



**LANDBANK**

SERVING  
THE NATION

**SUPPLEMENTAL/BID BULLETIN NO. 3  
For LBP-HOBAC-ITB-GS-20230706-02**

**PROJECT** : **Three (3) Years Subscription for Email Cloud Advanced Threat Protection**

**IMPLEMENTOR** : **HOBAC Secretariat Unit**

**DATE** : **September 1, 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 Nos. 1 and 8 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) Responses to bidder's query/clarifications per Annexes G-1 to G-5.
- 4) The submission and opening of bids is re-scheduled on September 8, 2023 at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams

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

# Technical Specifications

<b>Specifications</b>	<b>Statement of Compliance</b>
<p>Three (3) Years Subscription for Email Cloud Advanced Threat Protection</p> <ol style="list-style-type: none"><li><b>1. Terms of Reference and other requirements per attached Revised Annexes D-1 to D-6.</b></li><li><b>2. The documentary requirements indicated in the Revised Terms of Reference (Revised Annex D-5) shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements.</b></li></ol> <p>Non-submission of the above documents may result in the post-disqualification of the bidder.</p>	<p><b>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.</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 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. **Revised 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)]**
  1. **Duly filled-out Revised Terms of Reference signed in all pages by the authorized representative/s of the bidder.**
  2. Certificate or Attestation of Compliance that the vendor is compliant with the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC 2) Type II Certification for Security and Confidentiality.
  3. Datasheet or website reference showing list of countries presence in the in Asia Pacific Region for the Cloud Service Point of Presence.
  4. Notarized self-certification with reference to Securities and Exchange Commission showing at least five (5) years of existence in the IT Industry.
  5. Manufacturer's authorization (sample form - Form No. 9) or back to back certification confirming that the bidder is authorized to provide the subscription being offered and consumable supplied by the manufacturer, including any warranty obligations and after sales support as may be required.
  6. Certificate of Employment, resume/curriculum vitae, and list of seminars and trainings attended of at least two (2) local Information Technology engineers with at least three (3) years work experience and at least one (1) year experience in handling the email cloud security products.
  7. Manufacturer's complete address, contact numbers and contact person.
  8. **List of at least two (2) installed base in the Philippines of the same brand or any Email Advanced Persistent Threat (APT) Security solution being offered, wherein one (1) is a Commercial or Universal Philippine Bank, with client name, contact person, complete address, contact number and email address.**
  
- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**
  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 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.***

April 10, 2023

**Three (3) Years Subscription for Email Cloud Advanced Threat Protection for 5000 user mailbox licenses – Terms of References**

**Objective:** To provide an Advance Email Threat protection in the Bank cloud-based email services by providing real-time detection and prevention against email threats in the form of email-based spam, hidden threats in the attachment (malware, ransomware, viruses), embedded URLs linked to phishing sites, fraudulent wire transfer request and weaponized file attachments.

	Technical Specifications	Comply?
<b>General Requirements</b>		
1	The solution must provide Three (3) years support and license subscriptions for Email Cloud Advanced Threat Protection for 5000 mailbox/email users	
<b>Advanced Email Threat Protection Solution</b>		
2	The proposed solution must be a Software-As-A-Service (SaaS) cloud with 5000 mailbox/email users license.	
3	The proposed solution must be able to analyzed and quarantined (blocked) if unknown and advanced threats are found hidden in the following:  -All attachment types, including EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives -Password-protected and encrypted attachments -Credential-phishing and typosquatting URLs -URLs embedded in emails, PDFs, and Microsoft Office documents - OS, browser, and application vulnerabilities -Malicious code embedded in spear-phishing emails	
4	The proposed solution must support image classification engine that uses deep learning to compile and compare screenshots of trusted and commonly targeted brands against web and login pages referenced by URLs in an email.	
5	The proposed solution must detect phishing attacks in email using domain and page content analytics augmenting machine learning based detection.	
6	The proposed solution must support a technology engine to detects zero-day, multiflow, and other evasive attacks by using dynamic, signatureless analysis in safe virtual environments	
7	The proposed cloud solution should be integrated with the existing Network Advance Threat Protection solution of the bank. The integration must include the quick the alert correlation of alerts from the email and network advance threat protection solution.	
8	The proposed cloud solution must be able detect, isolate, and immediately stop URL, and attachment-based attacks, before they enter an organization’s environment.	
9	The cloud solution must supports sending of email trace logs to remote rsyslog server.	
10	The proposed cloud solution must allow administrators to create create Advanced Threat Engine Configuration policies. These polices should enables admins to allow or block specified URLs and attachment hashes (MD5/SHA256).	

