SUPPLEMENTAL/BID BULLETIN NO. 2
For LBP-HOBAC-ITB-CS-20220802-01

PROJECT	:	**Supply, Delivery, Installation and Configuration of Network Detection and Response (NDR) Solution with Three (3) Years Support Services**
IMPLEMENTOR	:	**HOBAC Secretariat**
DATE	:	**October 06, 2022**

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 Responses to Bidders' Clarifications/Queries have been revised (Annexes G-1 to G-9).

3) The submission and opening of bids is re-scheduled on **October 14, 2022** at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams.

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

Project Identification Number	**LBP-HOBAC- ITB-GS-20220802-01**
Project Name	**Supply, Delivery, Installation and Configuration of Network Detection and Response (NDR) Solution with Three (3) Years Support Services**
Subject	**Response to Bidders' Queries**

Item No.	Details	Bidder Inquiry	LBP Response
131	Demonstrate ability to store detailed flow records for historical lookback	Question – is this compliance requesting for Netflow support and as requested in the RFP Netflow data should stay on-premises? Is that correct. Please elaborate	No. This does not require netflow. More like transaction records with metadata that can be search within the tool
136	Provide programmability NDR allowing for the real-time analysis of any custom protocol based on TCP or UDP. Examples may include extensibility to support: ISO8583, SCADA, NTP, Custom XML, etc.	Question- this is a metrics specific to network monitoring tools. Is the solution looking into OT networks such as SCADA? Also custom XML and programmability requested is a big risk and not recommended because that allowing such languages can lead to risks if these languages are not securely written for rules and allowing 3rd party or custom developer code such as javascripts can cause risks as anyone with access to NDR or with stolen admin credentials can write custom script and run it from the NDR system, which is highly unrecommended	Item removed in the TOR
137	Availability of NDR that can analyze traffic for real-time extraction of layer 2 to 7 and payload metrics, up to 100GBps continuous sustained throughput of analysis on a single appliance	Question - Is the network throughput in scope 100Gbps? If not, please indicate the actual throughput for each location in scope.	No. 10Gbps, but must be scalable since there will be an expected increase of throughput with the growing number of network traffic.
139	Physical Appliances should have a dedicated SSL/TLS decryption chipset to handle high volume processing of SSL traffic loads	Question - Is Landbank allowing private certificates to be stored on 3rd party NDR appliances? Also, are agents allowed to be installed with admin privileges on Landbank servers for decryption?	Yes. We can install certificate in the NDR appliance to monitor SSL traffic.

140	Must have a Perfect Forward Secrecy (PFS, mode of encryption whereby session keys are not negotiated over the wire (contrast with traditional RSA key exchange), solution must have some capabilities to perform real-time decryptions in a Perfect Forward Secrecy encrypted environment e.g. TLS 1.3 with Diffie-Hellman Key exchange.	Question - Is landbank allowing installation of agents on all the servers which need TLS 1.3 decryption?	Yes. We can allow the installation of an agent to decrypt for more visibility
141	PFS decryption technique must allow for both software key forwarder approach as well as Load Balancer integration techniques	Question - Is LandBank allowing Man in the middle approach of sending the keys for PFS decryption to 3rd party NDR solution?	No. Man-in the middle approach is not allowed. Should be done out of band
148	Provide real-time metrics for dashboarding, alerting, and historical reporting: '- TCP Connections, Aborts, Resets, Timeouts due to retransmissions, Zero Windows, Nagie's Delay, Out of Order packets L4 TCP Metrito' mentioned above must be retained for at least a month	Question - All the above are Network performance metrics and not security metrics. Kindly elaborate if these metrics are in optional as they will not assist risk or SOC team in any investigations	No. not an optional. We want this as an added features, this can be helpful in application and network troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.
153	Provide real-time metrics for dashboarding, alerting, and historical reporting: Record All GET/POST/PUT/HEAD transactions and their corresponding URIs, clients, and ser Er IP	Question – this is a Network performance metrics	Yes. As an added features, this can be helpful in application and network troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.
155	Monitor database protocols out of the box at Layer-7 (applicafon) level such as but not limited to: *Oracle *Microsoft SQL *MongiDB *DB2 *Sybase & SyBase IQ *REDIS *Postgres *Informix *MySQL Provide: real-time SQL statements, stats, errors and performance as relates to database traffic.	Question -What is the expectation from the above requirement as this is more towards DAM. Does Landbank already have a DAM and if so does it need this in NDR.	Yes, the bank has an existing one but the DAM license is limited to a number of databases. Having this feature will add more visibility on the database traffic so that the team can check any abnormalities or help in threat hunting against database attacks.

