Bid Notice Abstract

Invitation to Bid (ITB)

Reference Number	11138840
Procuring Entity	OFFICE OF TRANSPORTATION COOPERATIVES
Title	SUPPLY AND DELIVERY OF ONE (1) NETWORK FIREWALL WITH FIVE (5) YEAR SUBSCRIPTION
Area of Delivery	Metro Manila

Solicitation Number:	GEPS 2024-011	**Status**	Awarded
Trade Agreement:	ADB Procurement Guidelines		
Procurement Mode:	Public Bidding	**Associated Components**	2
Classification:	Goods		
Category:	Information Technology		
Estimated Budget for the Contract:	PHP 2,100,000.00	**Bid Supplements**	0
Delivery Period:	30 Day/s		
Client Agency:		**Document Request List**	27
Contact Person:	Francis Emmanuel Seres Balcita BAC Secretariat 5th Floor Main, Ben-Lor Bldg., 1184 Quezon Avenue, Brgy. Paligsahan, Quezon City Metro Manila Philippines 1103 63-2-83329315 63-2-83329313 bac.secretariat@otc.gov.ph	**Date Published**	14/08/2024
		Last Updated / Time	25/11/2024 15:27 PM
		Closing Date / Time	09/09/2024 16:00 PM

Description

Firewall Network Protection Subscription Features

*Subscription Duration- At least 5 years

*TLS Inspection- Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.

*Intrusion Prevention (IPS)- Must be able to prevent malicious network traffic with packet inspection (IPS); Perimeter Defenses; and

*Advanced Threat Protection
- Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall);
- System that instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
- System that can create policies that limits access to network resources or completely isolate compromised systems until they are cleaned
- Intelligent firewall policies
- Multi-layered, call-home protection

*Clientless VPN - Ability to implement a Clientless VPN

*Web Control
-Must be able to block risky downloads, protect against data loss, prevent users from accessing websites that are inappropriate for work, and generate logs of blocked visited sites.
-Surfing quota time and access time policies per user/group

-Advanced web malware protection
-Live Protection real-time in-the-cloud lookups for the latest threat intelligence
-HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions
-SSL protocol tunneling detection and enforcement
-Certificate validation
-High performance web content caching
-File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
-Web keyword monitoring and enforcement to log, report or block web content matching keyword
lists with the option to upload customs lists
-Block Potentially Unwanted Applications (PUAs)
-Web policy override option for selected users to temporarily allow access to blocked sites or categories that are fully
customizable and manageable by select users.

*App Control
-Must provide the administrator the ability to define "acceptable web usage" settings (defined by categories) in order
to control the sites on which users are allowed to visit.
-Signature-based application control with patterns for thousands of applications
-App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
- Micro app discovery and control
-Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g.
P2P), and risk level
-Per-user or network rule application control policy enforcement

*Threat Intelligence Analysis
-All files containing active code downloaded via the web or coming into the firewall as email attachments such as
executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, and .rtf and
PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z,
Microsoft Cabinet) are automatically sent for Threat Intelligence Analysis
-Files are checked against a massive threat intelligence database and subjected to multiple machine learning models
to identify new and unknown malware

=Firewall Appliance Specifications=

*Firewall Throughput- At least 39,000 Mbps / 39 Gbps
*Firewall Throughput (appmix/IMIX)- At least 20,000 Mbps / 20 Gbps
*Threat Protection/Prevention Throughput- At least 1,500 Mbps / 1.5 Gbps
*Concurrent Connections- At least 6,500,000
*New Connections per Second- At least 148,000
*IPsec VPN Throughput- At least 20,000 Mbps / 20 Gbps

=Physical Interfaces and Expansion=

*Minimum Storage- At least 120 GB SSD
*Ethernet Interfaces
-Fixed Copper at least 8x Gigabit Ethernet ports
-Fixed Fiber at least 2x SFP ports
*Management Ports- At least 1x RJ45 Ethernet port
*Other I/O Ports- At least 1x USB Port

=Warranty and Support=

*Warranty and RMA- Hardware warranty & RMA for at least 5 years
*Support- 24x7 International Support via Telephone & Email with Remote Consultation
*Security Updates and Patches
-Security Updates & Patches for the duration of Firewall Subscription (5 years)
-Firewall Subscription (5 years)
-Software Features Updates & Upgrades for the duration of Firewall Subscription (5 years)
*Training
-Online Basic Training / Knowledge Transfer
-Training Certifications for at least 2 End users

=Additional Requirements=

1. Quality Assurance
● The supplier must ensure that the firewall delivered is free from defects and conform to the specified technical
requirements.
● Any defective units must be replaced within seven (7) days at no additional cost to the OTC.

2. Compliance with Government Policies
● The procurement process must adhere to all applicable government procurement policies and regulations.
● The contractor must comply with all relevant labor laws and regulations in the delivery of services.

Line Items

Item No.	Product/Service Name	Description	Quantity	UOM	Budget (PHP)
1	Information Technology	Network Firewall with Five (5) Year Subscription	1	Lot	2,100,000.00

Pre-bid Conference

Date	Time	Venue
27/08/2024	1:00:00 PM	OTC Board Conference Office of Transportation Cooperatives 5th Floor Main, Ben-Lor Building, 1184 Quezon Avenue, Brgy. Paligsahan, Quezon City 1103 Tel. No.: 8332-9315/8332-9311

Other Information
OTC BAC SECRETARIAT
Office of Transportation Cooperatives
5th Floor Main, Ben-Lor Building, 1184 Quezon Avenue, Brgy. Paligsahan, Quezon City 1103
Tel. No.: 8332-9315/8332-9311

Please send your Technical Component Envelope (legal, technical and financial documents as Envelope 1), and Financial Component Envelope (As Envelope 2) via a sealed envelope in five (5) sets of copies.

I. TECHNICAL COMPONENT ENVELOPE

Legal Documents:
1. Latest Mayor's/Business Permit
2. DTI, SEC, or CDA Certificate of Registration
3. Latest Tax Clearance
4. PhilGEPS Platinum Certificate of Registration and Membership;

Technical Documents:
1. Statement of all ongoing contracts,
2. Single Largest Completed Contract (SLCC)
3. Conformity with the Technical Specifications, delivery schedule
4. Original duly signed Revised Omnibus Sworn Statement (Notarized)
5. Bid-Securing Declaration (Notarized);
6. Original duly signed Secretary's certificate in case of corporation, partnership, or cooperative (Notarized); 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.

Financial Documents:
1. Audited Financial Statements for FY 2022 and FY 2023 (stamped "received" by the BIR).
2. Net Financial Contracting Capacity (NFCC) or committed Line of Credit.

II. FINANCIAL COMPONENT ENVELOPE

1. Original of duly signed and accomplished Financial Bid Form; and
2. Original of duly signed and accomplished Price Schedule(s).

Bidding Documents Price - Php 2,100.00

Reservation Clause: Pursuant to Section 41 of the IRR of R.A. 9184, the procuring entity reserves the right to 1)reject bids, 2) declare a failure of bidding, and 3) not to award the contract without incurring any liability if the funds/allotments for said program/project/activity have been withheld or reduced through no fault of its own.

Created by	Francis Emmanuel Seres Balcita
Date Created	09/08/2024

The PhilGEPS team is not responsible for any typographical errors or misinformation presented in the system. PhilGEPS only displays information provided for by its clients, and any queries regarding the postings should be directed to the contact person/s of the concerned party.