PROJECT	:	**Three (3) Years Subscription for Email Cloud Anti-Spam and Security Solution**
IMPLEMENTOR	:	**HOBAC Secretariat Unit**
DATE	:	**April 5, 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-4), Technical Specifications (Section VII) and Checklist of Bidding Documents (Item 12 of the Technical Component) have been revised. Please see revised Annexes D-1 to D-4 and specific sections of the Bidding Documents.

3)   Responses to bidder's queries/clarifications (Annex H).

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

Land Bank of the Philippines
LANDBANK Plaza, 1598 M.H. Del Pilar corner Dr. J. Quintos Sts., Malate, Manila, Philippines 1004
T (632) 8522-0000 8551-2200 8450-7001   **W** www.landbank.com

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.
Three (3) Years Subscription for Email Cloud Anti-Spam and Security Solution 1. Minimum technical specifications and other requirements per attached Revised Terms of Reference (Annexes D-1 to D-4). 2. The documentary requirements indicated in the Revised Terms of Reference (Annex D-3) shall be submitted in support of 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 the bidder.	**Please state here either "Comply" or "Not Comply"**

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:_**

  o **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.

o **Technical Documents**

9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder.

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.*

o **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**

1. Notarized self-certification with reference to Securities and Exchange Commission showing at least five (5) years of existence in the IT Industry.

2. Manufacturer's authorization (sample form - Form No. 9) or back to back certification confirming that the bidder is authorized to provide the subscription supplied by the principal, including any warranty obligations and after sales support as may be required.

3. Certificate of Employment, Resume/Curriculum Vitae and list of seminars and trainings attended of at least two (2) certified local engineers, showing at least three (3) years work experience in handling the offered IT product or other related products and have at least one (1) year experience in handling email cloud security products.

4. Certificate of Employment and resume/curriculum vitae of the dedicated Project Manager showing at least three (3) years work experience and handled at least one (1) Philippine Commercial or Universal Bank and one (1) non-bank client.

5. Manufacturer's complete address, contact numbers and contact person.

6. List of at least two (2) installed base in the Philippines of the same brand of Email Security Solution being offered, wherein one (1) is a Commercial or Universal Bank, with client name, contact person, complete address, contact number and email address.

7. Escalation Procedure and Support Plan Flow Chart/Details.

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

1. 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.

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

3. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).

4. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

5. 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 Forms 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.

Three (3) Years Subscription for Email Cloud Anti-Spam and Security Solution – Terms of References

Objective: To provide protection in the Bank cloud-based email mailboxes/users against spam that may clog up inboxes, spreads malware and viruses, phishing, and unsolicited product/promotions. To provide email-based security authentication requirements such as SPF, DKIM and DMARC.

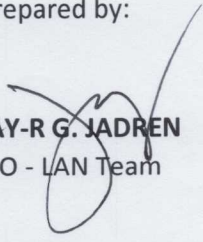|	Technical Specifications	Comply?
General Requirements		
1	The email security system offering should be Software-as-a-Service (SaaS) offering to protect customers from email-based threats before they reach a user's mailbox.	
2	**The email security solution should be compatible and interoperable with LANDBANK's existing email security gateway. Compatibility and operability of the system shall mean minimal or no configuration change and no downtime due to MX record propagation.**	
3	The gateway should support a comprehensive email security solution defense against latest email threats such as Graymail Safe unsubscribing, snowshoe spam, viruses, Malicious URL Blocking, URL category-based filtering, Robust anti-APT, DNS RBL verification, reputation filtering and phishing filtering utilizing a strong global threat intelligence capability	
4	The solution should support 5,000 users for anti-spam, anti-virus, virus outbreak, Anti-APT, Graymail and File reputation. All features required from day one.	
5	Solution should have false positive efficacy of 1 in 1 million	
6	Proposed solution should have greater than 99% spam catch rate and should be a leader/Top Player in published email security gateway report	
7	Propose solution should not be software based and installed in mail server. It should be purpose built dedicated email security gateway.	
8	Proposed solution should support centralized reporting and message tracking.	
9	Proposed solution should support spam quarantine on centralized management system. Holds spam and suspected spam messages for end users and allow end users and administrators to review messages that are flagged as spam before making a final determination.	
10	The solution should support ability to perform SMTP session control and traffic rate limiting according to sender's IP address/range, domain, or email reputation. The solution should be able to assign maximum SMTP sessions per IP address.	
11	The solution should perform SMTP conversational bounce for invalid recipients (prevent Non-Delivery Report Attack), directory harvest prevention, and have ability to perform SMTP session control and traffic rate limiting (down to per recipient) according to sender's IP address/range, domain, or email reputation.	
12	Solution should have Multi-layer Anti-spam filter: It should have capability to scan mails for spam with 3rd party SPAM engine before OEM Spam engine.	
13	The solution should have the option for dual virus scanning available.	