LANDBANK PROCD  
AUG 14 2023 3:21PM



11	The proposed cloud solution must supports searching of mails by attachment MD5/SHA256 hashes and attachment names in the Email Trace.	
12	The proposed cloud solution must support various signature, analytics, and machine learning capabilities to detect URL-based email phishing attacks	
13	The solution must support deep learning capabilities that compiles and compares screenshots of trusted and commonly targeted brands against web and login pages referenced by URLs contained within an email.	
14	The solution must support auto remediation policy either quarantine, move to an administrator-defined folder, or permanent deletion.	
15	The solution must support inline deployment mode or Out of Band (OOB) mode	
16	The solution must be able to extract suspicious URLs that are embedded in a PDF file within an email message body. If the embedded URL that is extracted from the PDF file is detected as malicious, the solution must immediately block the email from being delivered to the recipient and marks the malicious email for quarantine.	
17	The solution must have protection from Advanced Evasion Techniques (AETs) that use malformed email as the attack vector. This attack attempt to bypass detection by using emails that have non-compliant headers or non-compliant Multipurpose Internet Mail Extensions (MIME) attachment header formats.	
18	The solution must support retroactive alerting. If the solution delivers an email to end users containing a URL not currently known to be malicious. Then if that URL is later determined to be malicious, a retroactive alert should be generated by the solution.	
19	The solution must support native dashboard statistics that includes a threat map which displays threat locations	
20	The solution must support integration with Microsoft O365 in inline mode for protection against advance threats and targeted email attacks.	
21	The solution must support auto remediation policy either quarantine, move to an administrator-defined folder, or permanent deletion.	
22	The solution must support seamless API integration with Office 365 for auto remediation. Should supports auto remediation for Office 365 to remove the emails from user's inbox when retroactive alert is generated by the solution.	
23	The proposed solution must support API for acknowledging alerts, marking alerts as read, and deleting alerts using API.	
24	The proposed solution must allow administrators to create and schedule automatic dashboard reports. Created reports must be able to send to up to 5 recipients.	
25	The proposed solution must support RESTful APIs for custom integration. The APIs must be for Advanced Threats, Email Trace and Quarantine functionalities.	
26	The proposed cloud solution must support APIs for the following Advance Threat alerts functions: -Alert summary request, -Alert details request, -Download alert artifact as ZIP request, -Download alert malware files as ZIP request, -Download alert PCAP files as ZIP request, -Alert acknowledge request, -Alert delete request, -Alert read request, -URL click reporting request	
27	The cloud solution must support APIs for the following email quarantine functions: -Download quarantined email request,	

