



**SUPPLEMENTAL/BID BULLETIN NO. 1**  
**For LBP-HOBAC-ITB-GS-20210210-01**

**PROJECT** : **Additional INTSIGHTS Credits and Takedown Services**  
**IMPLEMENTOR** : **Procurement Department**  
**DATE** : **July 16, 2021**

---

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 (Annex D), Technical Specifications (Section VII), and Checklist of Bidding Documents (Item No. 12 of the Eligibility and Technical Components) have been revised. Please see attached revised Annexes D-1 to D-3 and specific sections of the Bidding Documents.

  
**ALWIN I. REYES**  
Assistant Vice President  
Head, Procurement Department and  
HOBAC Secretariat

## Technical Specifications

<p style="text-align: center;"><b>Specifications</b></p>	<p style="text-align: center;"><b>Statement of Compliance</b></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 style="text-align: center;"><b>Additional INTSIGHTS Credits and Takedown Services</b></p> <p><b>1. Terms of Reference per attached Revised Annexes D-1 to D-3.</b></p> <p>2. The following documents shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements:</p> <p>2.1 Duly filled-out Terms of Reference signed in all pages by the authorized representative/s of the bidder.</p> <p>2.2 Notarized Certification with reference to Security and Exchange Commission (SEC) indicating that the bidder has at least five (5) years of existence in the IT Industry.</p> <p>2.3 Certification from distributor or principal as an authorized reseller</p>	<p style="text-align: center;"><b>Please state here either "Comply" or "Not Comply"</b></p>

<p>or distributor of the brand being offered.</p> <p>2.4 Certificate of Employment, Resume/Curriculum Vitae and List of Trainings and Seminars attended of at least three (3) local Technical Manager or Information Technology (IT) support engineers with at least five (5) years of work experience in handling the product being offered or other related security devices.</p> <p>2.5 Detailed escalation procedure and support including contact numbers and email addresses of local helpdesk that will provide 24/7 technical assistance.</p> <p>2.6 Certificate of Employment, Resume/Curriculum Vitae of Project Manager (PM) with at least five (5) years of work experience and handled at least one (1) Philippine Commercial of Universal Bank and one (1) non-bank client.</p> <p><b>2.7 List of at least two (2) installed bases in the Philippines of the product being offered wherein one (1) is a Universal or Commercial Philippine Bank (with client name, contact person, address, telephone number and email address). (Note: LANDBANK will sign a Non-Disclosure Agreement, if necessary).</b></p> <p>Non-submission of the above-mentioned documents/requirements may result in bidder's post-disqualification.</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); or all of the following:
  - Registration Certificate from Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for cooperatives, or any proof of such registration as stated in the Bidding Documents;
  - Valid and current mayor's/business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or equivalent document for Exclusive Economic Zones or Areas.

In cases of recently expired Mayor's/Business permits, it shall be accepted together with the official receipt as proof that the bidder has applied for renewal within the period prescribed by the concerned local government unit: Provided, That the renewed permit shall be submitted as a post-qualification requirement in accordance with Section 34.2 of this IRR; and

- Tax Clearance per Executive Order 398, Series of 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).

#### 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).

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

14. 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.
15. Latest Income Tax Return filed manually or through EFPS.
16. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
17. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

**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. Dully filled out Bill of Quantities Form signed by the Bidder's authorized representative (Annex E).

