LANDBANK

BID BULLETIN NO. 1
For LBP-HOBAC-ITB-GS-20171116-01

PROJECT	:	**Three (3) Years Managed Detection and Response**
IMPLEMENTOR	:	**Procurement Department**
DATE	:	**January 24, 2018**

This Bid Bulletin is issued to modify, amend or clarify items in the Bid Documents. This shall form an integral part of the Bid Documents.

The modifications, amendments or clarifications are as follows:

- The Terms of Reference (Annex A), Section VII (Specifications) and Checklist of the Bidding Documents (Items 3.h & 6) have been revised. Please see attached revised Annexes A-1 to A-4 and the specified sections of the Bidding Documents.

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

Managed Detection and Response Technical Requirements

MD-CV Continous Vigilance or equivalent, Full Coverage 3Y from 5K to 9999	☐Yes ☐ No
PX MD Tech Enabler Bundle (HW) or equivalent , 3 years warranty	☐Yes ☐ No
4X1Gbps SFP ports, with 500 mbps max record speed	
PX MD Tech Enabler Bundle (HW) or equivalent, 3 years warranty	☐Yes ☐ No
4X10Gbps SFP+ ports, with 5Gbps max record speed	
2 HW-1000BaseT Tranceiver module - 1G copper or equivalent, 3 years warranty	☐Yes ☐ No
2 HW-10GBase-SR Transceiver module - 10G fiber SR or equivalent, 3 years warranty	☐Yes ☐ No
2 HW-1000BaseSX Tranceiver module - 1G fiber SX or equivalent, 3 years warranty	☐Yes ☐ No
1. The service must provide continuous compromise assessment and response using the existing advanced threat protection platforms of Land Bank to detect signs of intrusion early, rapidly investigate and provide the answers needed to respond effectively.	☐Yes ☐ No
2. The service must be able to leverage existing advanced threat protection solutions of Land Bank for the purpose of security monitoring.	☐Yes ☐ No
3. The service must be familiar with and be able to perform forensics/investigation using the existing Endpoint Detection & Response (EDR) solution of Land Bank	☐Yes ☐ No
4. The service must be familiar with and be able to perform forensics/investigation using the existing Network Forensics / Packet Capture solution of Land Bank	☐Yes ☐ No
5. The service must be able to perform forensics/investigation using 3rd party logs through SIEM or Threat Analytics solution	☐Yes ☐ No
6. The detection through response should occur within hours to drastically minimize the scope, impact, and cost of a breach.	☐Yes ☐ No
7. The service must be operated by competent personnel with a wide range of skill sets, including network and endpoint monitoring threat detection specialists, forensic experts, malware and intelligence analysts, and incident responders.	☐Yes ☐ No
8. The service must be operated with security and threat intelligence experts with strong capabilities in deep analysis and forensics of advanced cyber-threats, kill-chains and attack campaigns.	☐Yes ☐ No

Revised Annex A1

9. The service must be able to monitor for advanced threat protection security alerts, breaches, anomalies and advanced persistent threats, regardless of the number of nodes/users.	☐Yes ☐ No
10. The service must notify for critical security alerts, breaches, anomalies and advanced persistent threats, based on assessed severity and in real-time.	☐Yes ☐ No
11. The service must provide real-time, in-depth, contextual and non-trivial analysis of advanced and zero-day threats with highly actionable mitigation, to protect from APT attacks or determine if such attacks are currently occurring or have occurred in the past.	☐Yes ☐ No
12. The service must provide regular management reporting of detected, emerging threats, trends and actionable mitigation.	☐Yes ☐ No
13. When the investigation reveals a compromise, then within one (1) hour of the time the vendor makes that determination, the vendor should send a compromise report related to that activity.	☐Yes ☐ No
14. In addition to a summary, threat context and attacker details, the compromise report must also provide recommended actions and next steps.	☐Yes ☐ No
15. When a more comprehensive investigation is necessary, the service must be able to pivot into remote live response or onsite incident response seamlessly.	☐Yes ☐ No
16. The service must proactively hunt for signs and indicators of compromise, and pursue adversaries in the network and endpoints using advanced analytical techniques.	☐Yes ☐ No
17. The service must employ an arsenal of technologies and methodologies to investigate system artifacts, perform full-packet capture, conduct netflow analysis, reverse-engineer malware, and inspect emails to detect indicators of compromise.	☐Yes ☐ No
18. The service must be able to identify data that was stolen or offer insight into intellectual property that the attackers are targeting, where possible.	☐Yes ☐ No
19. The service must be able to automatically contain compromised devices with Land Bank's existing endpoint detection and response technology.	☐Yes ☐ No
20. The service must offer the ability to request for investigative actions outside the scope of normal service delivery actions. This ability must be able to acquire and analyze forensic artifacts, identify new host-based or network-based indicators, identify unknown malicious code, confirm lateral movement, identify compromised accounts, determine infection vectors and confirm attacker activity on enterprise systems.	☐Yes ☐ No
21. The vendor methodology must include forensic assessment of Land Bank's systems based on NBI (Network Based Indicators) as well as HBI (Host Based Indicators).	☐Yes ☐ No
22. Indicators of Compromise (IOCs) used by the vendor must have been derived from breach investigations at Financial Institutions of similar nature and scale, within APJ as well as the U.S. and EMEA.	☐Yes ☐ No