	<ul style="list-style-type: none"> <li>-Bulk release quarantined email request,</li> <li>-Release quarantined email request,</li> <li>-Bulk delete quarantined email request,</li> <li>-Delete quarantined email request,</li> <li>-Query quarantined email request,</li> </ul>	
28	<p>The proposed cloud solution must support APIs for the following email trace functions:</p> <ul style="list-style-type: none"> <li>-Email trace request,</li> <li>-Message trace information request,</li> <li>-Original message ID request,</li> <li>-Downstream message ID request,</li> <li>-Message file request,</li> <li>-Remediate messages request,</li> </ul>	
29	The solution must be able to retain quarantined emails within 15 days (including current day)	
30	The solution must be able to retain the alerts within 90 days (including current day)	
31	The solution must be able to retain events within 31 days (including current day)	
32	The solution must be able to retain Dashboard Data within 3 months (including current month)	
33	The solution must be able to retain email trace within 31 days (including current day)	
34	The solution must be able to retain activity logs within 90 days (including current day)	
35	The solution must be hosted in cloud that provides real-time, dynamic threat protection without the use of signatures to protect an organization across the email threat vector. The solution must include an end-user portal that allows quarantine management, as well as review of malicious email and statistics.	
36	The solution must support BCC deployment mode option that provides passive (out of band) analysis of incoming email to identify advanced threats	
37	The solution must support inline deployment mode that provides active (inline) analysis of incoming email to identify advanced threats. In this mode the malicious email should be blocked and quarantined.	
38	<b>The proposed solution must have native integration with existing central management appliance of the bank. The email alerts should be seen from the existing central management console. The integration must be using a web socket over TLS using port 443.</b>	
39	The cloud solution should be able to integrate with on-prem Network Advance Threat Protection for alerts correlation between web and email vector	
40	The solution must support daily digests of all the quarantined emails for specific user/recipient. If enabled by the admin, the end user may be able to release some of the emails him/herself.	
41	<p>The solution must supports native Dashboard displaying the following information</p> <ol style="list-style-type: none"> <li>a. Email Traffic Volume, broken down by Received, Accepted, and Delivered</li> <li>b. chart of the types of email attachments contained in the email messages</li> <li>c. Top Sender email addresses that sent the most suspicious or malicious email for the specified time period, along with the total size of content sent</li> <li>d. Top Recipient email addresses that received the most suspicious or malicious email, and the total size of that content</li> <li>e. Advanced Threats graph of the number of threats over the specified time period</li> <li>f. Recent Alerts</li> <li>g. Threat Map with color-coded map of the world which details Countries identified as sources of suspicious emails displayed in color representing the relative threat.</li> </ol>	

	The above information should be able to display from the last few hours, a day, a week, or the last 30 days.	
42	The solution must provide the following information on every Advance Threat Alert: Alert ID, Date and time that the malicious email was received, Sender's email address, Targeted email addresses, Malicious email subject, MD5 hash, Malicious URL or name of the malicious attachment file, originating email server that sent the malicious email, Email Status (ie. Quarantined, released, delivered, etc.), Threat classification of the malicious attachment or URL, and Severity (High, Medium, Low) of the malicious attachment or URL	
43	The solution must be able to provide information about the dynamic analysis that includes the malware file type, vulnerable applications and operating systems, whether the organization's current antivirus solution would have detected the malware, message-digest algorithm (MD5) and checksum of the malicious file.	
44	The solution must be able to provide forensic evidence like the detected actual malicious file in a protected archived file and any associated network activity packet captures (VM Captures).	
45	The solution must provide Malware Communications report that includes the analysis that was performed by the system pertaining to any URL that the malware communicated with. Information displayed in the report should include the HTTP method, host name, and port that were used to connect to the malicious site. It should also include a copy of the raw request.	
46	The solution must provide native report that includes the analysis that was performed by the system on any operating system changes that occurred. Information displayed should include services that were started or stopped, registry keys that were modified, and other system configuration changes that occurred.	
47	The solution must have Threat Intel report that provides all the intelligence information on a threat detected, including the threat name, risk level, and type associated with a threat. It must also detail the affected software, vulnerability information, and its remediation patches if available. It must give a summary of the risk, information about how it can spread, the known targets for a specific type of malicious content or URL and the attribution associated with the threat.	
48	The solution must allow the administrator either to release or delete quarantined emails natively via the Web GUI/Portal	
49	The solution must provide an executive summary report of the email traffic during the selected dates. The report must include data about the type of traffic received and delivered, content analysis, and distribution across threat categories. The report must also include top rejection reasons and information such as the policies violated or matched by the accepted emails.	
50	The solution must be able to dynamically analyze the following attached file types: EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 and ZIP/RAR/TNEF archives	
51	The solution must be able to dynamically analyze the attached files even with password-protected and encrypted	
52	The solution must be able to detect and block the 3 primary categories of advanced threats in emails: attachment and URL	
53	The vendor 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	
54	The cloud solution must be SOC2 Type II compliant. The vendor must comply with the American Institute of Certified Public Accountants (AICPA) Service Organization Controls	

