



LANDBANK

**SUPPLEMENTAL/BID BULLETIN NO. 1  
For LBP-ICTBAC- ITB-GS-20250609-02**


**PROJECT : Supply, Delivery and Installation of Additional Intrusion Prevention System with Three (3) Years Warranty and Support Services**

**DATE : 09 July 2025**

---

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.

1. Response to the bidders queries per attached Annex H.
2. Section VII. Technical Specification (pages 41-42), Checklist of the Bidding Documents (pages 63-66) and Terms of Reference (Annex D-1 to D-8) 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 is on 18 July 2025 at 10:00 AM and the Opening is on 18 July 2025 at 10:15 AM. **Late bids will not be accepted.**
4. The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.

  
**SVP MARILOU L. VILLAFRANCA**  
Chairperson, ICT-BAC



(632) 8522-0000 | 8551-2200 | 8450-7001  
[www.landbank.com](http://www.landbank.com)



LANDBANK Plaza, 1598 M.H. Del Pilar corner  
Dr. J. Quintos Sts., Malate, Manila, Philippines 1004



**LANDBANK**

SERVING THE NATION



BAGONG PILIPINAS

**CLASS D**

Project Identification No	LBP-ICTBAC-ITB-GS-20250609-02
Project Name	Supply, Delivery and Installation of Additional Intrusion Prevention System with Three (3) Years Warranty and Support Services
Subject	Responses to Bidder's Queries

Item No.	Portion of Bidding Documents	Queries And/Or Suggestions	LBP Responses
6	The solution must support up to <b>120 million</b> concurrent connections	In reference to this RFP, may we clarify the following.  <b>Item #6 of the TOR, which states below:</b> <ul style="list-style-type: none"> <li>The solution must support up to <b>120 million</b> concurrent connections</li> </ul>	We will retain item #12 where the device should support 300 million concurrent sessions and will remove item #6 on the revised Terms of Reference.
12	The solution should be able to support up to 1 million new connections per second and <b>300 million</b> concurrent sessions	<b>Item #12 of the TOR, which states below:</b> <ul style="list-style-type: none"> <li>The solution should be able to support up to 1 million new connections per second and <b>300 million</b> concurrent sessions.</li> </ul> <p><b>For Clarifications:</b> Our question is which from the 2 items above are we going to follow for the Concurrent Connections requirement?</p>	

Evaluated by:

**MARK ANTHONY YABUT**  
SITS - LAN Team

Checked by:

**JAY-R G. JADREN**  
ITO - LAN Team

Approved by:

**EDWARD A. JUAN**  
HEAD - HONMD

ANNEX #

## Technical Specifications

Specifications	Statement of Compliance
<p><b>Supply, Delivery and Installation of Additional Intrusion Prevention System with Three (3) Years Warranty and Support Services</b></p> <ol style="list-style-type: none"> <li>1. Minimum technical specifications and other requirements per attached <b>Revised Annexes D-1 to D-8</b>.</li> <li>2. The documentary requirements enumerated in Annexes D-5 and D-6 of the Terms of Reference shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements.</li> </ol> <p>Non-submission of the above documents may result in the post-disqualification of the bidder.</p>	<p><b>Bidders must signify their compliance to the Technical Specifications/Terms of Reference by stating below either “Comply” or “Not Comply”</b></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><b>Please state here either “Comply” or “Not Comply”</b></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.

