BAGONG PILIPINAS

PHILIPPINE PORTS AUTHORITY

SUPPLY, DELIVERY AND INSTALLATION OF A CORPORATE ANTI-VIRUS WITH ENDPOINT DETECTION AND RESPONSE (EDR) FOR THREE (3) YEARS AT THE PPA HEAD OFFICE AND PORT MANAGEMENT OFFICES NATIONWIDE

BID DOCS
ASD-126-2025

Table of Contents

Glossary of Acronyms, Terms, and Abbreviations 3

Section I. Invitation to Bid 6

Section II. Instructions to Bidders 9

1. Scope of Bid 10
2. Funding Information 10
3. Bidding Requirements 10
4. Corrupt, Fraudulent, Collusive, and Coercive Practices 10
5. Eligible Bidders 10
6. Origin of Goods 11
7. Subcontracts 11
8. Pre-Bid Conference 11
9. Clarification and Amendment of Bidding Documents 11
10. Documents comprising the Bid: Eligibility and Technical Components 11
11. Documents comprising the Bid: Financial Component 12
12. Bid Prices 12
13. Bid and Payment Currencies 13
14. Bid Security 13
15. Sealing and Marking of Bids 13
16. Deadline for Submission of Bids 13
17. Opening and Preliminary Examination of Bids 14
18. Domestic Preference 14
19. Detailed Evaluation and Comparison of Bids 14
20. Post-Qualification 15
21. Signing of the Contract 15

Section III. Bid Data Sheet 16

Section IV. General Conditions of Contract 18

1. Scope of Contract 19
2. Advance Payment and Terms of Payment 19
3. Performance Security 19
4. Inspection and Tests 19
5. Warranty 20
6. Liability of the Supplier 20

Section V. Special Conditions of Contract 21

Section VI. Schedule of Requirements 25

Section VII. Technical Specifications 26

Section VIII. Checklist of Technical and Financial Documents 52

Section IX. Bidding Forms 55

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

Bid – A signed offer or proposal to undertake a contract submitted by a bidder in response to and in consonance with the requirements of the bidding documents. Also referred to as *Proposal* and *Tender.* (2016 revised IRR, Section 5[c])

Bidder – Refers to a contractor, manufacturer, supplier, distributor and/or consultant who submits a bid in response to the requirements of the Bidding Documents. (2016 revised IRR, Section 5[d])

Bidding Documents – The documents issued by the Procuring Entity as the bases for bids, furnishing all information necessary for a prospective bidder to prepare a bid for the Goods, Infrastructure Projects, and/or Consulting Services required by the Procuring Entity. (2016 revised IRR, Section 5[e])

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

Consulting Services – Refer to services for Infrastructure Projects and other types of projects or activities of the GOP requiring adequate external technical and professional expertise that are beyond the capability and/or capacity of the GOP to undertake such as, but not limited to: (i) advisory and review services; (ii) pre-investment or feasibility studies; (iii) design; (iv) construction supervision; (v) management and related services; and (vi) other technical services or special studies. (2016 revised IRR, Section 5[i])

CDA - Cooperative Development Authority.

Contract – Refers to the agreement entered into between the Procuring Entity and the Supplier or Manufacturer or Distributor or Service Provider for procurement of Goods and Services; Contractor for Procurement of Infrastructure Projects; or Consultant or Consulting Firm for Procurement of Consulting Services; as the case may be, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

DDP – Refers to the quoted price of the Goods, which means "delivered duty paid."

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

Foreign-funded Procurement or Foreign-Assisted Project– Refers to procurement whose funding source is from a foreign government, foreign or international financing institution as specified in the Treaty or International or Executive Agreement. (2016 revised IRR, Section 5[b]).

Framework Agreement – Refers to a written agreement between a procuring entity and a supplier or service provider that identifies the terms and conditions, under which specific purchases, otherwise known as "Call-Offs," are made for the duration of the agreement. It is in the nature of an option contract between the procuring entity and the bidder(s) granting the procuring entity the option to either place an order for any of the goods or services identified in the Framework Agreement List or not buy at all, within a minimum period of one (1) year to a maximum period of three (3) years. (GPPB Resolution No. 27-2019)

GFI – Government Financial Institution.