23. The vendor must have the capability to scale the forensic assessment to all Windows systems within the Bank.	☐Yes ☐ No
24. The vendor must have the capability to detect lateral movement by attackers on the internal network even if such lateral movement is purely internal and not visible on Internet egress link.	☐Yes ☐ No
25. The service must be complemented with real-time and correlated global threat intelligence network.	☐Yes ☐ No
26. The service must be able to distinguish between advanced threat actors who routinely evade commercial prevention tactics and the more opportunistic, nuisance threats.	☐Yes ☐ No
27. The service must have exceptional insight into threat actor tactics, modus operandi, and geo-political context gleaned from front-line incident response work. The service must also have the ability to foresee and predict attacker trends based on gathered intelligence.	☐Yes ☐ No
28. The service must provide personalized intelligence reports that offer insight into organization's risk profile, key findings, attacker profiles and motivations, and industry-specific intelligence.	☐Yes ☐ No
29. The vendor must have established track record in performing large scale cyber forensic investigations, specifically involving cyber criminals and nation-state attackers.	☐Yes ☐ No
30. The vendor must have deep intelligence of cyber threat actors especially those related to financial crimes.	☐Yes ☐ No
31. The service must offer an intelligence portal that contains at least 10 years worth of intelligence on financial and nation-state (APT) threat actors, as well as hacktivists and other cyber criminals.	
32. The service must offer a portal that is intuitive, user-friendly and allows an unlimited number of user accounts. The vendor should ensure the portal availability for 99.9% of the time during each calendar month.	☐Yes ☐ No
33. The service must offer a portal that allows analysis of suspicious domains and IP addresses, and also allows submission of suspicious files for an on-demand, automated analysis.	☐Yes ☐ No
34. The service must fulfill the role of a trusted advisor, engage in information sharing against advanced threat actors through regular contact, offer service performance feedback and reports, customized risk analyses and routine delivery of intelligence reports.	☐Yes ☐ No
35. The service must provide access to a trusted security advisor, who acts as the go-to security and incident response subject matter expert and specialist that handles all aspects of customer communication and service delivery.	☐Yes ☐ No
36. The service must offer community protection with industry experts who are constantly scanning for and reacting to the latest attacks, geopolitical triggers and cyber events across multiple countries and industries.	☐Yes ☐ No
37. The service must offer a daily analyst perspective on key media reports, which will allow Land Bank to make timely decisions on emerging global cyber incidents.	☐Yes ☐ No
38. The service must be available 24x7 using a follow-the-sun model for global coverage, with Security Operations Centers in the major geographies viz. Americas, Europe, Asia, Pacific and Japan.	☐Yes ☐ No

39.The service must monitor system health for the existing advanced threat protection solutions, including aspects like power supply and fan failure, RAID abnormalities, high system temperature and excessive disk space usage. The vendor should provide Customer with notifications of system health issues such as connectivity problems.	☐Yes ☐ No
Must be a certified Gold Partner of the Product represented. Must submit certification from the Product Principal	☐Yes ☐ No
Must have at-least 2 certified engineers of the Product offered. Must submit list of Certified Engineers	☐Yes ☐ No
Must have at-least 4 Anti-APT installed base of the Product Brand being offered where 1 is a Bank. Must submit list of installed base.	☐Yes ☐ No
Three (3) years warranty on hardware and software and must have a local helpdesk to provide 24x7 technical assistance. Warranty shall also cover any reconfiguration/integration after successful implementation. Submit warranty certificate and must provide detailed escalation procedure and support including contact numbers and email addresses.	☐Yes ☐ No
Must have a dedicated Project Manager to oversee the project. Must be included detailed escalation procedure and support.	☐Yes ☐ No

Specifications

Specifications	Statement of Compliance **Bidders must state below either "Comply" or "Not Comply" against each of the individual parameters of each specification.** Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid. 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 provisions of **ITB** Clause 3.1(a)(ii) and/or **GCC** Clause 2.1(a)(ii)
Three (3) Years Subscription of Managed Detection and Response **Minimum specifications and other requirements per attached Revised Terms of Reference (Revised Annexes A1 to A4).** The following documents shall be submitted inside the eligibility/technical envelope: ▪ **Duly filled-out Revised Terms of Reference signed in all pages by authorized representative/s.** ▪ Gold Partner Certification from the product principal for the offered item. ▪ List of at least two (2) certified engineers of the product being	**Please state here either "Comply" or "Not Comply"**

3.d Statement of the prospective bidder identifying its single largest completed contract similar to the contract to be bid, equivalent to at least fifty percent (50%) of the ABC supported with contract/purchase order, end-user's acceptance or official receipt(s) issued for the contract, within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the PBDs prescribed by the GPPB. (sample form - Form No. 4).

3.e 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.

3.f The prospective bidder's computation for its Net Financial Contracting Capacity (sample form - Form No. 5).

3.g 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 the legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance.

3.h Duly filled-out Revised Terms of Reference signed in all pages by authorized representative/s.

3.i Gold Partner Certification from the product principal for the offered item.

3.j List of at least two (2) certified engineers of the product being offered.

3.k Detailed escalation procedure with employment certificate of the project manager.

3.l List of at least four (4) Anti-APT installed bases of the product being offered where one (1) is a Bank.

4. Bid security in the prescribed form, amount and validity period (ITB Clause 18.1 of the Bid Data Sheet);

5. Schedule VI - Schedule of Requirements with signature of bidder's authorized representative.

6. Revised Section VII - Specifications with response on compliance and signature of bidder's authorized representative.