LANDBANK

BID BULLETIN NO. 3
For LBP-HOBAC-ITB-GS-20171116-01

PROJECT	:	**Three (3) Years Managed Detection and Response**
IMPLEMENTOR	:	**Procurement Department**
DATE	:	**February 8, 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 Revised Terms of Reference (Annex A) has been updated. Please see attached updated Annexes A1-A6 of the Bidding Documents.

- The deadline of submission and the schedule of opening of eligibility/technical and financial documents/proposals for the above project is re-scheduled to **February 15, 2018 11:00 A.M.** at the Procurement Department, 25th Floor, LANDBANK Plaza Building, 1598 M. H. Del Pilar corner Dr. Quintos Streets, Malate, Manila.

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

Managed Detection and Response
Technical Requirements

Hardware Description	Compliance	Compliance Validation - Site, Manual Name & Page, or URL
MD-CV Continuous 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 500mbps max record speed	☐Yes ☐ No	
PX MD Tech Enabler Bundle (HW) or equivalent, 3 years warranty	☐Yes ☐ No	
- 4x10Gbps SFP+ ports, with 5Gbps max record speed	☐Yes ☐ No	
2 HW-1000BaseT Transceiver 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 Transceiver module - 1G fiber SX or equivalent, 3 years warranty	☐Yes ☐ No	
Technical Description	**Compliance**	**Compliance Validation - Site, Manual Name & Page, or URL**
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	
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	

9

REVISED ANNEX A-1 (UPDATED)

Managed Detection and Response
Technical Requirements

Technical Description	Compliance	Compliance Validation - Site, Manual Name & Page, or URL
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	

REVISED ANNEX A-2 (UPDATED)

Managed Detection and Response
Technical Requirements

Technical Description	Compliance	Compliance Validation - Site, Manual Name & Page, or URL
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.	☐Yes ☐ No	
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	

REVISED ANNEX A-3 (UPDATED)

Managed Detection and Response
Technical Requirements

Technical Description	Compliance	Compliance Validation - Site, Manual Name & Page, or URL
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	☐Yes ☐ No	
Other Technical Requirements for Network Forensic Platform		
40. The above Network forensic platform must be utilized by the service provider to investigate activity or to hunt for network threats.	☐Yes ☐ No	
41. The Network Forensics Platform must support continuous, lossless packet capture with nanosecond time stamping	☐Yes ☐ No	
42. The Network Forensics Platform must suport real-time indexing of all captured packets with nanosecond time stamps and connection attributes provides data for immediate forensics	☐Yes ☐ No	
43. The Network Forensics Platform must support Ultrafast search and retrieval of target connections and packets using patentpending indexing architecture	☐Yes ☐ No	
44. The Network Forensics Platform must accelerate the investigative process by using Event Based Capture to identify suspicious sessions that should be the focus for deeper investigations.	☐Yes ☐ No	
45. The Network Forensics Platform must seamlessly be integrated with the customer portal that contains compromise reports	☐Yes ☐ No	
46. The PRINCIPAL (Manufacturer) represented by the BIDDER (Vendor/Partner) must have a multiple SOC's delivering MDR service capable of remote investigation and response 24x7x365	☐Yes ☐ No	
47. The PRINCIPAL (Manufacturer) represented by the Bidder (Vendor/Partner) must have at-least five years of experience as an MDR Service Provider. Must provide proof of documentation that the PRINCIPAL (Manufacturer) has been in the MDR business for at-least 5 years.	☐Yes ☐ No	

REVISED ANNEX A-4 (UPDATED)

Managed Detection and Response
Technical Requirements

Other requirements for MDR Service		
48. The bidder's MDR service MUST be able to remotely leverage Landbank's already existing Endpoint Detection and Response (EDR) solution (FireEye HX) for investigations and response.	☐Yes ☐ No	
49. The bidder's MDR service MUST be capable of remotely investigating forensic data across : Endpoint, Network, 3rd Party log	☐Yes ☐ No	
50. The PRINCIPAL (Manufacturer) represented by the Bidder (Vendor/Partner) MUST be listed as a representative vendor in Gartner's "Market Guide Detection and Response Services". The Bidder must be able to provide proof of documentation from Gartner	☐Yes ☐ No	
51. The PRINCIPAL (Manufacturer) represented by the Bidder (Vendor/Partner) must provide reputable IR services in addition to MDR services, and the IR services MUST use the same technology stack that the MDR services use	☐Yes ☐ No	
52. The PRINCIPAL (Manufacturer) represented by the Bidder (Vendor/Partner) must have a customer portal that contains compromise reports with the functionality to perform remote containment	☐Yes ☐ No	
53. The MDR service must have proven experience detecting zero-day exploits in the wild.	☐Yes ☐ No	
54. The MDR service must have an assigned trusted security advisor who will be the primary point of contact and will provide context on the threats that have been reported as well as provide recommendations to Landbank on how to increase their security posture. Their threat briefings must contain: - Current Engagement Status - Investigations / Reporting Q&A - Appliance & Device Health - News / Outstanding Items - Hunting statistics from previous month - Recent Intel on threat actors impacting the financial sector - Tales from the Trenches	☐Yes ☐ No	
54. The MDR service upon confirmation of the compromise report must answer: - What happened within Landbank's environment that prompted them to be notified? - What does other technology tell them about the activity? - What alerts, if any, did other appliances generate? - What other data, if any, did our investigative appliances log? - Did the event activity result in a compromise? - Why do they think the event is malicious or suspicious? - What they know about the threat actors associated with the event? - What is recommended to do about the activity?	☐Yes ☐ No	
55. The MDR service must provide access to an intel portal that contains detailed information on TTPs for advanced threat actors.	☐Yes ☐ No	

REVISED ANNEX A-5 (UPDATED)

Managed Detection and Response
Technical Requirements

Other requirements for MDR Service		
56. The MDR service must have a portal that allows interaction on reported threats between Landbank the MDR service provider.	☐Yes ☐ No	
57. The MDR service must have operational advanced SOCs in seven locations throughout the world, delivering 24 x 7.	☐Yes ☐ No	
58. The MDR service must have defined hunting techniques that are implemented using the capabilities from existing LANDBANK Anti-APT technologies	☐Yes ☐ No	
59. The MDR service must be able to provide attacker TTPs, threat attribution, and the initial infection vector (when available).	☐Yes ☐ No	
60. The MDR service must have an assigned service transition manager to oversee the onboarding of the FireEye technologies and will provide a project management schedule.	☐Yes ☐ No	
61. The MDR service must have security analysts with the following skillsets: - Working knowledge of network security architecture: how packets traverse a network, ability to assess security configurations of network devices - Working knowledge of Windows & UNIX security model: common vulnerabilities, ability to assess security configuration - Understanding of malware analysis - Understanding of the attack life-cycle and techniques used by the attacks	☐Yes ☐ No	
62. The MDR service must be able to report severity levels criteria.	☐Yes ☐ No	
Vendor Requirements	**Compliance**	**Compliance Validation - Site, Manual Name & Page, or URL**
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. All project documents to be submitted.	☐Yes ☐ No	

REVISED ANNEX A-6 (UPDATED)