GOCC – Government-owned and/or –controlled corporation.

Goods – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term "related" or "analogous services" shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

Infrastructure Projects – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

Procurement Project – refers to a specific or identified procurement covering goods, infrastructure project or consulting services. A Procurement Project shall be described, detailed, and scheduled in the Project Procurement Management Plan prepared by the agency which shall be consolidated in the procuring entity's Annual Procurement Plan. (GPPB Circular No. 06-2019 dated 17 July 2019)

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

Supplier – refers to a citizen, or any corporate body or commercial company duly organized and registered under the laws where it is established, habitually established in business and engaged in the manufacture or sale of the merchandise or performance of the general services covered by his bid. (Item 3.8 of GPPB Resolution No. 13-2019, dated 23 May 2019). Supplier as used in these Bidding Documents may likewise refer to a distributor, manufacturer, contractor, or consultant.

UN – United Nations.

BAGONG PILIPINAS

PHILIPPINE PORTS AUTHORITY

INVITATION TO BID

FOR THE SUPPLY, DELIVERY AND INSTALLATION OF A CORPORATE ANTI-VIRUS WITH ENDPOINT DETECTION AND RESPONSE (EDR) FOR THREE (3) YEARS AT THE PPA HEAD OFFICE AND PORT MANAGEMENT OFFICES NATIONWIDE

The Philippine Ports Authority, through the Corporate Budget of the Authority for CY 2025 intends to apply the sum of **P30,500,000.00** being the Approved Budget for the Contract (ABC) to payments under the contract for the Supply, Delivery and Installation of a Corporate Anti-Virus with Endpoint Detection and Response (EDR) for Three (3) years at the PPA Head Office and Port Management Offices Nationwide (ASD-126-2025). Bids received in excess of the ABC shall be automatically rejected at bid opening.

The Philippine Ports Authority now invites bids for the above Procurement Project. The Corporate Anti-Virus with Endpoint Detection and Response (EDR) should be installed and configured and accepted within Ninety (90) days upon receipt by the winning bidder of the Notice to Proceed. The license and support period of Three (3) years shall commence upon issuance of the Certificate of Acceptance by the end-user. Bidders should have completed, within five (5) years from the date of submission and receipt of bids, a contract similar to the Project. 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) 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 5183.

Prospective Bidders may obtain further information from the Philippine Ports Authority Bids and Awards Committee (BAC) and inspect the Bidding Documents at the address given below during 8:00 a.m. to 5:00 p.m., Monday to Friday.

A complete set of Bidding Documents may be acquired by interested Bidders on **29 July 2025** from the given address and website(s) below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of **Twenty Five Thousand (P25,000.00) Pesos.** The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person.

The Philippine Ports Authority's Bids and Awards Committee will hold a Pre-Bid Conference on **06 August 2025 at 10:00 a.m.** at the PPA Function Room, 7th Floor, PPA Bldg., Bonifacio Drive, South Harbor, Port Area, Manila, which shall be open to all prospective bidders.

Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below on or before **19 August 2025 at 9:00 a.m.** Late bids shall not be accepted.

All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in ITB Clause 14.

Bid opening shall be on **19 August 2025 at 10:00 a.m.** at the 7th Floor, PPA Building, A. Bonifacio Drive, South Harbor, Port Area, Manila. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

The Philippine Ports Authority 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.

For further information, please refer to:

BAC Secretariat, Philippine Ports Authority
5th Floor, PPA Bldg., A. Bonifacio Drive,
South Harbor, Port Area, Manila
Telephone Nos. 527-47-35
527-83-56 to 83 loc. 539
PPA Website: www.ppa.com.ph
PhilGEPS Website: www.philgeps.gov.ph

for: **MARK JON S. PALOMAR**
Chairperson, PPA Head Office Bids and Awards
Committee for the Procurement of Goods and
Consultancy Services (HO-BAC-PGCS)