160	Real-time metrics for dashboarding, alerting, and historical reporting of SMTP and POP3 traffic such as sender/recipient addresses, processing time, errors, SMTP/POP3 response/status codes. Email Metrics must be retained for at least a month	Question -Above are network performance metrics. Is Landbank looking at Email security solution?	No. But as long as the product can comply with real-time dashboarding and alerting using SMTP/POP3
163	Real-time metrics for dashboarding, alertirg, and historical reporting of protocols such as: -Extensive Markup Language (XML) -Simple Object Access Protocol (SOAP) -Apache Jserv Protocol (AJP)	Question - Is Landbank looking for Network performance metrics or application security metrics from the above protocol and if so then this will be best addressed by a SAST or a DAST solution	Yes. As an added feature, this can be helpful in application troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.

Item No.	Details	Bidder Inquiry	LBP Response
7	Capability for a single virtual appliance to monitor up to 10 Gbps of real-time traffic and 200 GB daily of packet capture storage.	Can Landbank please confirm that by "200GB daily of packet capture storage" they are referring to network transaction metadata (such as stored by ExtraHop Reveal(x) 360)?	Included in the revised TOR per bid bulletin no. 1. Capability to support virtual and/or physical appliances that range from 1Gbps to 100Gbps in a single virtual/physical form factor
32	The proposed solution should be able to store the raw packets for more than 3 months;	Is Landbank referring to storing continuous raw PCAP collection for over 3 months? At 10Gbps sustained this equates to 108TB per day of storage for full packet capture (PCAP).	Included in the revised TOR per bid bulletin no. 1. The proposed solution should be able to store the network transaction to support forensics investigations with purpose built hardware and expansion storage.
40	Proposed solution should have the option to include 24/7 MDR (Managed Detection and Response) service delivered by the solution provider.	May we add this as an optional item in the proposal? (note that the question says "should have the option")	Yes. This is an optional requirement for future deployment/integration.
75	The proposed solution should not store any data in any cloud rather all the data should be stored on-premises	ExtraHop Reveal(x) 360 utilizes cloud based Cloud Record Store for network transaction metadata. Reveal(x) Enterprise can be deployed to use on-premise record datastore.	Network Transaction Metadata is acceptable.
97	The proposed solution should be able to work in air-gapped	Why does Landbank require an air-gapped solution? ExtraHop	Item removed in the TOR.

	environment without depending on the external network connectivity and should not send any data outside the customer data center	can be deployed in air-gapped environment with reduced functionality.	
98	The proposed solution should have on-box machine learning and should not be dependent on machine learning on the cloud	Why does Landbank want to be restricted by the limits of on-board machine learning with limited datasets that can be processed? ExtraHop is not limited to restricted on-box ML capabilities - ExtraHop uses cloud-scale ML services to ensure the best possible threat and anomaly detection	Included in the revised TOR per bid bulletin no. 1. The proposed solution should have a machine learning capability in the cloud.
100	The proposed solution must store detections and PCAP's on box for a period of no less than 3 months	Is Landbank referring to detection data and supporting metadata needed to support investigations? Detections and related metadata are stored for 3 months. If needed, the EDA can use extended Data Store for longer metrics and detection retention	Yes. To support forensic investigation.
134	Proposed solution must allow the capability for human analysts to perform an unbiased analysis and identify improvement areas in the IT infrastructure. Deliverables include periodic (e.g. monthly, quarterly) reports with specific security findings and recommendations.	May we add this as an optional item in the proposal? This overlaps with item 40 MDR services	Yes. Can be added as an optional requirement for support analysis, can be an added service provided by an NDR vendor to check and help with the bank security posture.
170	The solution must be capable of integrating with endpoint and identity solutions such as Active Directory to increase host coverage in remote work scenarios and support an identity focused, Zero Trust security strategy.	May we request for additional information or use cases for the integration with endpoint and identity solutions?	This is to help track Active Directory activity.
	The solution must integrate with threat intelligence feeds (commercial, industry specific or internal)	Will the integration be used to derive user information from parsed network traffic?	Yes. Integration to Intelligence feed as other data sources.
173	Deduplication of data should happen at the sensors and also in-addition at the centralized management appliance	Deduplication of what data? ExtraHop sensors perform native deduplication packets collected in the datafeed.	Deduplication of packet data

