



SERVING
THE NATION

LANDBANK

**SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-HOBAC-ITB-GS-2022621-01**

PROJECT : **Three (3) Years Subscription for Attack Surface Management Solution**

IMPLEMENTOR : **HOBAC Secretariat**

DATE : **October 21, 2022**

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-4), Technical Specifications (Section VII), and Checklist of Bidding Documents (Item 12 of Technical Documents and Items 20 & 21 of Other Documents to Support Compliance with Technical Specifications) have been revised. Please see attached revised Annexes D-1 to D-4 and specific sections of the Bidding Documents.
- 3) Responses to bidder's queries/clarifications (Annex G).


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

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. |
|---|--|
| <p>Three (3) Years Subscription for Attack Surface Management Solution</p> <p>1. Minimum technical specifications and other requirements per attached Revised Annexes D-1 and D-4.</p> <p>2. The documentary requirements enumerated in Item Nos. 47, 48, 49, 50, 51, 52 and 53 of the Revised Technical Specifications shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements.</p> <p>Non-submission of the above documents may result in the post-disqualification of the bidder.</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 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 or Domestic Entity.

○ **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 Terms of Reference signed in all pages by the authorized representative/s of the bidder.
15. Notarized Certification that bidder has at least five (5) years existence in the IT industry with reference to SEC Registration document.
16. Notarized manufacturer's certification as gold partner and authorized vendor/integrator to sell and provide support of the product.
17. Manufacturer's authorization (sample form - Form No. 9) or its equivalent document, confirming that the bidder is authorized to provide the product/ solution supplied by the manufacturer, including any warranty obligations and after sales support as may be required.
18. Certificate of Employment, Curriculum Vitae, Valid Certification and Training/Seminar Certificates of at least three (3) certified local IT support engineers with at least three (3) years work experience in handling the product being offered and other related products.
19. Certificate of Employment and Curriculum Vitae of a dedicated Project Manager 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 distributor's local sales and technical office in the Philippines for guaranteed support with address, contact person and contact number.**
21. **List of at least two (2) installed base clients in the Philippines of the same brand and model being offered from Commercial/Universal Bank, Financial Institution or Philippine Government Agency with name of client, bank, agency, contact person, contact number, address and email address.**
22. Detailed Escalation and Support Plan Procedure.

- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**
 - 23. 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.
 - 24. Latest Income Tax Return filed manually or through EFPS.
 - 25. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
 - 26. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
 - 27. 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.

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

| | |
|--|---|
| DATE | OCTOBER 17, 2022 |
| PROJECT IDENTIFICATION NO. | LBP HOBAC ITB-GS-2022621-01 |
| PROJECT NAME | Three (3) Years Subscription for Attack Surface Management Solution |
| PROPONENT UNIT/TECHNICAL WORKING GROUP | Network Operations Department |

| ITEM NO. | PORTION OF BIDDING DOCUMENTS | QUERIES AND /OR SUGGESTIONS | LANDBANK'S RESPONSES |
|----------|---|---|--|
| 51 | The Manufacturer's must have local sales and technical office in the Philippines for guaranteed support. Bidder must submit the Manufacturer's address, contact number, and contact person | Can the bank relax the requirement of the Manufacturer having a local sales office here for guaranteed support with Just the local Distributor office representing the Manufacturer or Principal (Product) being offered to the Bank? The distributor representing product here together with the Bidder (Vendor) has its own support team to guarantee support | YES. Included in the revised TOR. The Local Distributor and the Bidder of the product being offered must have local sales and technical office in the Philippines for guaranteed support. Must submit the address, contact number, and contact person. |
| 52 | The Bidder must have at least two (2) installed base in the Philippines of the same brand and model being offered where one (1) is a Commercial or Universal Philippine Bank. Must submit a list of installed base with (client name, contact person, address, telephone number and email). | Can the bank relax or accept the two (2) installed base in the Philippines of the same brand and model being offered from a Government Agency and Telco instead of at least one (1) from any Commercial or Universal Bank? | YES. Included in the revised TOR. The supplier must have at least two (2) installed base on the same brand being offered in the Philippines wherein one (1) is from either of the (Commercial/Universal Philippine bank, Financial Institution or Philippine Government Agency). Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed. |