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, PHILIPPINE PORTS AUTHORITY wishes to receive Bids for the **SUPPLY, DELIVERY AND INSTALLATION OF A CORPORATE ANTI-VIRUS WITH ENDPOINT DETECTION AND RESPONSE (EDR) FOR THREE (3) YEARS AT THE PPA HEAD OFFICE AND PORT MANAGEMENT OFFICES NATIONWIDE** with identification number **ASD-126-2025.**

The Procurement Project (referred to herein as "Project" is composed of a single lot, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

2.1. The Philippine Ports Authority through its corporate budget for the Calendar Year (CY) 2025 in the amount of **THIRTY MILLION FIVE HUNDRED THOUSAND PESOS (Php30,500,000.00)**.

2.2. The source of funding is the Corporate Budget of the PHILIPPINE PORTS AUTHORITY.

3. Bidding Requirements

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex "I" of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.

5. Eligible Bidders

5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.

5.2 Foreign ownership limited to those allowed under the rules may participate in this Project.

5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to at least fifty percent (50%) of the ABC.

5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

6. Origin of Goods

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **ITB** Clause 18.

7. Subcontracts

7.1 The Bidder may subcontract portions of the Project to the extent allowed by the Procuring Entity as stated herein, but in no case more than twenty percent (20%) of the Project.

The Procuring Entity has prescribed that:

Subcontracting is not allowed.

8. Pre-Bid Conference

The Procuring Entity will hold a Pre-Bid conference for this Project on the specified date and time and either at its physical address at the PPA Function Room, 7th Floor, PPA Building, Bonifacio Drive, South Harbor, Port Area, Manila and/or through videoconferencing/webcasting as indicated in paragraph 6 of the **IB.**

9. Clarification and Amendment of Bidding Documents

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents).**

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within five (5) years prior to the deadline for the submission and receipt of bids.

10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

11. Documents comprising the Bid: Financial Component

11.1. The second bid envelope shall contain the financial documents for the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.

11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.

11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **IB** shall not be accepted.

11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

12. Bid Prices

12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:

a. For Goods offered from within the Procuring Entity's country:

i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);

ii. The cost of all customs duties and sales and other taxes already paid or payable;

iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and

iv. The price of other (incidental) services, if any, listed in e.

b. For Goods offered from abroad:

i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination

in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

ii. The price of other (incidental) services, if any, as listed in **Section VII (Technical Specifications).**

13. Bid and Payment Currencies

13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.

13.2. Payment of the contract price shall be made in Philippine Pesos.

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and bid security shall be valid for One Hundred Twenty (120) calendar days from the date of the opening of bids. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

Each bidder shall submit one copy of the first and second components of the Bid.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.

16. Deadline for Submission of Bids

16.1. The Bidders shall submit on the specified date and time and either at its physical address or through online submission as indicated in paragraph 7 of the **IB.**

17. Opening and Preliminary Examination of Bids

17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **IB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

18. Domestic Preference

18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

19. Detailed Evaluation and Comparison of Bids

19.1. The Procuring BAC shall immediately conduct a detailed evaluation of all Bids rated *"passed,"* using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.

19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB** Clause 15 shall be submitted for each lot or item separately.

19.3. The descriptions of the lots or items shall be indicated in **Section VII (Technical Specifications)**, although the ABCs of these lots or items are indicated in the **BDS** for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the 2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.