○ **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. **Revised Section VII – 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 Technical Specifications and Terms of Reference duly accomplished and signed in all pages by the authorized representative/s of the bidder.**
  15. Securities and Exchange Commission (SEC) Registration as proof that the bidder has at least ten (10) years of existence in the IT industry.
  16. 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.
  17. Valid Certification or Website URL link for verification as proof that the bidder is an ISO 9000: 2015 and ISO/IEC 27001:2022 certified.
  18. Certificate of Employment (indicating the date hired), Resume/Curriculum Vitae, Certificate of Training/Seminar related to the proposed solution and at least two (2) valid Cybersecurity Certifications each of at least two (2) Local Support Engineers who are employed with the bidder for at least three (3) years and with at least one (1) year experience in implementation, administration and support of the proposed solution.
  19. Certificate of Employment (indicating the date hired), Resume/Curriculum Vitae and Project Management Professional (PMP) or Information Technology Infrastructure Library (ITIL) Certification of one (1) Project Manager (PM) who is employed with the bidder for at least two (2) years and with at least three (3) years of experience in project management. The dedicated PM shall have handled IT Security solution for at least one (1) Philippine bank and one (1) non-bank client [with names of end-user/client company name, project name and project duration (start and end date)].
  20. List of at least one (1) installed base of the same or other Intrusion Prevention System solution in a Financial/Insurance or Government Institution with client name, address, contact person, contact number and email address.
  21. Security Incident Management and Communication Plan in handling security incidents such as but not limited to:
    - Loss of information due to unknown reasons
    - Hardware resources and component lost/stolen
    - Virus incident regarding e-mail, internet and others
    - Supply chain attacks in the hardware and software being used
    - Critical security vulnerabilities in firmware and software
    - Exploiting weakness in existing infrastructure, policies and standards
  22. Detailed Escalation Procedure and Support Plan Flow Chart.

23. Business Continuity Plan that will support the operations of a Commercial or Universal Bank and List of Updated Technical Support (including names, contact numbers and email addresses).
- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**
  24. 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.
  25. Latest Income Tax Return filed manually or through EFPS.
  26. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
  27. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
  28. 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.***



### Technical Specifications and Terms of Reference for Supply, Delivery and Installation of additional Intrusion Prevention System with Three (3) Years warranty and support

**Objectives:** *The Intrusion Prevention System solution will be installed in the bank's colocation site to continuously monitor, prevent identified threats, and secure the bank's internal network from malicious attacks.*

No	Technical Specifications	Comply	Remarks
1	The solution should be a Next-Generation Intrusion Prevention System and is based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane		
2	The solution underlying OS must be based on the proprietary OS and not general purpose OS such as Windows, Linux or Unix OS to prevent common vulnerabilities.		
3	The solution should be capable of trusting traffic and bypassing it by configuring rules in hardware layer		
4	The solution allows VLAN translation selectively inspect traffic based on the configuration of the aggregation or distribution switch.		
5	The solution should have a flexible licensing model based on the customer's inspection throughput needs.		
6	The solution must have a latency of less than sixty (60) microseconds.		
<b>Hardware Specifications</b>			
7	The solution should have two (2) 4-segment 10G Fiber Bypass interface		
8	The solution should have redundant hot-swappable power supply		
9	The solution should have an on-box 240GB SSD storage		
10	The solution should have 2 network I/O modules slots that supports different modular bypass interfaces		
11	The solution should be able to support up to 1 million new connections per second and 300 million concurrent sessions.		
12	The solution should be able to support up to 20,000 new TLS connections per second and 250,000 concurrent TLS connections		
13	The solution should have a scalability that can support up to 40Gbps inspection throughput capacity in a single 1RU appliance.		
<b>High Availability</b>			
14	The solution must support full redundancy solution (Active-Passive, Active-Active).		
15	The solution must able to operate in Asymmetric traffic environment with Digital Vaccine filters protection.		
16	The solution must support high-availability without any synchronization.		
17	The solution must have a built-in power failure bypass module that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedures		
18	The solution must support Dual Power Supplies		
19	The solution must be scalable by using Link aggregation, such as 5Gbps IPS can be scalable to 10Gbps by adding additional 5Gbps IPS to the second link aggregation.		

