LBP LEASING AND FINANCE CORPORATION
(A LANDBANK Subsidiary)
15th Floor SycipLaw Centre Bldg, #105 Paseo de Roxas St. 1226 Makati City
Telephone Number 8818-2200/ Fax Number 819-6176

INVITATION TO QUOTE FOR RENEWAL AND UPGRADE OF ENDPOINT SECURITY LICENSE SUBSCRIPTION

(LLFC-CAP-23-015)

REQUEST FOR QUOTATION (Small Value Procurement)

LBP Leasing and Finance Corporation (LLFC) through its Bids and Awards Committee (BAC) will undertake a Small Value Procurement in accordance with Section 53.9 of the 2016 Revised Implementing Rules and Regulations of the Republic Act No. 9184.

Name of the Project	**Renewal and Upgrade of Endpoint Security License Subscription (LLFC-CAP-23-015)**
Approved Budget of the Contract (ABC)	**Five Hundred Thousand Pesos and 00/100 (PHP 500,000.00)**

BACKGROUND

LBP Leasing and Finance Corporation's existing endpoint security license subscription will expire on September 25, 2023 thus renewal is necessary for continuous updates of the application databases, continuous protection of the endpoints and to continue virus scan tasks.

OBJECTIVES OF THE PROCUREMENT

The objective of subscription renewal and upgrade of Endpoint Security Licenses is to provide comprehensive visibility across all endpoints on the Corporation's network.

SCOPE OF WORK

QUANTITY AND SUBSCRIPTION PERIOD	▪ 100 units Renewal and Upgrade from Endpoint Security Business Select to Endpoint Detection and Response – Optimum for 2 Years (September 25, 2023 to September 24, 2025) ▪ 30 units Additional Endpoint Security with Detection and Response-Optimum for 2 Years (September 25, 2023 to September 24, 2025)
BASIC SECURITY FEATURE SET	▪ File, Web, Mail Threat Protection, Firewall ▪ Behavior Detection, Exploit Prevention and Remediation ▪ Web, Device, and Application Control for desktop ▪ Vulnerability Scan
EXTENDED SECURITY FEATURE SET	• SIEM Integration • Encryption Management • Adaptive Anomalies Control • Patch Management and Systems Management • Application Control for Server
EDR FEATURE SET	• Visibility across all endpoints • Root Cause Analysis/ Attack chain visualization • Centralized IOC search • Incident response action
ARCHITECTURE AND DESIGN	▪ The suggested solution must support integration with a free of charge threat intelligence portal, which contains and displays information about the reputation of files and URLs. ▪ The suggested solution must support integration with cloud reputation service.

	▪ The suggested solution must support central management and analytics through on-prem Web console and cloud management console. (Incident related data, System status and health check data, Settings, etc.) ▪ EDR agents must have integration with Endpoint Protection applications. ▪ EDR and Endpoint Protection solutions must have unified console for administrators and analysts ▪ EDR should support standalone agent installation (without Endpoint Protection application). ▪ Hardware platform where the solution is installed should be flexible for any upgrade include network interfaces, RAM and CPU
DETECTION	▪ The suggested solution must supplement verdict information from the Endpoint Protection solution with system artifacts about the detection. ▪ The suggested solution must support auto generation of threat indicators (IoC) after detection occurs with ability to apply response action. ▪ The solution must have the capability to force an IoC scan across all endpoints with installed EDR agents. ▪ The suggested solution must support IoC scanning run according to a scheduler. ▪ The suggested solution must support import of third-party IoC in OpenIoC format for its use in network scanning. ▪ The suggested solution must support scanning using auto generated, uploaded or external (third party) IoC's to detect earlier undetected threats. ▪ The suggested solution must support exporting of IoC generated by the solution to a file in OpenIoC format.
VISIBILITY	▪ The suggested solution must generate detailed incident cards related to the detected threat on an endpoint. ▪ An incident card must include at least the following information about detected threat: - Threat development chain graph (kill chain). - Information about the device on which the threat is detected (name, IP address, MACaddress, user list, operating system). - General information about the detection, including detection mode. - Registry changes associated with the detection. - History of the file presence on the device. - Response actions performed by the application. ▪ Threat development chain (kill chain) graphs must provide visual information about the objects involved in the incident, for example, about key processes on the device, network connections, libraries, registry, etc. ▪ An incident card must present detailed view on system artifacts and incident-related data for root cause analysis: - Process spawning - Network connections - Registry changes - Downloading object - Dropped objects, etc.
RESPONSE	▪ The suggested solution must support ‘Single-click” response form management console ▪ The suggested solution must support at least the following response actions that an administrator can perform when threats are detected: **a.** Prevent object execution - EDR solution must support both modes:records to the events about attempts to launch objects or open documents that meet the criteria of the Execution prevention, but does not block launch or opening these objects.Blocks launch of the objects or opening the documents that meet criteria of the Execution prevention rules. - EDR solutions must support blocking objects by hash (MD5 or SHA256) or by path pattern. - EDR solution must support blocking executables, scripts and documents - EDR solution must support notification user about prevention option **b**. Host isolation.