19.4. The Project shall be awarded as one Project having several items that shall be awarded as one contract.

19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

20. Post-Qualification

20.1. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

21. Signing of the Contract

21.1. The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS**.

Bid Data Sheet

ITB Clause	
5.3	For this purpose, contracts similar to the Project shall be: a. SUPPLY, DELIVERY, AND INSTALLTION OF ANY SOFTWARE SUBSCRIPTION. b. completed within the last five (5) years prior to the deadline for the submission and receipt of bids.
7.1	Subcontracting is not allowed.
12	The price of the Goods shall be quoted DDP *[Manila]* or the applicable International Commercial Terms (INCOTERMS) for this Project.
14.1	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: a. The amount of not less than SIX HUNDRED TEN THOUSAND PESOS (Php610,000.00), if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or b. The amount of not less than ONE MILLION FIVE HUNDRED TWENTY FIVE THOUSAND PESOS (Php1,525,000.00) if bid security is in Surety Bond.
15	Each Bidder shall submit **ONE (1) original and SIX (6) copies** of its Technical and Financial Components of its Bid in two (2) separate sealed bid envelopes, which should be submitted simultaneously. Each of the bid documents should be individually sealed. All bid documents shall be book-bound with hard cover and properly labelled with index tabs. Failure to comply with the said requirements is a ground for automatic disqualification of the bidder.
19.3	Partial bid is not allowed. The goods are grouped in a single lot and the lot shall not be divided into sub-lots for the purpose of bidding, evaluation, and contract award.
20.1	No additional requirements.
21.1	No additional requirements.

Section IV. General Conditions of Contract

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC).**

2. Advance Payment and Terms of Payment

2.1. Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.

2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the SCC.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the SCC, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

5.1 In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.

5.2 The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section V. Special Conditions of Contract

Special Conditions of Contract

GCC Clause	
1	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *[For Goods supplied from abroad, state:]* "The delivery terms applicable to the Contract are DDP delivered [*indicate place of destination*]. In accordance with INCOTERMS." *For Goods supplied from within the Philippines, state:*] "The delivery terms applicable to this Contract are delivered *[indicate place of destination].* Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative/s at the Project Site is the **Acting Manager, Information & Communication Technology Department (ICTD), Philippine Ports Authority Head Office, Manila.** **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: 1. Performance or supervision of on-site assembly and/or start-up of the supplied Goods; 2. Furnishing of tools required for assembly and/or maintenance of the supplied Goods; 3. Furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; 4. Performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and 5. The winning bidder must provide free classroom training to fifteen (15) technical personnel of PPA on the installation, configuration, management, monitoring and maintenance of the solution. A Certificate of Completion must be provided after the training has been completed.

	6. Submit the following documents: (a) Training Syllabi and Materials; (b) Installation, Troubleshooting, Monitoring and Management Procedure Manual. 7. The winning bidder shall shoulder all expenses (parking, venue, meals, etc.) during the training. 8. The winning bidder shall conduct one (1) online cybersecurity awareness and/or technical training session annually for all PPA employees throughout the duration of the project. The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. **Packaging –** The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit. The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity. The outer packaging must be clearly marked on at least four (4) sides as follows: Name of the Procuring Entity Name of the Supplier Contract Description Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. **Transportation –** Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract,

	shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price. Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price. Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights –** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	Payment shall be made in accordance with the following: The Corporate Anti-Virus with EDR should be installed and configured, and accepted within ninety (90) days upon receipt of Notice of Proceed (NTP). The license and support period of three (3) years shall commence upon issuance of the Certificate of Acceptance by the end-user. Payment shall be made upon issuance of Certificate of Acceptance by the end-user.
4	No additional requirements.

Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Item Number	Description[1]	Quantity	Total	Delivered, Weeks/Months
	Supply, Delivery and Installation of a Corporate Anti-Virus with Endpoint Detection and Response (EDR) for Three (3) Years at the PPA Head Office and Port Management Offices Nationwide	4,000 licenses	4,000 licenses	The Corporate Anti-Virus with EDR should be installed and configured, and accepted within ninety (90) days upon receipt of the winning bidder of the Notice to Proceed. The license and support period of three (3) years shall commence upon issuance of the Certificate of Acceptance by the end-user.

Section VII. Technical Specifications

Technical Specifications

Item	Specification	Statement of Compliance
		[Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A

		statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.]
	SUPPLY, DELIVERY AND INSTALLATION OF A COPORATE ANTI-VIRUS WITH ENDPOINT DETECTION AND RESPONSE (EDR) FOR THREE (3) YEARS AT THE PPA HEAD OFFICE AND PORT MANAGEMENT OFFICES NATIONWIDE	

SCOPE OF BID

- The bid proposal would be for the provision of **Four Thousand (4000)** licenses for PPA's Head Office and Project Management Offices' Desktop Computers, Servers and Laptops.
- Upgrade of the PPA's existing corporate Anti-Virus from Endpoint Protection to Endpoint Detection and Response (EDR).
- The proposal shall include the installation, setup and configuration of the Corporate Anti-Virus with EDR Client and Server at the Head Office and Remote Sites.

