

INVITATION TO BID FOR

PROVISION OF CONSOLIDATED ICT SECURITY SOFTWARE SUBSCRIPTIONS FOR THE PHILIPPINE COMPETITION COMMISSION 2024

- The *Philippine Competition Commission (PCC)*, through the *F.Y. 2024 Budget pursuant to the General Provision of the National Expenditure Program (NEP) and Section 7.6 of the Revised 2016 Implementing Rules and Regulations of the Republic Act No. 9184*, intends to apply the sum of *Three Million Pesos (Php3,000,000.00)* being the ABC to payments under the contract for the *Provision of Consolidated ICT Security Software Subscriptions for the Philippine Competition Commission 2024* under *Invitation to Bid (IB) No. 2024-EPA-0010*.

Lots	Description	ABC (Php)
Lot 1	Anti-Virus (Endpoint and Server)	500,000.00
Lot 2	Cloud Based Intrusion Detection System	1,500,000.00
Lot 3	Backup Software for On-premises Infrastructure	1,000,000.00
TOTAL:		3,000,000.00

Bids received in excess of the ABC for each lot shall be automatically rejected at bid opening.

- The *PCC* now invites bids for the above Procurement Project. Delivery of the Goods is required upon receipt of the Notice to Proceed. Bidders should have completed a contract similar to the Project within five (5) years from the date of submission and receipt of bids. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).
- Bidding will be conducted through open competitive bidding procedures using a non-discretionary “*pass/fail*” criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.

Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA No. 5183.

4. Prospective Bidders may obtain further information from *PCC* and inspect the Bidding Documents at the address given below during *office hours from 8:00 A.M. to 5:00 P.M. (Monday through Friday)*.
5. A complete set of Bidding Documents may be acquired by interested Bidders on *15 November 2023* from the address below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB and internal issuance of PCC Bids and Awards Committee (PBAC), in the amount in the amount based on the lots to be bid as enumerated below:

LOT	PROJECT	ABC
Lot 1 Only	Anti-Virus (Endpoint and Server) (AV)	PhP 1,000.00
Lot 2 Only	Cloud Based Intrusion Detection System (CBIDS)	PhP 2,000.00
Lot 3 Only	Backup Software for On-premises Infrastructure (BSOI)	PhP 1,000.00

The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person or through e-mail.

It may also be downloaded free of charge from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and the website of the Procuring Entity, provided that Bidders shall pay the nonrefundable fee for the Bidding Documents not later than the submission of their bids.

6. The *PCC* will hold a Pre-Bid Conference on *23 November 2023, 2:00PM* at the given address below or through Microsoft Teams teleconference which shall be open to prospective bidders.
7. Bids must be duly received by the PBAC Secretariat through *IB No. 2024-EPA-0010* on *06 December 2023, 12:00NN* at *25^F Vertis North Corporate Center 1, North Avenue, Quezon City* or via *e-bid submission through this link: <https://pccgov.sharepoint.com/sites/E-BIDSubmission>*. Late bids shall not be accepted.
8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 14.
9. Bid opening shall be on *06 December 2023, 2:30PM* at the given address below or through Microsoft Teams Teleconference. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.
10. Bids submitted through online submission must be put in a compressed/zip folder. The compressed folders and the files in it must be **both password-protected**. Kindly refer to the Guidelines on PCC E-Bid Submission uploaded under the E-Bid System window of the PCC website. In case of tie, bidders' presence is required during tie breaking through toss coin or draw lots.

11. The **PCC** reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.

12. For further information, please refer to:

THE SECRETARIAT

Bids and Awards Committee

Philippine Competition Commission

25F Tower 1, Vertis North Corporate Center,

North Avenue, Quezon City

Telephone No.: (02) 771-9722 local 204

e-mail: procurement@phcc.gov.ph or cpsioson@phcc.gov.ph

13. You may visit the following websites:

For downloading of Bidding Documents:

<https://www.phcc.gov.ph/procurement/request-for-quotation-expression-of-interest-invitation-to-bid/>

For online bid submission: <https://pccgov.sharepoint.com/sites/E-BIDSubmission>

14 November 2023



ATTY. JOSEPH MELVIN B. BASAS

Chairperson, PCC Bids and Awards Committee



DETAILED TECHNICAL SPECIFICATIONS

Provision of Consolidated ICT Security Software Subscriptions for the Philippine Competition Commission

I. RATIONALE:

The Philippine Competition Commission (PCC), through the Information and Communications Technology Division (ICTD), manages, maintain and secure its network, endpoint and servers, as well as ensure reliable backup of documented information.

Currently, the ICTD manages cloud-based anti-virus and intrusion detection systems for its 300 endpoints and servers. Finally, it uses a backup software which connects to the cloud for the required data protection.