Three (3) Years Subscription for Attack Surface Management Solution – Terms of References

Objective: To provide a continuous discovery, classifying and security monitoring of external LANDBANK assets (internet-facing, digital assets contains or process bank data) including recently merged (UCPB), that might be vulnerable or where an attacker could use as an entry point to penetrate and gain access to the bank systems and extract data or any sensitive information.

| | Technical Specifications | Comply? |
|--|---|---------|
| Assets Discovery and Management | | |
| 1 | The solution must provide detailed discovery path and location of up to 10,000 assets. | |
| 2 | Must group and attribute assets to business units and organizational structure. | |
| 3 | Must perform continuously and externally on Internet facing IT Infrastructure. | |
| 4 | Must perform without requiring input information or data from the client (E.g., seed information, IP ranges to scan, etc.). | |
| 5 | Must perform without requiring any software or hardware deployment, integration, or configuration. | |
| 6 | Require no whitelisting, firewall or access control changes. | |
| 7 | Must perform in a way that resembles regular internet "background noise" to simulate a sophisticated attacker's mode of stealthy operations | |
| 8 | Discover and map exposed databases regardless of the port used (e.g. a MySQL, SQL, MongoDB, ElasticSearch etc.) offering might be running in a port not typically used for those offerings. | |
| 9 | Assets Types should be but not limited to IP Addresses, Domain Names, SSL Certificates & Web Applications | |
| 10 | Must automatically assign business context to the discovered assets. | |
| 11 | Able to cluster all the relevant asset types that are associated with a specific web application. | |
| 12 | Must be able to identify technology platforms and/or products (E.g., Cisco Routers, Citrix VPNs, etc.). | |
| 13 | Must be able to identify and assign a risk/security ranking or grade to every asset based on issues / vulnerabilities / misconfigurations/etc. | |
| 14 | The offered solution can rank assets based on discoverability or how easily an asset can be found and associated with the organization. | |
| 15 | The offered solution can rank assets based on the attractiveness to attackers (perceived business value). | |
| 16 | Must be able to support customer requests for additions and exclusions of assets. | |
| 17 | Can support role-based access control to limit viewing of assets to an assigned organization's staff. | |

| | | |
|--------------------------------------|--|--|
| 18 | Must be able to search for assets based on platform type, environment, discoverability, customer-created tags, and other applicable parameters. | |
| Attack Vector Detection | | |
| 18 | Must performed as a "Black-Box" analysis of an unbiased attacker's reconnaissance techniques. | |
| 19 | Must be able to run in a way that poses no danger to business continuity or technical operations for customizing scenarios. | |
| 20 | Must be able to find highly exploitable assets and issues that can provide access to other critical assets. | |
| 21 | Must be able to find and detect the following security issues: 1. Server and Application Vulnerabilities 2. Server and Application Misconfiguration issues 3. Architecture/Network Design issue 4. Authentication Misconfiguration issues 5. Default Credentials 6. Encryption Weaknesses 7. Man-in-the-Middle Susceptibility 8. Phishing Threats 9. Data Exposures 10. Cross Site Scripting (XSS) 11. Decryption Threats (i.e. Exposed Certificates) 12. Code Injection Risks 13. Domain Spoofing Risks 14. DNS Hijacking Issues 15. DOS Threats 16. Certificate Expiration 17. Known CVEs Against External IP Addresses 18. Known CVEs Against Vulnerable Software | |
| Prioritizing Remediation | | |
| 22 | Must provide guidance on prioritizing security issues. | |
| 23 | Can prioritize based on how discoverable the asset is as it is related to the organization. | |
| 24 | Can prioritize based on an attractiveness level from the attackers perspective - "Perceived" business value. | |
| 25 | Can prioritize based on Exploitation Complexity | |
| 26 | Must be able to provide detailed remediation recommendations. | |
| 27 | Must be able to provide additional threat intelligence to help prioritize security issues. | |
| Integrations & Workflows: | | |
| 28 | Must be able to natively support integration with orchestration third-party applications being used by the LANDBANK. | |
| 29 | Must be able to provide automation workflows within its application (E.g., changing investigation statuses and commenting on assets and issues). | |
| 30 | Must have a REST API that can be used to extract asset and issue endpoint data for integrations with orchestration solutions being used by LANDBANK. | |
| 31 | Must allow export of asset and issue data in CSV format for integrations with the bank current Security Information and Events Management (SIEM) or other reporting tool. | |