20	The solution must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors.		
21	The solution must support Adaptive Filter Configuration (AFC) which will alert or disable ineffective filter in case of noisy filters		
22	The solution must support hitless OS upgrade/Reboot which allow upgrading of the IPS operating system without required network downtime		
23	The solution must have the solution for scalability that can support up to 200Gbps IPS throughput.		
<b>Security Coverage</b>			
24	The solution must provide intrusion prevention functionality out of the box		
25	The solution filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine		
26	The solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic, detect and block unknown threats associated with known malware families as well as unknown malware in real-time as they enter and cross the network		
27	<p>The solution filters must be categories into the following categories for easy management. For example.</p> <ul style="list-style-type: none"> <li>• Exploits</li> <li>• Identity Theft/Phishing</li> <li>• Reconnaissance</li> <li>• Security Policy</li> <li>• Spyware</li> <li>• Virus</li> <li>• Vulnerabilities</li> <li>• Network Equipment</li> <li>• Traffic Normalization</li> <li>• Peer to Peer</li> <li>• Internet Messaging</li> <li>• Streaming Media</li> </ul>		
28	<p>The solution must have the following security features on top of the IPS filters:</p> <ul style="list-style-type: none"> <li>• Domain Generation Algorithm (DGA) Defense family</li> <li>• Ransomware protection</li> <li>• Identify malicious Internet Protocol (IP)</li> </ul>		
29	<p>The solution must be able to support granular security policy enforcement based on the following methods:</p> <ul style="list-style-type: none"> <li>• Per IPS device (all segments)</li> <li>• Per physical segment uni-direction and bi-directional</li> <li>• Per 802.1Q VLAN Tag uni-direction and bi-directional</li> <li>• Per CIDR IP address range</li> <li>• Per 802.1Q VLAN Tag and CIDR as well</li> <li>• Firewall policy per security profile</li> <li>• "Vulnerability based filter are known for most effectively for Zero Day Attack Protection. There must be a vulnerability-based filters as part of the security policies. "</li> </ul>		
30	The solution should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods		
31	The solution must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc		

32	The solution must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C		
33	The solution must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment		
34	The solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploitability type and the reputation score		
35	The solution engine must be a smart enough to inspect the traffic based on condition (if then else). If the traffic is suspicious then it goes for the deep packet inspection		
36	The solution engine must be a smart enough to block the malicious traffic without further inspection on subsequent packets after the packets turn out to be a malicious traffic from the unknown traffic		
<b>Threat Intelligence Updates</b>			
37	The solution must support update on a daily/weekly basis.		
38	The solution must be able to provide zero-day filters that must be included in weekly signature update.		
39	The solution vendor must provide a global threat intelligence portal that provide real-time monitoring and statistics of malicious threats and attacks		
40	The solution must have the ability to view attack activities base on continent and countries		
41	The solution must allow drill-down to view detailed threat source and destination data on each attack type		
42	The solution must have the ability to monitor and highlight recent new and growing threats		
<b>Central Management Appliance</b>			
43	The solution must support a centralized management server for enterprise management of the IPS devices.		
44	The centralized management server must be an appliance based on a hardened OS shipped by-default from factory		
45	The centralized management server must have at least 64GB RAM and 800GB storage (2x800GB disks, RAID 1)		
46	The centralized management server should have redundant hot-swappable power supply		
47	The central management server should be a single 1RU appliance		
48	The central management server should be able to store up to 200 million historical events		
49	The central management server should have a GbE RJ45 out-of-band remote management such as iDRAC or iLO		
50	The central management server shall be able to manage at least 25 IPS system.		
51	The central management server shall allow the update of latest Digital Vaccine to be manually, automatically or based on schedule		
52	The central management server shall also be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through IPS.		
53	The central management server should serve as a central point for IPS security policies management including versioning, rollback, import and export (backup) tasks.		