The PCC needs to procure subscription licenses for network, endpoint and server security, as well as backup protection of PCC documented information, for the continuous operation of its systems infrastructure.

Procurement of the following ICT security subscription shall be done on a lot basis namely:

Lot 1: Anti-Virus (Endpoint and Server)

Lot 2: Cloud-Based Intrusion Detection System

Lot 3: Backup Software for On-premises Infrastructure

II. OBJECTIVE:

1. Strengthen PCC computing assets and improve its cybersecurity stance by implementing an efficient, reliable and cost-effective security system and software subscription;
2. Protect valuable information assets of the Commission from being compromised brought about by malicious activities;
3. Protect endpoint computers and servers against malicious software, viruses, and unwanted network intrusions that may harm PCC's computing ecosystem; and
4. Increase capability of the ICTD in monitoring health of PCC information assets.

III. SCOPE OF WORK:

Lot 1 – Anti-Virus (Endpoint and Server)

- Submit manufacturer's catalog and product data;
- Provide all materials, equipment and peripherals, and scope of works (to include those not mentioned in this Detailed Technical Specifications but needed in the completion of the project);
- The supplier must submit the following project documentation:

- i. Project Management Team (Name, Role, Qualifications/Certifications, Contact Numbers)
 - ii. Deployment Plan
 - iii. User Acceptance Test
 - iv. Testing and Technical Report
- Service Level Agreement
 - Replace defective units / licenses in full within fifteen (15) days from the date of delivery, if found defective during installation without additional cost to PCC;
 - Provide a single point of contact for technical and customer support, either phone or electronic mail;
- Provide 8X7 call and onsite technical support with three (3) hours response time for technical problem that requires on-site services, including weekend and holidays.
- Backup configurations, data and information before installation;
- Upgrade firmware version to latest stable version;
- Deploy, install and configure the Anti-Virus (Endpoint and Server);
- Verify if rules and policies and other configurations are working and no unplanned changes were made

Lot 2 – Cloud-Based Intrusion Detection System:

- Submit manufacturer’s catalog and product data;
- Provide all materials, equipment and peripherals, and scope of works (to include those not mentioned in this Detailed Technical Specifications but needed in the completion of the project);
- The supplier must submit the following project documentation:
 - i. Project Management Team (Name, Role, Qualifications/Certifications, Contact Numbers)
 - ii. Deployment Plan
 - iii. User Acceptance Test
 - iv. Testing and Technical Report
- Service Level Agreement
 - Replace defective units / licenses in full within fifteen (15) days from the date of delivery, if found defective during installation without additional cost to PCC;
 - Provide a single point of contact for technical and customer support, either phone or electronic mail;
- Provide 8X7 call and onsite technical support with three (3) hours response time for technical problem that requires on-site services, including weekend and holidays.
- Backup configurations, data and information before installation;
- Upgrade firmware version to latest stable version;
- Deploy, install and configure the Intrusion Detection System;
- Verify if rules and policies and other configurations are working and no unplanned changes were made

Lot 3 – Backup Software for On-premises Infrastructure:

- Submit manufacturer’s catalog and product data;
- Provide all materials, equipment and peripherals, and scope of works (to include those not mentioned in this Detailed Technical Specifications but needed in the completion of the project);
- The supplier must submit the following project documentation:

- i. Project Management Team (Name, Role, Qualifications/Certifications, Contact Numbers)
 - ii. Deployment Plan
 - iii. User Acceptance Test
 - iv. Testing and Technical Report
- Service Level Agreement
 - Replace defective units / licenses in full within fifteen (15) days from the date of delivery, if found defective during installation without additional cost to PCC;
 - Provide a single point of contact for technical and customer support, either phone or electronic mail;
- Provide 8X7 call and onsite technical support with three (3) hours response time for technical problem that requires on-site services, including weekend and holidays. Backup configurations, data and information before installation;
- Upgrade firmware version to latest stable version;
- Deploy, install and configure the Backup Software;
- Verify if rules and policies and other configurations are working and no unplanned changes were made

IV. INFORMATION SECURITY AND NON – DISCLOSURE AGREEMENT

To ensure protection of PCC information assets, bidders are expected to observe and abide by the established PCC Information Security Management System (PCC ISMS) and shall agree to sign a non-disclosure agreement.

All data, documents, records, configuration files and metadata (collectively “Information”) to be provided to the bidders for purposes of delivering the Services are considered confidential information and shall remain the sole property of PCC. The Service Providers shall acknowledge the importance of maintaining security and confidentiality of the Information and agree to prevent unauthorized transfer, disclosure, or use of these Information by any third person or entity. Bidders shall not use the Information for any purpose other than in connection with the Services. Bidders shall ensure that it will not retain, after completion of the Services with which the Information was provided, all or any portion of the Information, in any manner whatsoever.