	- EDR solutions must provide means of isolating machines from the rest of the network in case of a security incident, while preserving controlled communication with agents' administration and management servers. - EDR solution must support creating custom host isolation rules (i.e. adding particular network resources to exclusion e.g. DNS or selecting predefined profiles) - EDR solution must support manual bringing the host back online from isolation. **c.** Terminate a process on the device. **d.** Quarantine an object - The suggested solution must support object recovery from quarantine. **e.** Run system scan **g.** Remote program / process / command execution **h.** Start IoC scan for a group of hosts.
ADMINISTRATION AND REPORTING	▪ The solution must have a unified policies, centralized reporting and tasks execution within a Single-console for centralized management – on-prem or cloud based. ▪ Suggested solution management server must have ability to send logs to SIEM, SYSLOG servers ▪ The solution must have different administrator functions that have a single interface/dashboard during sign on and controlled by privileges and rights based on their functions (Administrator, Reviewer, Investigator, etc.). ▪ The suggested solution must support secure communication between management console and endpoints with EDR agent ▪ The suggested solution must support management of EDR agent through command line interface ▪ Suggested solution must have an inbuilt feature/module to collect the data required for troubleshooting, without requiring a physical access to the endpoint. ▪ EDR agents must have a self-defense mechanism to prevent agent modifying agent-related files/system components entries etc. ▪ The solution must allow the creation of accounts with different roles used to administer the solution, just monitor the alerts, or review changes ▪ Administration server upgrade must not require installation from scratch and losing settings, etc. ▪ The solution should be able to send email notifications when certain types of security alerts are generated. ▪ The solution must support backup and restore the solution configuration. ▪ The solution should be simple to install and operate, and not require high-level skills from IT/Information Security staff ▪ The solution should provide minimal impact on existing IT/Information Security staff load ▪ The solution should be able to work in autonomous mode without access to external threat intelligence sources ▪ Requirements for the solution documentation. A documentation for EDR software, including administration tools, should include at least online help for Administrators
ADDITIONAL FEATURES	▪ The suggested solution must support integration with Sandbox with ability to automatically scan endpoints and apply responses in case if suspicious activity has been detected by the Sandbox. ▪ The suggested solution must support integration with the APT solution. ▪ The suggested solution must support integration with Managed Detection and Response service. ▪ The suggested solution must support automated detection of malicious activity using Endpoint Protection solution and Sandbox.
TECHNOLOGY REPUTATION	▪ Quality technologies that are constantly proven by independent testing laboratories year by year including specific tests certification on advanced threats and performance. ▪ Have perfect scores on protection, performance, and usability TEST for business users for at least two (2) years prior to the current year.

MAINTENANCE AND SUPPORT	▪ Have a reputable local vendor representative in the Philippines that has been active in cybersecurity trade for at least 10 years now. ▪ Supplier of the solution have at least two (2) certified engineers for end-point solution ▪ Able to provide 3-Tier support (1st local, 2nd Distributor and 3rd Principal) ▪ Provides regular call or email check-up for concerns and product health monitoring even after sales. ▪ Available support through phone, email, web-remote assistance and on-site/on-call support. ▪ The solution must be able to provide comprehensive after-sales agreement options ▪ Conducts quarterly preventive maintenance for endpoint protection ▪ Regular daily pattern updates and firmware upgrade in co-term with the years of subscription ▪ Includes installation and configuration ▪ Includes Knowledge Transfer with completion and configuration report. Onsite conducted by Certified Professional Engineer for product served ▪ Includes vulnerability assessment for one (1) server on quarterly basis for Windows/Linux operating system.