54	The central management server must provide rich reporting capabilities. For example, (All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report)		
55	The central management server must support the report generation on a manual or schedule (Daily, Weekly and Monthly) basis		
56	The central management server must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.		
57	The central management server must support the archiving and backup of events and export to NFS, SMB, SCP and sFTP.		
58	The central management server shall be able to provide different level of users account and access management. It shall provide at least 3 level - SuperUser, Administrator and User		
59	The central management server must be able to support the syslog format.		
60	The central management server must support Active Directory for user ID correlation		
61	The central management server must support 3rd party leading Vulnerability Management scanners.		
62	The central management server shall have a big data engine that allows customers to provide faster security analytics and faster report generation		
63	The central management server shall support the drill-down events from the report templates, such as drill-down from top 10 attacks report.		
64	The central management server shall support 'threat insights' dashboard that show correlated data such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered		
65	The central management server must be able to integrate with the existing Endpoint and Server Security solution to share IOC (Indicator of compromise) feed with IPS for protection		
<b>Load Management</b>			
66	The solution must support an Out-Of-Band ethernet management port.		
67	The solution must have at least one (1) RJ45 console port		
68	The solution should support SSH2/Telnet and HTTPS/HTTP as a means of local management.		
69	The solution must support SNMP and a private MIB that can be utilized from an Enterprise Management Application.		
70	The solution must be able to be managed locally independently without any centralized management server		
71	The solution must support the option to send events in syslog messages, SNMP Traps and SMTP email messages within the need for a centralized management server		
<b>Other Requirements</b>			
72	The supplier 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.		
73	<p>The supplier must notify the bank IT personnel of any related security incidents such as, but not limited to:</p> <ul style="list-style-type: none"> <li>• Loss of information due to unknown reasons</li> <li>• Hardware resources and component lost/stolen</li> <li>• Virus incident regarding e-mail, internet and others.</li> <li>• Supply chain attacks in the hardware and software being used.</li> </ul>		

	<ul style="list-style-type: none"> <li>• Critical security vulnerabilities in firmware and software</li> <li>• Exploiting weakness in existing infrastructure, policies and standards</li> </ul> <p>It must be reported within 24 hours' time-frame upon learning or confirming of the incident.</p>		
74	The supplier must notify the bank IT personnel through email, SMS, Calls or other channels of any critical security vulnerability, firmware upgrade and performance patches and fixes that is needed to be applied. Application of fixes, patches, upgrade, etc. Should be supported by a Methods of Procedure (MOP) before the implementation.		
75	The supplier shall be subjected to Performance Assessment regularly. The results of the Performance Assessment shall be considered in the renewal of the contract. The performance assessment of the winning bidder shall also be considered upon them entering into other contracts with the Bank.		
76	The vendor must provide/conduct semi-annual health check or as requested by the bank IT personnel.		
<b>Bidder's Eligibility Requirements</b>			
77	Securities and Exchange Commission (SEC) Registration as proof that the bidder has at least ten (10) years of existence in the IT industry.		
78	The bidder must be an authorized reseller or distributor of the brand being offered. The bidder must submit certification from the principal.		
79	The bidder must be an ISO 9000: 2015 and ISO/IEC 27001:2022 certified. Must submit un-expired certification or provide website URL link for verification.		
80	<p>The bidder must have at least Two (2) Local Support Engineer to support the re-configuration, maintenance and online/onsite support within the contract period.</p> <ul style="list-style-type: none"> <li>• Must be employed with the bidder for at least three (3) year before the bid opening</li> <li>• At least one (1) year experience in implementation, administration &amp; support of the proposed solution.</li> <li>• Each local engineer must have at-least two (2) Certification in Cybersecurity such as (but not limited to) ISC2, CompTIA Security+, CySA+, GIAC Security Essential, CISA, CEH, OSCP, SSCP and other related security certifications.</li> </ul> <p><b>Must submit the following:</b></p> <ul style="list-style-type: none"> <li>• Certificate of Employment for the assigned personnel indicating the date of hire</li> <li>• Resume or Curriculum Vitae indicating that the personnel assigned have training and experience to support the proposed solution.</li> <li>• Must submit un-expired cybersecurity certification.</li> </ul>		
81	<p>The bidder must have One (1) Project Manager who shall oversee the implementation of the solution, ensuring they are properly implemented and fine-tuned.</p> <ul style="list-style-type: none"> <li>• Must be employed with the bidder for at least two (2) years before the bid opening</li> <li>• At least three (3) years working experience in project management.</li> <li>• Must be Project Management Professional (PMP) or Information Technology Infrastructure Library (ITIL) Certified.</li> </ul> <p><b>Must submit the following:</b></p> <ul style="list-style-type: none"> <li>• Certificate of Employment for the assigned personnel indicating the date of hire.</li> </ul>		