V. APPROVED BUDGET FOR THE CONTRACT (ABC)

The ABC for the project is **Three Million Pesos Only (3,000,000.00)** inclusive of all applicable government taxes and service. The contract price shall include all the costs and profits arising from the or in relation to the services rendered in connection with the engagement and until the end of the contract.

Breakdown of Approved Budget per Lot

Lot 1: Anti-Virus (Endpoint and Server)	500,000.00
Lot 2: Cloud Based Intrusion Detection System	1,500,000.00
Lot 3: Backup Software for On-premises Infrastructure	1,000,000.00
TOTAL	3,000,000.00

Bids received in excess of the ABC per lot shall be automatically rejected at bid opening.

VI. QUALIFICATION OF THE SUPPLIER

The Bidder/s should have the following minimum requirement:

- a. Should be an established IT company with experience with the following:

Lot No. / Project	Years / Relevant Experience
Lot 1: Anti-Virus (Endpoint and Server)	Three (3) years experience in installing and configuring Anti-Virus
Lot 2: Cloud Based Intrusion Detection System	Three (3) years experience in installing and configuring Intrusion Detection System (IDS)
Lot 3: Backup Software for On-premises Infrastructure	Three (3) years experience in installing and configuring Backup Software for On-premises Infrastructure

- b. Must submit certification of authorized distributorship / dealership / resellership from the distributor / manufacturer of the product/s offered.
- c. Submit the list of identified certified engineers and/or technicians with **signed curriculum vitae** that will be involved in the software and/or equipment maintenance, **with at least three (3) years of experience working in similar field of engagement.**
- d. Should submit copies of client’s satisfactory certificates and/or certificate of completion and acceptance from at least three (3) clients for the last five (5) years, with similar contracts. Similar contracts refer to installation and configuration of Network Security Module, Anti-Virus for Endpoint and Server, Cloud-Based Intrusion Detection System, Backup Software.

The pertinent documents to support the above-mentioned qualifications shall be part of the bid submission.

VII. TECHNICAL SPECIFICATIONS:

Minimum and/or equivalent functional requirements, technical specifications, features, characteristics and numbers.

Lot 1: Endpoint and Server Anti-Virus

A. Endpoint Anti-virus

1. At least Three Hundred (300) licenses
2. Subscription period for Twelve (12) Months from installation of software
3. Must be compatible with the existing PCC Antivirus for Endpoint
4. Includes Agent for Windows and MacOS
5. Must be centrally cloud-managed
6. With the following features:
7. With Advance Threat Hunting and IT Security (Endpoint Detection and Response)

- Deep Learning
- Exploit Prevention
- Active Adversary Protection
- Cryptoguard and WipeGuard Anti-Ransomware
- Root Cause Analysis
- Application Whitelisting
- Anti-Malware
- Live Protection
- Web Security
- Web Control
- Malware Removal
- Peripheral Control
- Application Control
- Behavior Analysis
- Data Loss Prevention
- Download Reputation
- Malicious Traffic Detection
- Potentially Unwanted Application Blocking

B. Server Anti-virus

1. At least Fifteen (15) Licenses
2. Subscription period for Twelve (12) Months from installation of software
3. Must be compatible with the existing PCC Antivirus for Servers
4. Includes agent for Windows and Linux
5. Must be centrally cloud-managed
6. With the following features:
 - Deep Learning
 - Exploit Prevention
 - Active Adversary Protection
 - Cryptoguard and WipeGuard Anti-Ransomware
 - Root Cause Analysis
 - Application Whitelisting
 - Anti-Malware
 - Live Protection
 - Malicious traffic detection
 - AWS Integration for windows server
 - Server Application Whitelisting
 - Automatic Exclusion
 - Behavior Analysis
 - Web Security
 - Download Reputation
 - Web Control
 - Peripheral Control
 - Application Control
 - Data Loss Prevention
 - Anti-Ransomware
 - Malware Removal

Lot 2: Cloud-Based Intrusion Detection System (IDS)