178	The solution must have a strong integration with Active Directory and allow for either a manual or automated disabling, lockdown of accounts in the platform's UI.	What is the desired functionality for this integration?	This is to help track Active Directory activity. And prevent AD attacks.
180	The solution must have native, UI or API based response capability with leading NGFW, please explain how the solution can respond? i.e., block via global blacklist	Does industry standard format include CEF or LEEF?	Yes. CEF is acceptable

Item No.	Details	Bidder's Inquiry	LBP Response
32	The proposed solution should be able to store the raw packets for more than 3 months;	Requesting to change to "Network Transaction record" instead because storing a "raw packet" for three months would need 10 Petabyte storage	Included in the revised TOR per bid bulletin no. 1. The proposed solution should be able to store the network transaction to support forensics investigations with purpose built hardware and expansion storage.
94	The solution must only start collecting PCAPs once behavior of interest is triggered	Please elaborate and clarify the second sentence OR can just **delete** this portion.	Item removed in the TOR
97	The proposed solution should be able to work in air-gapped environment without depending on the external network connectivity and should not send any data outside the customer data center	Requesting to delete as this would cap the efficiency of the technology. The technology itself would be more efficient with their cloud intelligence database and would be beneficial to the bank to maximize the technology.	Item removed in the TOR
98	The proposed solution should have on-box machine learning and should not be dependent on machine learning on the cloud	Requesting to delete as this would cap the efficiency of the technology. The technology itself would be more efficient with their cloud intelligence database and would be beneficial to the bank to maximize the technology.	We revise the item instead of deletion. Included in the revised TOR per bid bulletin no. 1. The proposed solution should have a machine learning capabilities in the cloud.
186	Manufacturer Certification as the Gold Partner	Would like to request to change to Authorized Partner	Included in the revised TOR per bid bulletin no. 1. The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.

190	The Bidder must have at-least two (2) installed bases in the Philippines of the same brand and model being offered where one (1) is a Commercial or Universal Philippine Bank. Must submit a list of installed base with (client name, contact person, address, telephone number and email).	Requesting that the installed base would be for only ONE (1) from the Commercial or Universal Bank in the Philippines	Included in the revised TOR per bid bulletin no. 1. The supplier must have of at least one (1) installed base of the same brand being offered in a Philippine commercial or universal bank. Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed.

Item No.	Details	Bidder Inquiry	LBP Response
164	Some of the compliances are more for network performance such as VOIP, MOS score, which are not related to security	Not Related to Security	Yes this is not related to security. However, the features are still can be beneficial to the team in terms of monitoring and troubleshooting.
55	Regarding database detection and response, does Landbank have any DAM (Database Activity Monitoring) solution, so is database visibility optional.	NDR solutions even if they detect database anomalies, they do not act on it and provide	Yes, but current DAM licenses are limited to a number of databases. Having this feature will add more visibility on the database traffic so that the team can check any abnormalities or help in threat hunting against database attacks.
132	Demonstrate ability to create custom record format include custom application data record -	this is more of Network performance metrics	This is to help facilitate more advanced threat hunting use cases.
	Is industry standard Bro, Zeek, Surricata, Snort for custom rules OK? or are you looking at complex languages such as JavaScript's or Ruby for custom rules (please note that allowing such languages can lead to risks if these languages are not securely written for rules and allowing 3rd party or custom developer code such as javascripts can cause risks as anyone with access to NDR or with stolen admin credentials can write custom script and run it from the NDR system, which is highly unrecommended)		Yes. And as long as the log format can be supported by the bank current SIEM