SPECIFICATIONS

Bidders must be able to supply the Corporate Anti-Virus with EDR that meets the following technical specifications:

Technical Specification	
Endpoint Detection and Response (EDR)	
General Features	a. The solution should have all its components deployed on-premises
	b. Solution should NOT share any data of endpoints i.e. telemetry details in public cloud.
Management Console	a. The solution should provide a unified web-based console for all functionalities and should allow administrators to access the management interface from any authorized machine, without installing additional software.
	b. The solution should support multi-site configuration.
	c. The solution should provide the flexibility to have individual rules/policies for every group. The solution should also support policy inheritance from Account to Site to Group with the ability to break inheritance if required.
	d. Solution should provide a console easy to understand and to navigate with common workflows.
	e. The proposed solution must have the option to create role-based access/view(s) of the management console.
	f. Solution should support multi-factor authentication for the management console

			g. The solution should offer centralized auditing of incident response activities, accessible through the management console.	
		Agent Capabilities	a. The solution should deliver both Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities through a single agent, eliminating the need for multiple software installations. Additionally, all other security features—such as Firewall, Host Intrusion Prevention System (HIPS), Threat Intelligence, Device Control, Application Control, real-time analysis, and threat hunting—must also be integrated and accessible via the same unified agent.	
			b. Solution should provide strong anti-tamper capabilities, to ensure that an end user can not remove, disable or modify the product in any way.	
			c. Solution should have ability to trigger/schedule on-demand scans (from console and/or endpoint) to look for malware or ensure a threat has been remediated.	
			d. Solution should have ability to upgrade agents with no impact to the end users.	
			e. All the features of the solution should be functional even if license count is exceeded.	
			f. Agent to be uninstalled remotely from the management console.	
			g. Solution must allow to export device inventories.	
			h. Deployed agents must be able to communicate with central management server via a web- proxy.	
		Operating System Support	a. Solution must support all supported versions of Operating Systems and should continue support for a minimum period of 12 months after the OS version is end of sale/life.	
			b. EDR Solution must provide prevention across all major Operating Systems – Windows, MacOS and Linux.	
			c. Solution must support all the latest versions of Windows Operating Systems. Following but not limited to: Windows Server Core 2016 and 2019, Windows Server 2022, 2019, 2016, 2012 R2, Windows 10, 11, 10, 8.1, 8, 7, Vista, XP SP2.	

			d. Solution should support all the latest Linux environments CentOS, Debian, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server, Ubuntu and Mint.	
			e. Solution should support all the new OS Updates/Versions within 60 days of release.	
		Threat Prevention	a. The proposed solution should offer context-aware Endpoint Detection and Response (EDR) capabilities, including comprehensive recording and detailed reporting of system-level activities. This will enable threat analysts to quickly assess the nature and extent of an attack. Additionally, the solution must support custom detection, threat intelligence integration, and advanced control mechanisms.	
			b. Blocks attempts to exploit software or system vulnerabilities before they can be executed.	
			c. EDR Solution must have capability to protect the system against known and unknown malwares.	
			d. EDR solution should ensure that every read, write and execute operations on files is checked for malware	
			e. Solution should be effective against sophisticated attacks by analyzing Behaviors on an endpoint, along with signature-based approach.	
			f. The solution should incorporate robust mechanisms to protect endpoints from malware even in offline environments. The agent must operate in a fully autonomous manner, without dependency on a management server, cloud infrastructure, or any external resources. It should be capable of independently detecting and responding to advanced threats, including zero-day attacks, file-less malware, memory-based exploits, ransomware, crypto miners, lateral movement, and advanced persistent threats (APTs), in real time as they occur.	
			g. EDR solution should leverage Artificial Intelligence or Machine Learning to analyze files pre-execution as well as analyze behaviors while a file is running.	
			h. The solution should allow the user to perform threat hunting to detect dormant threats as well.	