### Additional INTSIGHTS Credits and Takedown Services Term of Reference

Item No	Description	Comply (Yes/No)
1	The solution must provide additional 15,000 credit points which can be use for Investigation Services for threat intelligence research report, incident response, integration support services, Dark Web Purchases and UDRP (Uniform Domain Name Dispute Resolution Policy) Remediation / Takedown services.	
2	The solution must provide 100 takedown, takedown include fake mobile applications, phishing sites, fake social media sites and malicious domains.	
3	The solution must compatible to existing Cyber Threat Intelligence solution to provide an automated remediation service that enables the take down of malicious content published on the web covering the following:	
	a. Fraudulent social media pages impersonating the bank	
	b. Fake and/or suspicious mobile applications posing as a legitimate bank application	
	c. Pastes which contain sensitive data and/or any attack intention	
	d. Domains that were involved in phishing campaigns against the bank	
	e. Phishing websites posing as an official website of the bank	
	f. Files or any malicious items involved in phishing or malware attacks against the bank	
	g. Google search results leading to phishing websites and fraudulent activities	
	h. Personal information of the bank customers' executives	
4	The solution must have a dedicated team of takedown experts that would gather prerequisites, accelerate requests and streamline workflows to take down malicious campaigns as quickly as possible.	
5	The solution must continuously monitor code and fil sharing sites to identify exploits, sensitive data, or leaked credentials, and initiate removal requests	
6	The proposed solution must cover the following source sites which are available for takedown:	
	a. WHOIS records (phishing domains and phishing websites)	
	b. Social media networks (Facebook, LinkedIn, Twitter, and many more)	
	c. Mobile application stores	
	d. Online boxes and file sharing links used for malware distribution	
	e. Removal of Google search results due to copyright infringement	
	f. Personally Identifiable Information (PII) websites or malware attacks against the organization	
7	The proposed solution has the capability of providing remediation and alerts for paste sites that includes target list of employees and lists of credential leakages, including compromised employee emails and passwords.	
8	The proposed solution should be capable to automatically detect and remediate suspiciously registered domains that are similar to the bank assets.	
9	The proposed solution must be able to deliver alerts for websites using the bank names and graphics for malicious purposes.	
10	The proposed solution must be able to alert and remediate mobile and desktop applications coming from both official app stores and pirate app store that carry the bank brand or name but were uploaded without their knowledge and consent	
11	The proposed solution must provide a wide intelligence and remediation coverage for social media platforms and is capable of removing pages and profiles impersonating the banks legitimate pages and websites, as well as its executives.	
12	The proposed solution should have the capability of taking down files shared through different file sharing platforms.	

Revised Annex D-1

13	The proposed solution must be able to provide intelligence and remediation covering various PII (Personally Identifiable Information) websites.	
14	The proposed solution must be able to provide assistance in filing an Internet Corporation for Assigned Names and Numbers (ICANN) Uniform Domain-Name Dispute-Resolution Policy (UDRP) take down.	
15	The proposed solution is capable of providing research services that would help the bank take a deeper dives into external threat intelligence directly related to the bank or financial institution.	
16	The proposed solution must be able to go on the clear, deep & dark web in order to form a report as per the organization needs in order to provide with a better threat intelligence understanding such as:	
	a. Dark Web Hunting	
	b. Leaked Personally Identifiable Information (PII)	
	c. Information Related to VIP Exposure or Targeting	
	d. Threat Actor Profiling	
	e. Open Source Intellegence (OSINT)	
	f. Information Gathering	
	g. Sector or Vulnerability Research	
	h. Complex Threat Actor Analysis	
	i. Advanced Persistent Threat (APT) Research	
	j. New Technologies and Threats Profiling/Landscape	
17	The proposed solution must be an around the clock support any incidents by providing an in-depth review of the threats, help to assess and the magnitude of the attack, and help with performing the damage control for incidents such as a phishing attacks, malicious social media profiles, ransomware, data breaches and malware analysis.	
18	The proposed solution must be able to provide the required support for integrating with any of the bank's proprietary components, generation of unique customized reports as well as custom integrations or advanced automation capabilities.	
19	The proposed solution must be able to provide and start an investigation that can help the bank to counter the attack and/or to obtain more details on the identity of the attacker, malware, or fraud.	
20	The proposed solution is capable to provide research regarding a threat actor, fraud attempt, malware, breach or incident for which additional information is required.	
21	The proposed solution is capable to securely and anonymously purchase leaked databases, credit cards, and/or personally indentifiable information (PII) on the clear, deep and dark web.	
<b>Supplier's Eligibility Requirements</b>		
22	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.	
23	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.	
24	The principal represented by the supplier must have atleast three (3) local Technical manager or Information Technology (IT) support engineers to support the installations, configurations and 24x7 uptime services within the warranty period. Must submit Certificate of employment and Resume/Curriculum Vitae (that the local IT support engineers has at-least 5 years work experience in handling of the product being offered or other related security devices, include list of trainings and seminars attended)	
25	The supplier must have a local helpdesk to provide 24x7 technical assistance. Must	



	provide detailed escalation procedure and support including contact numbers and email addresses.	
26	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 5 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.)	
27	The supplier must have at-least two (2) installed base of same solution and one (1) complex technology like Application Programming Interface (API) Management, Security Information and Event Management (SIEM) wherein one (1) is a Universal or Commercial Philippine Bank. Must submit list of installed base with client name, contact person, address, telephone number and email address.	
<b>Other Requirements</b>		
28	The Winning Bidder must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank. 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>Delivery Terms and Conditions</b>		
29	Delivery after receipt of NTP: 60 days	