1. Please accomplish the following:
   a.) Price Quotation Form (Annex "A") together with the supplier's official proposal/quotation
   b.) Statement of Compliance under Schedule of Requirements and Technical Specifications (Annex "B")

   Submit in a sealed envelope to LBP Leasing and Finance Corporation office located at 15th Floor, SyCip Law Centre Bldg, #105 Paseo de Roxas St., Makati City **on or before September 12, 2023 04:00PM** together with the **Certified True Copies** of the following **Eligibility documents**:

   a.) Valid and current year Mayor's Permit
   b.) Valid and current PhilGEPS Registration Number
   c.) DTI/SEC Registration (for Partnership/Corporation)
   d.) Notarized Secretary's Certificate for proof of authorization

2. All quotations must include all applicable taxes and shall be valid for a period of thirty (30) calendar days from the deadline of submission of quotations. Quotations received in excess of the approved budget shall be automatically rejected.

3. Liquidated damages equivalent to one tenth (1/10) of the one percent (1%) of the value of Purchase Order not completed within the prescribed completion period shall be imposed per day to day of delay. LLFC may rescind the agreement once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of purchase order, without prejudice to other courses of action and remedies open to it.

4. The project shall be awarded to the proponent determined to have submitted the complete and lowest quotation including compliance with the Schedule of Requirements and Eligibility documents.

5. The prospective bidder shall be a Filipino citizen/sole proprietorship/partnership/Corporation duly organized under the laws of the Philippines.

6. LLFC reserves the right to reject any or all quotations at any time prior to award of the project without thereby incurring any liability to the affected proponents and to waive any minor defects therein to accept the quotation as may be considered more advantageous to the Government.

7. Payment shall be within thirty (30) calendar days from date of acceptance. The procurement of LLFC is subject to a final VAT withholding of five percent (5%) in addition to the applicable withholding tax.

For further information, please visit LBP Leasing and Finance Corporation office or contact the BAC Secretariat Ms. Jose Emmanuel I. Guerrero at telephone number 8818-2200 loc. 231 or send e-mail to procurement@lbpleasing.com

Date of issue: 08 September 2023

(Sgd.)
MS. RIZA M. HERNANDEZ
CHAIRPERSON
BIDS AND AWARDS COMMITTEE

TERMS OF REFERENCE
FOR LBP LEASING AND FINANCE CORPORATION

PROJECT NAME	**:**	**Renewal and Upgrade of Endpoint Security License Subscription**
APPROVED BUDGET FOR THE CONTRACT	**:**	**Five Hundred Thousand Pesos (Php 500,000.00) inclusive of all applicable taxes**
MODE OF PROCUREMENT	**:**	**Small Value Procurement**

I. SUMMARY

Endpoint security (antivirus) protection refers to securing endpoints such as laptops, desktops, servers and mobile devices, from cybersecurity threats. Endpoints can create entry points to organization's networks which cybercriminals can exploit. Endpoint security protects these entry points from malicious attacks.

II. BACKGROUND

The Corporation's existing endpoint security license subscription will expire on September 25, 2023 thus renewal is necessary for continuous updates of the application databases, continuous protection of the endpoints and to continue virus scan tasks.

III. OBJECTIVES

The objective of this subscription renewal and upgrade is to continuously and further provide comprehensive visibility across all endpoints on the Corporation's network.

IV. SCOPE OF WORK

QUANTITY AND SUBSCRIPTION PERIOD	▪ 100 units Renewal and Upgrade from Endpoint Security Business Select to Endpoint Detection and Response – Optimum for 2 Years (September 25, 2023 to September 24, 2025) ▪ 30 units Additional Endpoint Security with Detection and Response- Optimum for 2 Years (September 25, 2023 to September 24, 2025)
BASIC SECURITY FEATURE SET	▪ File, Web, Mail Threat Protection, Firewall ▪ Behavior Detection, Exploit Prevention and Remediation ▪ Web, Device, and Application Control for desktop ▪ Vulnerability Scan
EXTENDED SECURITY FEATURE SET	• SIEM Integration • Encryption Management • Adaptive Anomalies Control • Patch Management and Systems Management • Application Control for Server
EDR FEATURE SET	• Visibility across all endpoints • Root Cause Analysis/ Attack chain visualization • Centralized IOC search • Incident response action
ARCHITECTURE AND DESIGN	▪ The suggested solution must support integration with a free of charge threat intelligence portal, which contains and displays information about the reputation of files and URLs. ▪ The suggested solution must support integration with cloud reputation service.

