	
Software authenticator must support CT-KIP (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.	
Up to ten software tokens must be supported on one device.	
The "seed record" must be securely stored on smart card and USB devices and used in conjunction with the software authenticator on the user's desktop for maximum security.	
2.3 On-Demand Authenticator	
The on-demand authenticator must support both sms and email as the delivery medium.	
2.4 Risk-based Authentication	
The solution must support risk-based authentication based on device identification and user behaviour information captured by SSL VPNs, web portals, OWA and Sharepoint.	
The risk engine in the risk-based authentication must provide SMS OTP or challenge questions when assurance level is identified as risky.	
2.5 Partner Authenticators	
The MFA solution must support the following partner authenticators: * USB Flash Devices * Biometric Devices * Trusted Platform Modules	
3.0 Authentication Agent	
The MFA solution must provide authentication agents to enable MFA authentication for different software operating platforms at no additional cost.	
The authentication agents must support the following platforms: 1. Microsoft Windows a. 32 Bit Platforms * Windows Server 2012 & Up * Windows 7 & Up b. 64 Bit Platforms * Windows Server 2012 & Up * Windows 7 & Up 2. Sun Java Web Server 3. Apache Web Server 4. Internet Information Server 5. Red Hat Enterprise Linux Version 6 and above 6. HP-UX 7. Sun Solaris 8. IBM AIX Version 5.3 and above 9. SUSE Linux 10. VMware ESX Version 6.5 and above	
Authentication agent for Microsoft Windows must provide the following functionality:	

* Local Authentication Client – A component that enforces RSA SecurID authentication during logon to the Windows desktop. * RSA EAP Client – A plug-in into the Microsoft Wireless and VPN client. The plug-in enables RSA SecurID authentication over a VPN, Dial-up or wireless connection established using native Microsoft Wireless and VPN software. The component is supporetd on the desktop class systems. * Remote Authentication Server – A plug-in into Microsoft IAS RADIUS Server or RRAS. This server-side component enables RSA SecurID authentication using a native Microsoft RADIUS environment. The component is supported on the server class systems. * Online and Offline Authentication - Must provide offline authentication mechanism in case the authentication server is not available.	
Authentication agent for Apache Web Server must provide the following functionality: * Local, domain, and multi-domain access * Private SSL communication channel between user and web server * Wireless access protocol authentication * Controls user and group access privileges to protected web resources * Provides customizable activity trace/security log, exception, incident, and system usage reports * Uses tamper-evident cookies to prevent cookie alteration or forging	
Authentication agent for Internet Information Service must provide the following functionality: * Local, domain, and multi-domain access * Private SSL communication channel between user and web server * Wireless access protocol authentication * Single sign-on access for Microsoft Outlook Web Access on Microsoft Exchange server 2013 SP1 and 2010 SP3 * Single sign-on access for Microsoft Exchange server 2013 SP1 and 2010 SP3 * Single sign-on access for Microsoft Office Sharepoint Server 2010 and 2013 * Controls user and group access privileges to protected web resources * Provides customizable activity trace/security log, exception, incident, and system usage reports * Uses tamper-evident cookies to prevent cookie alteration or forging	
Authentication agent for Unix/Linux must support PAM (Pluggable Authentication Module) and enable MFA authentication for the following tools and services: * login * rlogin * dtlogin * telnet * rsh * su * ftp * sftp * ssh * scp	
The authentication agent must be protected by a cryptographic algorithm.	

4.0 Administration Module	
Administration module must provide the following PIN policy settings: * Number of failed authentication attempts before system will lock the user account. * Period of time before systems automatically unlock the user account. * PIN characters requirement. * PIN length. * PIN history (cannot use the same PIN for period of time). * PIN can be randomly generated by authentication server or created by user themselves. * Number of days for offline authentication.	
5.0 Vendor Requirments	
The manufacturer must provide a certification that the vendor is an authorized reseller/partner of the proposed product; the manufacturer must also state that the vendor is reseller/partner for 3 years. Must submit certifications	
Three (3) years warranty on software and must have a local helpdesk to provide a 24x7 technical assistance. Warranty shall also cover any reconfiguration/integration after successful implementation. Must submit warranty certificates and must provide detailes escalation procedure, business continuity plan and support including contact numbers and email addresses.	
The vendor shall provide at least two (2) certified engineers of the solution. Must submit certification of certified engineers/s and certificate of employment.	
The vendor must have at-least three (3) installed base of similar solution and or equivalent technology like SSL and IPSEC VPN and FTP, one of which a Bank. Must submit list of installed base with client name, contact person, address, telephone number and email address.	
The winning bidder must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank (e.g. BSP, Third Party Auditor, etc.) Must submit [e.g. Latest Financial Statement (FS), Business Continuity Plan (BCP) that are related to the Bank, and List of Updated Technical Support (include name, contact numbers and email address), etc].	
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: • 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	
Delivery after receipt of NTP: 60 days	
Installation will start 1 week after delivery and will end 90 days after.	

Edward A. Juan
ITO, NOD-LAN

Archieval B. Tolentino
IT Manager, NOD

Enrique L. Sazon, Jr.
VP, NOD

Revised Annex D-6