	<ul style="list-style-type: none"> <li>Resume or Curriculum Vitae indicating that the personnel assigned have handled Information Technology Security solutions for at least one (1) Philippine bank and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date).</li> <li>Project Management Professional (PMP) or Information Technology Infrastructure Library (ITIL) Certification</li> </ul>																						
82	The bidder must have one (1) installed base of the same or other Intrusion Prevention System solution in a Financial / Insurance or Government institution. Must submit list of installed bases with client name, contact person, address, telephone number and email address.																						
83	<p>The bidder must submit Security Incident Management and Communication Plan in handling security incidents such as, but not limited to:</p> <ul style="list-style-type: none"> <li>Loss of information due to unknown reasons</li> <li>Hardware resources and component lost/stolen</li> <li>Virus incident regarding e-mail, internet and others.</li> <li>Supply chain attacks in the hardware and software being used.</li> <li>Critical security vulnerabilities in firmware and software</li> <li>Exploiting weakness in existing infrastructure, policies and standards</li> </ul>																						
84	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.																						
85	The bidder must submit a Business Continuity Plan (BCP) that will support the operations of a Commercial or Universal Bank, and List of Updated Technical Support (include name, contact numbers, and email addresses)																						
<b>Service Level Agreement (SLA)</b>																							
86	<p>The supplier must have a response time of 30 minutes to four (4) hours maximum upon receipt of calls to Service Desk/Helpdesk facility.</p> <table border="1"> <thead> <tr> <th>Severity Level</th><th>Service Response Time</th><th>Resolution Timetable (if can be resolved online)</th><th>Resolution Timetable (if can be resolved onsite)</th></tr> </thead> <tbody> <tr> <td>Level 1</td><td>30 minutes response time and within 120 minutes to be onsite (if needed)</td><td>Within 4 hours from the initial call or email</td><td>Within 4 hours from the time the Engineer arrives on site</td></tr> <tr> <td>Level 2</td><td>30 minutes response time and within 240 minutes to be onsite (if needed)</td><td>Within 8 hours from the initial call or email</td><td>Within 8 hours from the time the Engineer arrives on site</td></tr> <tr> <td>Level 3</td><td>180 minutes response time and onsite the next business day (if needed)</td><td>Within 2 business days from the initial call or email</td><td>Within 24 hours from the time the Engineer arrives on site</td></tr> <tr> <td>Level 4</td><td>240 minutes response time and scheduled* activities agreed with the customer (if needed)</td><td>Within 5 business days as scheduled</td><td>Within 5 Business Days as scheduled</td></tr> </tbody> </table>	Severity Level	Service Response Time	Resolution Timetable (if can be resolved online)	Resolution Timetable (if can be resolved onsite)	Level 1	30 minutes response time and within 120 minutes to be onsite (if needed)	Within 4 hours from the initial call or email	Within 4 hours from the time the Engineer arrives on site	Level 2	30 minutes response time and within 240 minutes to be onsite (if needed)	Within 8 hours from the initial call or email	Within 8 hours from the time the Engineer arrives on site	Level 3	180 minutes response time and onsite the next business day (if needed)	Within 2 business days from the initial call or email	Within 24 hours from the time the Engineer arrives on site	Level 4	240 minutes response time and scheduled* activities agreed with the customer (if needed)	Within 5 business days as scheduled	Within 5 Business Days as scheduled		
Severity Level	Service Response Time	Resolution Timetable (if can be resolved online)	Resolution Timetable (if can be resolved onsite)																				
Level 1	30 minutes response time and within 120 minutes to be onsite (if needed)	Within 4 hours from the initial call or email	Within 4 hours from the time the Engineer arrives on site																				
Level 2	30 minutes response time and within 240 minutes to be onsite (if needed)	Within 8 hours from the initial call or email	Within 8 hours from the time the Engineer arrives on site																				
Level 3	180 minutes response time and onsite the next business day (if needed)	Within 2 business days from the initial call or email	Within 24 hours from the time the Engineer arrives on site																				
Level 4	240 minutes response time and scheduled* activities agreed with the customer (if needed)	Within 5 business days as scheduled	Within 5 Business Days as scheduled																				
<b>Warranty</b>																							
87	Three (3) years warranty on hardware and software. Warranty shall cover any reconfiguration after successful implementation.																						
<b>Support and Services</b>																							
88	Three (3) years support and services includes installation, software updates, patches, and upgrades within this period.																						