	▪ The suggested solution must support central management and analytics through on-prem Web console and cloud management console. (Incident related data, System status and health check data, Settings, etc.) ▪ EDR agents must have integration with Endpoint Protection applications. ▪ EDR and Endpoint Protection solutions must have unified console for administrators and analysts ▪ EDR should support standalone agent installation (without Endpoint Protection application). ▪ Hardware platform where the solution is installed should be flexible for any upgrade include network interfaces, RAM and CPU
DETECTION	▪ The suggested solution must supplement verdict information from the Endpoint Protection solution with system artifacts about the detection. ▪ The suggested solution must support auto generation of threat indicators (IoC) after detection occurs with ability to apply response action. ▪ The solution must have the capability to force an IoC scan across all endpoints with installed EDR agents. ▪ The suggested solution must support IoC scanning run according to a scheduler. ▪ The suggested solution must support import of third-party IoC in OpenIoC format for its use in network scanning. ▪ The suggested solution must support scanning using auto generated, uploaded or external (third party) IoC's to detect earlier undetected threats. ▪ The suggested solution must support exporting of IoC generated by the solution to a file in OpenIoC format.
VISIBILITY	▪ The suggested solution must generate detailed incident cards related to the detected threat on an endpoint. ▪ An incident card must include at least the following information about detected threat: - Threat development chain graph (kill chain). - Information about the device on which the threat is detected (name, IP address, MACaddress, user list, operating system). - General information about the detection, including detection mode. - Registry changes associated with the detection. - History of the file presence on the device. - Response actions performed by the application. ▪ Threat development chain (kill chain) graphs must provide visual information about the objects involved in the incident, for example, about key processes on the device, network connections, libraries, registry, etc. ▪ An incident card must present detailed view on system artifacts and incident-related data for root cause analysis: - Process spawning - Network connections - Registry changes - Downloading object - Dropped objects, etc.
RESPONSE	▪ The suggested solution must support ‘Single-click” response form management console ▪ The suggested solution must support at least the following response actions that an administrator can perform when threats are detected: **a.** Prevent object execution

	- EDR solution must support both modes:records to the events about attempts to launch objects or open documents that meet the criteria of the Execution prevention, but does not block launch or opening these objects.Blocks launch of the objects or opening the documents that meet criteria of the Execution prevention rules. - EDR solutions must support blocking objects by hash (MD5 or SHA256) or by path pattern. - EDR solution must support blocking executables, scripts and documents - EDR solution must support notification user about prevention option **b**. Host isolation. - EDR solutions must provide means of isolating machines from the rest of the network in case of a security incident, while preserving controlled communication with agents' administration and management servers. - EDR solution must support creating custom host isolation rules (i.e. adding particular network resources to exclusion e.g. DNS or selecting predefined profiles) - EDR solution must support manual bringing the host back online from isolation. **c.** Terminate a process on the device. **d.** Quarantine an object - The suggested solution must support object recovery from quarantine. **e.** Run system scan **g.** Remote program / process / command execution **h.** Start IoC scan for a group of hosts.
ADMINISTRATION AND REPORTING	▪ The solution must have a unified policies, centralized reporting and tasks execution within a Single-console for centralized management – on-prem or cloud based. ▪ Suggested solution management server must have ability to send logs to SIEM, SYSLOG servers ▪ The solution must have different administrator functions that have a single interface/dashboard during sign on and controlled by privileges and rights based on their functions (Administrator, Reviewer, Investigator, etc.). ▪ The suggested solution must support secure communication between management console and endpoints with EDR agent ▪ The suggested solution must support management of EDR agent through command line interface ▪ Suggested solution must have an inbuilt feature/module to collect the data required for troubleshooting, without requiring a physical access to the endpoint. ▪ EDR agents must have a self-defense mechanism to prevent agent modifying agent-related files/system components entries etc. ▪ The solution must allow the creation of accounts with different roles used to administer the solution, just monitor the alerts, or review changes ▪ Administration server upgrade must not require installation from scratch and losing settings, etc. ▪ The solution should be able to send email notifications when certain types of security alerts are generated. ▪ The solution must support backup and restore the solution configuration. ▪ The solution should be simple to install and operate, and not require high-level skills from IT/Information Security staff ▪ The solution should provide minimal impact on existing IT/Information Security staff load