| | | |
|---|--|--|
| 32 | Must support customer-created comments or tags (e.g. organizational tags). | |
| 33 | Must support applying customer-created tags via individual and bulk actions. | |
| 34 | Must support automated alerts generated via custom user-selected filters; (for example, can the offering be configured to proactively send emails to specific users when the number of critical severity issues or number of cloud workloads change). | |
| 35 | Must allow for integration using condition based recipes across a multitude of services. | |
| Software as a Service (SaaS) Support & Access: | | |
| 36 | Can access the data collected and processed by the offering through a web portal or API. | |
| 37 | The offered solution can technically enforce password complexity (e.g. length, character types). | |
| 38 | Must support single sign-on (SSO) using Identity and Access Management standard protocols (e.g. SAML, OAuth, OpenID Connect). | |
| 39 | Must support role-based access control | |
| 40 | Access can be granted to specific teams and users for specific subsidiary information relevant to their business. | |
| 41 | Must encrypt user credentials at rest | |
| 42 | Must encrypt all communications between the user and the application via HTTPS. | |
| 43 | Must maintain a user-viewable audit log that tracks user activities, including login/logoff, exports, report generation, user management, and modifications of access permissions. | |
| 44 | The offered solution must be ISO 27001 Certified | |
| 45 | The offered solution must be GDPR (General Data Protection Regulation) compliant. | |
| 46 | Does not require any changes to software, hardware, firewalls, agents, integrations, or any customer configurations whatsoever. | |
| Supplier's Eligibility Requirements | | |
| 47 | The supplier must be at least five (5) Years of existence in the IT Industry. Information should be based from SEC (Security and Exchange Commission) incorporation information, that the vendor is at least five (5) years. The bidder must submit a notarize certification from them with reference to SEC documents. | |
| 48 | The supplier must submit manufacturer's certification as the Gold Partner | |
| 49 | The supplier must have at least three (3) certified local engineers of the solution provided to support the installations, configurations and 24x7 uptime series within the warranty period. Must submit Certificate of employment and Resume/Curriculum Vitae (that the local IT support engineers has at-least 3 years work experience in handling of the product being offered or other related products, include list of trainings, unexpired certification and seminars attended) | |
| 50 | The supplier must have a dedicated Project Manager (PM) to oversee the project. Must submit Certificate of Employment and Resume/Curriculum Vitae (that the PM has at-least 3 years work experience and handled at least One (1) Commercial or Universal bank and one (1) non-bank clients as proof of his/her experience on how to handle projects.) | |
| 51 | The Local Distributor and the Bidder of the product being offered must have local sales and technical office in the Philippines for guaranteed support. Must submit the address, contact number, and contact person. | |

| | | |
|----|--|--|
| | | |
| 52 | The bidder must have of at least two (2) installed based of the same brand being offered in the Philippines wherein one (1) is from either of the (Commercial/Universal Philippine bank, Financial Institution or Philippine Government Agency). Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed. | |
| 53 | The Bidder must have a local Helpdesk to provide 24 x 7 technical assistance. The Bidders must submit the escalation procedure and support plan flow chart/details. | |
| 54 | The Bidder must provide knowledge transfer training for at-least five (5) LBP IT personnel | |
| 55 | Three (3) years warranty on Software. Warranty shall also cover any reconfiguration/integration after successful implementation. (The warranty certificate will be submitted by the winning bidder) | |
| | Other Requirements | |
| 56 | The Winning Bidder must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank's Internal Audit and External auditors such as Bangko Sentral ng Pilipinas (BSP), Commission of Audit (COA), 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] | |
| | Delivery Terms and Condition | |
| 57 | Delivery after receipt of NTP: 60 calendar days | |
| 58 | Installation will start 7 calendar days after delivery and will end 90 calendar days after | |


Prepared by:


JAY-R.G. JADREN
SITS - LAN Team

Checked by:


ARCHIEVAL B. TOLENTINO
ITM - LAN Team

Approved by:


ENRIQUE L. SAZON JR.
VP - NOD