131	Demonstrate ability to store detailed flow records for historical lookback	Question – is this compliance requesting for Netflow support and as requested in the RFP Netflow data should stay on-premises? Is that correct. Please elaborate	No. This does not require netflow specially. More like transaction records with metadata that can be search within the tool.
136	14. Provide programmability NDR allowing for the real-time analysis of any custom protocol based on TCP or UDP. Examples may include extensibility to support: ISO8583, SCADA, NTP, Custom XML, etc.	Question- this is a metrics specific to network monitoring tools. Is the solution looking into OT networks such as SCADA ? Also custom XML and programmability requested is a big risk and not recommended because that allowing such languages can lead to risks if these languages are not securely written for rules and allowing 3rd party or custom developer code such as javascripts can cause risks as anyone with access to NDR or with stolen admin credentials can write custom script and run it from the NDR system, which is highly unrecommended	Item removed in the TOR
137	Availability of NDR that can analyze traffic for real-time extraction of layer 2 to 7 and payload metrics, up to 100GBps continuous sustained throughput of analysis on a single appliance	Question - Is the network throughput in scope 100Gbps? If not, please indicate the actual throughput for each location in scope.	No. 10G, but must be scalable since there will be an expected increase of throughput with the growing number of network traffic.
139	Physical Appliances should have a dedicated SSL/TLS decryption chipset to handle high volume processing of SSL traffic loads	Question - Is Landbank allowing private certificates to be stored on 3rd party NDR appliances ? Also, are agents allowed to be installed with admin privileges on Landbank servers for decryption?	Yes. We can install certificate in the NDR appliance to monitor SSL traffic.
140	Must have a Perfect Forward Secrecy (PFS, mode of encryption whereby session keys are not negotiated over the wire (contrast with traditional RSA key exchange), solution must have some capabilities to perform real-time decryptions in a Perfect Forward Secrecy encrypted environment e.g. TLS 1.3 with Diffie-Hellman Key exchange.	Question - Is landbank allowing installation of agents on all the servers which needs TLS 1.3 decryption?	Yes. We can allow the installation of an agent to decrypt for more visibility

141	PFS decryption technique must allow for both software key forwarder approach as well as Load Balancer integration techniques	Question - Is LandBank allowing Man in the middle approach of sending the keys for PFS decryption to 3rd party NDR solution?	No. Man-in the middle approach is not allowed. Should be done out of band.
148	Provide real-time metrics for dashboarding, alerting, and historical reporting: '- TCP Connections, Aborts, Resets, Timeouts due to retransmissions, Zero Windows, Nagie's Delay, Out of Order packets L4 TCP Metrito' mentioned above must be retained for at least a month	Question - All the above are Network performance metrics and not security metrics. Kindly elaborate if these metrics are in optional as they will not assist risk or SOC team in any investigations	No not an optional. We want this as an added features, this can be helpful in application and network troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.
153	Provide real-time metrics for dashboarding, alerting, and historical reporting: Record All GET/POST/PUT/HEAD transactions and their corresponding URIs, clients, and ser Er IP	Question – this is a Network performance metrics	Yes. As an added features, this can be helpful in application and network troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.
155	Monitor database protocols out of the box at Layer-7 (applicafon) level such as but not limited to: *Oracle *Microsoft SQL *MongiDB *DB2 *Sybase & SyBase IQ *REDIS *Postgres *Informix *MySQL Provide: real-time SQL statements, stats, errors and performance as relates to database traffic.	Question -What is the expectation from the above requirement as this is more towards DAM. Does Landbank already have a DAM and if so does it need this in NDR.	Yes, the bank has an existing one but the DAM licenses are limited to a number of databases. Having this feature will add more visibility on the database traffic so that the team can check any abnormalities or help in threat hunting against database attacks.
160	Real-time metrics for dashboarding, alerting, and historical reporting of SMTP and POP3 traffic such as sender/recipient addresses, processing time, errors, SMTP/POP3 response/status codes. - Email Metrics must be retained for at least a month	Question -Above are network performance metrics. Is Landbank looking at Email security solution?	No. But as long as the product can comply with real-time dashboarding and alerting using SMTP/POP3
163	Real-time metrics for dashboarding, alertirg, and historical reporting of protocols such as : -Extensive Markup Language (XML) -Simple Object Access Protocol	Question - Is Landbank looking for Network performance metrics or application security metrics from the above protocol and if so then this will be best addressed by a SAST or a DAST solution	Yes. As an added features this can be helpful in application troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.

	(SOAP) -Apache Jserv Protocol (AJP)		

Bidder's Inquiry	LBP Response
How many locations?	Head Office
Any cloud VPC in scope?	On the pipeline
What EDR are you using?	Must support leading EDR brand
What SIEM are you using?	Must support leading SIEM brand
What Firewall are you using?	Must support leading Firewall brand
What is the throughput of each location in scope?	10G
How many users, servers IP in the scope?	15,000++