Revised Annex D-1

14	**The solution should provide protection against zero-day and targeted attacks. It should be able to dynamically analyze message attachments for malware.**	
15	The solution shall ensure that the cloud solution is available (i.e., not experiencing a Service Outage) for 99.9% of the time during each calendar month.	
16	The solution must have a cloud service Point Of Presence (POPs) in Asia Pacific region for better performance and reliability.	
17	The solution must have a low-latency cloud access for a faster and responsive user access.	
Email Security Features		
18	The proposed sandbox capability should support 200 file uploads per day.	
19	To proactively respond to cyber threats such as malware, ransomware, phishing attacks, solution should have capability to consume external threat information in STIX/TAXII	
20	The solution should provide virus outbreak prevention on abnormal increase of emails with specific email attachments	
21	Solution should support scanning of URLs in message attachment and perform action on such message.	
22	The solution should provide the URL defense service to: Re-write the original suspicious URL in the mail body to another URL and On clicking the re-written URL, the browser session should pass through a cloud based Web security scanning infrastructure of the same product.	
23	Solution should be able perform URL filtering on shortened URIs, and retrieve actual URL from shortened URL and perform action based on reputation score	
24	Solution should provide forged email detection protection against business executive compromise and provide detail logs on all attempts and actions.	
25	The solution should have the option to do certificate management capabilities for S/MIME encryption and/or digital signatures including support for access to public key repositories, ability to harvest public keys from received emails, and export/import of public keys both individually or in bulk.	
26	The solution should support for SPF, DKIM, and DMARC email authentication including ability to apply email authentication requirements based on domain (specific or wildcard), ability to quarantine emails failing authentication, DMARC reporting, and any other authentication policy features. Include ability to selectively confirm email authentication success (SPF, DKIM, DMARC) for inbound messages on other filtering policies that may include whitelisting of those addresses.	
27	The solution should support following for system monitoring: - SNMP v2/v3, MIB-II, XML, Syslog support	
28	The solution should be able to consume external threat information in STIX Format communicated over TAXII Protocol	
29	The Solution should be able to integrate with Domain Reputation Service that provides a reputation verdict for email messages based on a sender's domain and other attributes.	
30	The Solution should come and integrate with a cloud-based platform that provides automation and orchestration capabilities to accelerate threat investigations and incident management.	
31	Quarantine Feature should be available for Centralized management instance from day 1	
32	Full quarantine access for Administrator or delegated Quarantined access.	

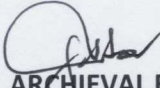Revised Annex D-2

33	The solution should provide separate Quarantine areas for different functionalities such as:	
34	Dedicated Spam Quarantine to quarantine spam/suspect-spam	
35	Virus Quarantine – to quarantine virus files	
36	Outbreak Quarantine – Dynamically quarantine zero-day threats	
37	Policy Quarantine – to quarantine based on policy such as "quarantine outbound Resume's"	
Supplier's Eligibility Requirements		
38	The supplier must be at least five (5) Years of existence in the IT Industry. Information should be based on 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.	
39	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from the principal.	
40	The supplier must have at least two (2) local Information Technology (IT) engineers to support the configurations and provide onsite support. Must submit the following: • Certificate of employment (must have at-least 3 years of work experience and have handled email cloud security products for at-least a year) • Resume or Curriculum Vitae Trainings and Seminars attended (including email cloud security related seminars)	
41	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.)	
42	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	
43	The Bidder must have at-least two (2) installed base in the Philippines of the same brand of Email Security solution being offered, wherein one (1) is a Commercial or Universal Philippine Bank. Must submit a list of installed bases with (client name, contact person, address, telephone number and email).	
44	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.	
45	The Bidder must provide knowledge transfer training for at-least five (5) LBP IT personnel	
46	The Bidder must provide Three (3) years Warranty on Product and Services. Services must also cover any reconfiguration/integration after successful implementation.	
	Other Requirements	
47	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.	
48	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 and Payment Terms and Condition	

Revised Annex D-3

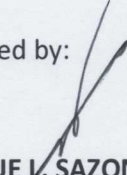| 50	Delivery after receipt of NTP: 30 calendar days	
51	The supplier must submit the following requirements for payment: • Sales invoice/Billing Statement/Statement of Account • Delivery Receipt with printed name and signature of LANDBANK employee who received the delivery and actual date of receipt of items. Payment shall be through direct credit to the supplier's deposit account with LANDBANK. The supplier is required to maintain a deposit account with LANDBANK's Cash Department or any of its Branches.	
52	Subscription and Services will start 7 calendar days after delivery	

Prepared by:

JAY-R G. JADREN
ITO - LAN Team

Checked by:

ARCHIEVAL B. TOLENTINO
ITM - LAN Team

Approved by:

ENRIQUE L. SAZON JR.
VP - NOD

Revised Annex D-4

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

DATE	March 27, 2023
PROJECT IDENTIFICATION NO.	ITB-GS-20230302-01
PROJECT NAME	Three (3) Years Subscription for Email Cloud Anti-Spam and Security Solution
PROPONENT UNIT/TECHNICAL WORKING GROUP	

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS	LANDBANK's RESPONSES
1	The email security system offering should be able to fully integrate with the existing LANDBANK's Email Security Gateway system infrastructure. Must be the same brand for seamless integration.	May we know the bank's existing email security gateway solution?	Ironport ESA
2		TOR mentioned it should be same brand for seamless integration - May we continue to offer other solution as long as we can comply with ALL the technical specifications and seamlessly integrate during implementation?	Yes, As long it will work and avoid long downtime but it should be a different Email Security solution (3rd party) and not a Microsoft Security product in order to provide countercheck against email threats.
3			
4			
5			

ANNEX H