	(SOC 2) Type II Certification for Security and Confidentiality. Must provide certificate or attestation of compliance.	
55	The solution must be able to fully integrate with the bank existing On-premises email Anti-APT infrastructure/solution for seamless integration.	
56	The solution should be cloud-based, with no hardware or software to install.	
57	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	
58	The solution must have a cloud service Point Of Presence (POPs) in Asia Pacific region or locations for better performance and reliability. Must provide data sheet or website with the list of countries presence.	
59	The solution must have a low-latency cloud access for a faster and responsive user access.	
<b>Supplier's Eligibility Requirements</b>		
60	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.	
61	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from the principal.	
62	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: <ul style="list-style-type: none"> <li>• Certificate of employment (must have at-least 3 years of work experience and have handled email cloud security products for at-least a year)</li> <li>• Resume or Curriculum Vitae</li> <li>• List of Trainings and Seminars attended (including email cloud security related seminars)</li> </ul>	
63	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.	
64	<b>The Bidder must have at-least two (2) installed base in the Philippines of the same brand or any Email Advanced Persistent Threat (APT) Security solution, where 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).</b>	
65	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.	
66	The Bidder must provide knowledge transfer training for at-least five (5) LBP IT personnel	
67	The Bidder must provide Three (3) years Warranty on Product and Services. Services must also cover any reconfiguration/integration after successful implementation.	
<b>Other Requirements</b>		
68	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.	
69	The winning bidder 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]	
<b>Payment and Delivery Terms and Condition</b>		
70	Payable Annually for Three (3) Years	
71	Delivery upon receipt of NTP: 30 calendar days	

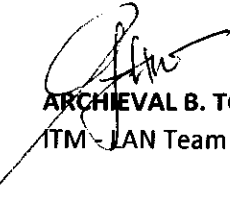
Revised  
Part 11 of  
107

72	Subscription and Services will start 7 calendar days after delivery	
73	<p>The supplier must submit the following requirements for payment:</p> <ul style="list-style-type: none"><li>• Sales invoice/Billing Statement/Statement of Account</li><li>• Delivery Receipt with printed name and signature of LANDBANK employee who received the delivery and actual date of receipt of items.</li></ul> <p>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.</p>	

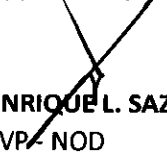
Prepared by:

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

Checked by:

  
**ARCHIEVAL B. TOLENTINO**  
ITM - LAN Team

Approved by:

  
**ENRIQUE L. SAZON JR.**  
VP - NOD

## RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

(ePLDT, INC.)

DATE	Aug. 22, 2023
PROJECT IDENTIFICATION NO.	ITB-GS-20230706-02
PROJECT NAME	<b>Three (3) Years Subscription for Email Cloud Advanced Threat Protection for 5000 user mailbox licenses</b>
PROPONENT UNIT/TECHNICAL WORKING GROUP	Network Operations Department

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS	LANDBANK's RESPONSES
58	The solution must have a cloud service Point Of Presence (POPs) in Asia Pacific region or locations for better performance and reliability. Must provide data sheet or website with the list of countries presence.	Since Fortinet's POPs are only located in Europe and US, is it ok to relax the specified APAC region.	No. We prefer that the solution must have POPs in Asia Pacific region to reduce latency and faster performance as much as possible end users.
65	The Bidder must have at-least two (2) installed base in the Philippines of the same brand and Email Advanced Persistent Threat (APT) Security solution being offered where 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).	<p>May we request to update this line item:</p> <p>From: The Bidder must have at-least two (2) installed base in the Philippines of the same brand and Email Advanced Persistent Threat (APT) Security solution being offered where 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).</p> <p>To: The bidder must have installed base of the same security brand/solution being offered where one (1) is a commercial or universal Philippine bank. Must submit a list of installed bases with</p>	<p>For revision:</p> <p><b>The Bidder must have at-least two (2) installed base in the Philippines of the same brand or any Email Advanced Persistent Threat (APT) Security solution, where 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).</b></p>