- At least Three Hundred (300) licenses
- Subscription period for Twelve (12) Months from installation of software
- Must be compatible with the existing PCC IDS;
- Must have a cloud-based management console;
- Must have a single pane of glass for hosts, devices, applications, users, files and geolocation, etc.;
- Must be compatible and able to protect laptops, workstations, servers, and mobile devices – running Windows, Mac OS, Linux, Android and iOS;
- Must be integrated/connected to latest global threat intelligence system to prevent/detect known attacks, threats, and vulnerabilities;
- Must work in conjunction with the current PCC Endpoint Security;
- Must have the following features and capabilities:
 - Continuous file analysis, recording of activity and history of behavior over time;
 - Must be able to do a back in time analysis and can establish root cause and remediation;
 - Correlation of file, telemetry and intrusion events;
 - Can continuously track device activity leading up to and after compromise;
 - With advance analytics and intelligence for file reputation;
 - Capable of sending alerts to administrator;
 - Tracking of file propagation in the corporate network for visibility and scoping;
 - With sandboxing technology;
 - With established threat grid technology and directly integrated to sandboxing technology;
 - Can easily search the entire corporate network of infected endpoints and quarantine files remotely;
 - Can display files that have been executed across the corporate network;
 - Identify software and application vulnerabilities and close attack pathways;
 - With comprehensive search features;
 - Must have capability to defend against from exploit-based and memory injection attacks;
 - Capable of command line visibility for determination of legitimate applications;
 - Can be integrated with third-party security tools and SIEMS;
 - Can show list of hosts that contain vulnerable software and application; and
 - With robust reportorial view of detection and remediation.

Lot 3: Backup Software for On-premises Infrastructure

1. The backup software must be able to handle rapid recovery, data loss avoidance, recoverability, and visibility with the following features:
 - Must be compatible with the current PCC HCI Hypervisor (Acropolis), hardware and related components;
 - With at least 70 Instances;
 - Subscription period for Twelve (12) Months from installation of software
 - Can be agent or agentless software;
 - With centralized management web user interface;
 - Can recover a Virtual Machine (VM) on the original host or a different host;
 - Can quickly restore service VM directly from a backup file on a regular backup storage;

- With point-in-time recovery for VM;
 - Can recover individual VM files;
 - Can backup virtual machine in a cloud storage;
 - Can recover files from windows, linux, BSD, Mac OS, etc.;
 - Restore individual VMs, guest files and applications from snapshots;
 - Must be compatible with the current PCC control system and applications such as Active Directory, Microsoft Exchange, SQL Server and Sharepoint;
 - With a self-service Web User Interface for restoration for guest files, Microsoft exchange mailbox and database recovery;
 - Must be application aware;
 - Can streamline ad-hoc backup for live VMs;
 - Can perform incremental backups;
 - With built-in deduplication, compressions and swap exclusions;
 - Can analyze the NTFS Master File Tables;
 - Can copy VM backups to Disaster Recovery storage solutions (e.g., azure) at least five (5) critical VM backup;
 - Fully integrated, fast and secure backup and can restore from cloud with end-to-end encryption;
 - Can replicate VMs for high availability and off-site disaster recovery;
 - Can test and verify VM for recoverability including support for custom application test scripts;
 - With sand boxing technology;
2. Must be the same brand and version as the current PCC Backup Software; and
 3. Must cover the warranty of the related software, hardware and peripherals.

VIII. SCHEDULE OF REQUIREMENTS:

Must complete the installation and provisioning within thirty (30) calendar days from receipt of Notice to Proceed.

IX. MODE OF PROCUREMENT:

The mode of procurement shall be Competitive Bidding provided under the Revised Implementing Rules and Regulations (IRR) of Republic Act (R.A.) No. 9184.

X. PAYMENT SCHEME:

Payment shall be **ONE TIME PAYMENT**. The PCC shall pay the Provider within fifteen (15) working days upon receipt of the original signed Statement of Account, or billing statement, supported by Certificate of Completion and/or Certificate of Satisfactory Service Rendered to be issued by the end-user.

XI. LIQUIDATED DAMAGES:

If the supplier fails to deliver any or all of the goods and/or to perform the services within the period specified in the contract, the Procuring Entity shall, without prejudice to its other remedies under this contract and under the applicable law, deduct from the contract price as liquidated damages, the applicable rate of one-tenth (1/10) of one percent (1%) of the cost of the unperformed portion of every day of delay. The maximum deduction shall be ten percent (10%) of the amount of the contract. Once, the maximum is reached, the procuring entity

reserves the right to rescind the contract, without prejudice to other courses of action and remedies open to it.

XII. DISPUTE AGREEMENT / RESOLUTION:

Should any dispute related to the Contract and/or rights of the parties arise, the same shall be submitted to mutual consultation, mediation and arbitration, in the order of application. The venue of the proceedings shall be in Quezon City.

In case of a court suit, the venue shall be the courts of competent jurisdiction in Quezon City, to the exclusion of all other courts; and

Any amendments and additional terms and conditions of the Contract must be in writing, signed and acknowledged by the Parties.

Prepared by:



SAMUELLE DAVID S. ONCHENGCO
Information Systems Analyst I

Approved by:



ALLAN ROY D. MORDENO, CISM
Chief, ICT Division

Noted by:



JESON Q. DE LA TORRE
Director IV, Administrative Office

Conforme:

Name and Signature of Authorized Representative

Designation

Name of Company

Date