<b>Delivery/Contract Period</b>			
89	Delivery and installation period: Within Sixty (60) calendar days upon receipt of Notice to Proceed (NTP)		
<b>Payment Terms and Condition</b>			
90	<ul style="list-style-type: none"> <li>One-Time payment on hardware and software after receipt of Certificate of Completion and Acceptance</li> <li>Maintenance and Services payable annually for three (3) years</li> </ul>		
91	Pursuant to Malacañang Executive Order No. 170 (Re: Adoption of Digital Payments for Government Disbursements and Collections) issued on 12 May 2022, directing all government agencies to utilize safe and efficient digital disbursement in the payment of goods, services and other disbursements, all payments for this Contract shall be through direct credit to the supplier's deposit account with LANDBANK. Thus, the supplier shall maintain a deposit account with any LANDBANK Branch where the proceeds of its billings under this Contract shall be credited.		
92	<p>The following documentary requirements for payment shall be submitted:</p> <ul style="list-style-type: none"> <li>Sales invoice/Billing Statement/Statement of Account on or before the 15<sup>th</sup> day after every delivery</li> <li>Delivery Receipt with printed name and signature of LANDBANK employee who received the delivery and actual date of receipt of items; and</li> <li>Warranty Certificate specifying the period covered by the warranty (if applicable)</li> <li>Updated Tax Clearance in accordance with Malacañang Executive Order No. 398, series of 2005 and BIR Regulations No. 17-2024.</li> </ul> <p>The Supplier shall be paid within sixty (60) calendar days after submission of sales invoice or claim and complete documentary requirements.</p>		
<b>Liquidated Damages</b>			
93	If the winning bidder fails to delivery any or all of the goods and/or services within the period/s specified in this Contract, the Bank shall, without prejudice to its other remedies under this Contract and under the Applicable Law, deduct from the contract price, as liquidated damages, a sum equivalent to one-tenth of one percent (0.001) of the price of the unperformed portion of the goods and/or services for each day of delay based on the approved contract. LANDBANK need not prove that it has incurred actual damages to be entitled to liquidated damages. Such amount shall be deducted from any money due or which may become due to Supplier. In case the total sum of liquidated damages reached ten percent (10%) of the total contract price, LANDBANK may rescind the contract and impose appropriate sanctions over and above the liquidated damages to be paid.		
<b>Pre-Termination/Termination of Contract</b>			
94	<p>Pre-termination/Termination of Contract shall be governed by the guidelines on Termination of the Contract per Annex "I" of the 2016 Revised Implementing Rules and Regulations.</p> <p>In addition to the grounds under the said Guidelines for Contract Termination, Unsatisfactory Performance by the service provider within the contract duration shall likewise be ground for Pre-Termination/Termination of contract.</p>		

Contact Person			
95	Name: Mark Anthony Yabut Email Address: mayabut@landbank.com Contact Number: 025220000 loc 7759		
	Name: Jay-R G. Jadren Email Address: jjadren@landbank.com Contact Number: 0284057769		

Prepared By:

MARK ANTHONY YABUT  
SITS, HONMD

Reviewed By:

JAY-R G. JADREN  
SITO, HONMD

Noted By:

EDWARD A. JUAN  
HEAD, HONMD