ANNEX G-1

		(client name, contact person, address, telephone number and email).	
--	--	---	--

ANNEX G-2

## RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

(First Data Corp)

<b>DATE</b>	Aug. 22, 2023
<b>PROJECT IDENTIFICATION NO.</b>	ITB-GS-20230706-02
<b>PROJECT NAME</b>	<b>Three (3) Years Subscription for Email Cloud Advanced Threat Protection for 5000 user mailbox licenses</b>
<b>PROPONENT UNIT/TECHNICAL WORKING GROUP</b>	Network Operations Department

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS	LANDBANK'S RESPONSES
		We would to inquire if the EAFS or AFS Electronic filing is acceptable?	Yes and it should be stamped "received" by the BIR or its duly accredited and authorized institutions
		For Ongoing and Private Contracts, do we need to attach the supporting documents? Or this can be submitted during the postqual activity?	No need to attached the supporting documents
60	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.	May we ask on what specific document is needed for this requirement?	Bidder/Supplier's notarized self-certification in reference to SEC registration document.
65	The Bidder must have at-least two (2) installed base in the Philippines of the same brand and Email Advanced Persistent Threat (APT) Security solution being offered where one (1) is a Commercial or Universal Philippine Bank. Must submit a list of installed	Under Technical Specification, Item #65, may we request if you can relax this requirement to any type of bank, either commercial or rural bank and if 1 installed solution will be consider?	No, since advanced email threat protection security solution is not new in the market. We prefer two (2) locally installed bases in which one (1) is a commercial or universal bank.

ANNEX 6-3



	person, address, telephone number and email).		
53	The vendor 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	<p>Under Technical Specification, Item #53/57, <i>The vendor 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.</i></p> <p><b>May we request to relax this item to:</b>  The vendor shall ensure that the cloud solution is available for 99.9% of the time during each calendar month, however if a Service Outage occurs, the vendor's technical team shall provide additional support for the troubleshooting and fix.</p>	No. Since it's a cloud subscription, the bank cannot afford to have a prolonged downtime on its email security due to continuous threat of phishing attacks.
57	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	<p>Under Technical Specification, Item #53/57, <i>The vendor 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.</i></p> <p><b>May we request to relax this item to:</b>  The vendor shall ensure that the cloud solution is available for 99.9% of the time during each calendar month, however if a Service Outage occurs, the vendor's technical team shall provide additional</p>	No. Since it's a cloud subscription, the bank cannot afford to have a prolonged downtime on its email security due to continuous threat of phishing attacks.

ANNEX G-4

		support for the troubleshooting and fix.	
		May we ask the exact time of bid opening?	The bid submission is rescheduled on September 8, 2023 at 10:00 AM.
		For required SLCC similar contract we would like to request if an IT software ONLY or hardware ONLY completed project will be consider?	IT Software or Hardware will be accepted, but it must be an Email APT Security Solution project only.
62	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: <ul style="list-style-type: none"> <li>• Certificate of employment (must have at least 3 years of work experience and have handled email cloud security products for at least a year)</li> <li>• Resume or Curriculum Vitae</li> <li>• List of Trainings and Seminars attended (including email cloud security related seminars)</li> </ul>	Under Tech Specs, on item 62, if the 2 engineers can be the same with the requirement of item 63, given that they can comply with the terms? Or is the requirement is for 4 unique engineers?	Two (2) local IT engineers from the bidders to support with the project (installation, configuration and troubleshooting).  Item 63 is more on a local TAC (Technical Assistance Center) if ever there's a need for an escalation.
		We would like to inquire your existing email security?	Cisco
71	Delivery upon receipt of NTP: 30 calendar days	Under Schedule of requirement, may we request if you can extend it to 45 calendar days upon receipt of NTP?	No, since this is a cloud based solution we expect that 30 day period is more than enough for the solution to be delivered.

ANNEX G-5