			i. The EDR solution should support protection capabilities across Windows, Mac, Linux	
			j. Solution must provide prevention across ALL major Operating Systems – Windows, MacOS and Linux.	
			k. The solution should protect endpoints from malicious documents and scripts.	
			l. The solution should monitor and protect the system from lateral movements & insider threats.	
			m. The EDR solution should monitor and protect from exploits and file-less attacks.	
			n. The EDR solution should identify and block potentially unwanted programs on the systems.	
			o. The solution should provide the flexibility to safely download malicious or convicted file from the management console	
		Response & Remediation Capabilities	a. The proposed solution should be able to perform threat sweeping based on the threat feeds (Files, URLs) or from intelligence received from the integrated on-premises sandbox solution.	
			b. The proposed solution be able to perform sweeps across endpoints using rich search criteria	
			c. The proposed solution will be able to Real time response on MITRE specific threat detection.	
			d. The proposed solution should provide option to sweep and assess the current (point in time/Live) state of the devices.	
			1. Scan disk Files	
			2. Scan in memory process	
			3. Search registry"	
			e. The proposed solution to provide the advance response capabilities as mentioned below	
			1. Kill process	
			2. Isolate device	
			3. Block process	
			f. The proposed solution shall allow ingestion of IOCs (Indicators of compromise) like URLs, file-hashes and shall also allow blocking of the files/file-hashes	

			g. The proposed solution can take risk-based response on the endpoint based on endpoint characteristics and reputation. The reputation of the endpoint is computed based on unusual or malicious behaviour of endpoint over time.	
			h. The proposed solution provide remediation console which provide functionality to access end user systems process, services, Task Manager, Registry, Active connection, cmd, application in startup, Directory etc.	
			i. Solution should detect and log all remote shell commands in a remote shell session.	
			k. Solution should alert on both suspicious and malicious threat behavior.	
			l. Solution should have ability to kill and quarantine an offending process.	
			m. Solution should support backup and restoration of files in order to reverse destructive data events that occur during attacks such as ransomware attack.	
			n. Solution should provide option to network quarantine a device and provide flexibility to configure the same.	
			o. Threat response capabilities offered by the solution should be easily automated.	
			p. Solution should provide a mechanism to take remedial actions on multiple systems at once.	
		Policy & Installation	a. Tool should provide Ability to support policy propagation across site or group of devices	
			b. Tool should have the option to provide dynamic policy assignment based on device attributes	
			c. Devices should be installed and placed directly into a specific device group at time of installation	
			d. Policy modifications should be applied in near real time	
			e. The product should have predefined list of known or recommended exclusions	
			f. Tool should include clauses to easily exclude false positives	
			g. Tool should provide the option for the administrators to make policy exclusions of the console at multiple levels? (Account, Group)	
			h. Provide exclusions set at process level	

		Device Control and Application Visibility	a. Tool to have the capability to control external USB media and fine tun policy to allow read only access	
			b. Tool should have the capability to control external Bluetooth devices	
			c. Solution should have granular USB and Device control to apply to a model, specific serial number or type of device.	
			d. Device control capabilities should be available on Mac, Linux and Windows	
			e. Solution should identify unpatched 3rd party software apps that may have vulnerabilities	
			f. The product must provide a software inventory for the environment	
		Firewall Control	a. The solution should provide Firewall Control	
			b. Single firewall rule should apply to multiply operating systems	
			c. Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups)	
		Integrations	a. The solution must Integrate with Active Directory for automatic Agent to Group Mappings and policy association.	
			b. The product should support grouping by Active Directory	
			c. The product should require AD configuration in order to have functionality with Active Directory	
			d. Active Directory should not require an agent to be installed on domain controllers for integration to work	
			e. Solution should be capable of identifying the following devices: Windows, Linux, Mac	
		Dashboards & Reporting	The Solution should have capability to report all known vulnerabilities in programs installed on an endpoint, along with export option.	
			Proposed solution should be able to monitor, log and block all application network activity	
			Once deployed, proposed solution should be able to scan, inventorize, categorize and list all applications running in the organization environment (including all running versions) for identification of any rogue applications	
			Proposed solution should be able to block all rogue applications from making a network	