	▪ The solution should be able to work in autonomous mode without access to external threat intelligence sources ▪ Requirements for the solution documentation. A documentation for EDR software, including administration tools, should include at least online help for Administrators
ADDITIONAL FEATURES	▪ The suggested solution must support integration with Sandbox with ability to automatically scan endpoints and apply responses in case if suspicious activity has been detected by the Sandbox. ▪ The suggested solution must support integration with the APT solution. ▪ The suggested solution must support integration with Managed Detection and Response service. ▪ The suggested solution must support automated detection of malicious activity using Endpoint Protection solution and Sandbox.
TECHNOLOGY REPUTATION	▪ Quality technologies that are constantly proven by independent testing laboratories year by year including specific tests certification on advanced threats and performance. ▪ Have perfect scores on protection, performance, and usability TEST for business users for at least two (2) years prior to the current year.
MAINTENANCE AND SUPPORT	▪ Have a reputable local vendor representative in the Philippines that has been active in cybersecurity trade for at least 10 years now. ▪ Supplier of the solution have at least two (2) certified engineers for end-point solution ▪ Able to provide 3-Tier support (1st local, 2nd Distributor and 3rd Principal) ▪ Provides regular call or email check-up for concerns and product health monitoring even after sales. ▪ Available support through phone, email, web-remote assistance and on-site/on-call support. ▪ The solution must be able to provide comprehensive after-sales agreement options ▪ Conducts quarterly preventive maintenance for endpoint protection ▪ Regular daily pattern updates and firmware upgrade in co-term with the years of subscription ▪ Includes installation and configuration ▪ Includes Knowledge Transfer with completion and configuration report. Onsite conducted by Certified Professional Engineer for product served ▪ Includes vulnerability assessment for one (1) server on quarterly basis for Windows/Linux operating system.

V. DELIVERABLES

License subscription shall be delivered before the expiry date September 25, 2023

VI. CONTRACT PAYMENT SCHEME

The supplier will be paid within 30 days after receipt of the license.

VII. DATA PRIVACY ACT

The supplier must comply with the requirements of the Data Privacy Act.

Annex "A"

Price Quotation Form

Date:

MS. RIZA M. HERNANDEZ
Chairperson, Bids and Awards Committee
LBP Leasing and Finance Corporation (LLFC)
15th Flr., Sycip Law Center, #105 Paseo de Roxas St.,
Makati City

Dear **Ms. Hernandez**:

After having carefully read and accepted the terms and conditions in the Request for Quotation (RFQ), hereunder is our quotation/s for the item/s as follows:

Description/ Specifications:	**Qty.**	**Unit Price (P)**	**Total Price (P)**
(In details)			
Amount in Words:_____			
Warranty			

The above-quoted prices are inclusive of all costs and applicable taxes. Delivery **to LBP Leasing and Finance Corporation** shall not be later than September 25, 2023.

Very truly yours,

_____
Printed Name over Signature of Authorized Representative

_____
Name of Company

_____
Contact No./s

Please submit all the required eligibility documents together with the Annexes "A, B and C"

Annex "B"

Schedule of Requirements and Eligibility Requirements

Bidders must state **"Comply"** in the column "Statement of Compliance" against each of the individual parameters.

Requirements		Statement of Compliance
QUANTITY	**DESCRIPTIONS**	
100	Renewal and Upgrade from Endpoint Security Business Select to Endpoint Detection and Response	
30	Additional Endpoint Security with Detection and Response	
	Period Coverage: September 25, 2023 to September 24, 2025	
	Compliant with the Terms of Reference	
Eligibility Requirements *(Certified True Copies only)* :		
1. Valid and Current Year Mayor's Permit		
2. Valid and Current PhilGEPS Registration Number		
3. DTI / SEC Registration (for Partnership / Corporations)		
4. Notarized Secretary's Certificate for proof of authorization		

I hereby certify to comply and deliver all the above Schedule of Requirements.

_____	_____	_____
Name of Company /Bidder	**Signature over Printed Name of Authorized Representative**	**Date**