			connection by way of an essential application whitelisting method.	
			Proposed solution should be able to monitor, log and block all browser/URL activities	
			Proposed solution should support pre-defined and categorized web/URL list as per industry standards.	
			Proposed solution should support additions, changes, removals or customization of web categorization lists.	
			Proposed system should support creation of custom web categorization Lists.	
			Proposed solution should enable blocking or allowing of web/URLs/IPs based on whitelisting or blacklisting approaches.	
			Proposed solution should present flexible deployment options for On-Premises server with support for DC and DR.	
			Proposed solution must support all required features to be handled by a single endpoint agent.	
			Proposed solution must perform all monitoring and block activities at the endpoint continuing to perform those actions irrespective of if user is connected to internal/private VPN network or offline (only blocking) and store the logs offline and send to the server once its connected back	
			All modules of the proposed solution must be centrally configurable from central management dashboards.	
			Proposed solution should be password protected from being uninstalled and should be tamper proof	
			Proposed solution should be able to implement temporary policies for uplifting the user privileges for a defined duration.	
			Proposed solution should support sub-admin accounts with different privileges/user groups/views and different user groups.	
			Proposed solution should support data export facility to SIEM Solutions.	
			Proposed solution should be capable of being deployed in stealth mode at the endpoints.	
			Proposed solution should offer a globally adjustable sync interval for policy and log synchronization	

			Proposed solution should support agent installation via manual or automated (silent/verbose) methods		
			Proposed solution console should in real time indicate agent connectivity status, last connected time and agent version		
			Proposed solution should support future agent update deployments via the console		
			Proposed solution should also support a CSV based Organization/Group/User Information imports and manual workgroup user creation		
			Proposed solution must support LDAP based authentication mapping for admins & sub-admin accounts		
			Proposed solution must have 2FA for administrator login and password enforcement for admin and sub-admin logins and automatic period-based password expiry		
			The solution should allow user to define a single set of policies once and deploy across all products		
			The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident		
			The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation and incident viewing for data at rest in motion or at the endpoint.		
			The unavailability of a management component/server in no way shall impact the functioning of a client.		
			Proposed solution should have dashboard notifications for each incident or violation.		
			Proposed solution incident summary dashboard should detail counts of each violation and a comparative analysis of previous period performance vis-a-vis present period performance.		
			Proposed solution should have an executive dashboard that summarizes overall organizational health scores and areas of concern		
			Proposed solution's executive dashboard should provide easy navigation and drill down capabilities to investigate areas of		

		concerns - department, region, zone to user level.		
		Proposed solution should be capable of filtering activity reports by user/or by device.		
		Proposed solution should also log and support audit of all admin and sub-admin activities		
		Proposed solution should support extraction of raw data logs or filtered reports via CSV/PDF formats		
		Proposed platform should be capable of generating alerts on any policy changes or agent uninstallation/ deletion performed by an admin or a sub-admin.		
		The solution should provide built-in reports and dashboards to analyze user behaviour and system health.		
		The solution should integrate with third-party reporting tools to provide meaningful reports on user activity and deployment.		
		The solution should be able to block outbound emails sent via SMTP if it violates the policy		
		The solution should provide a centralized, web-based administration console for classification, configuration and policy management.		
		The solution should support the ability to save configurations in a single configuration file irrespective of multiple AD group specific policies.		
		The solution should provide the ability to deploy in silent mode either natively or using third party software distribution tools so that software can be deployed and enabled in different phases.		
		Proposed solution should support Windows (7, 8.1, 10, 11), MacOS (Big Sur. Catalina, Monterey) and Linux OS (Ubuntu 18 L TS GUI and 20 L TS GUI) Desktop endpoints.		
		The unavailability of a management component server in no way shall impact the functioning of a client		
		The solution should provide flexibility to send user logs to SIEM, syslog server, text file and Windows event logs as per the need		
		The solution should be able to block booting operations in windows networking safe		

			mode. In windows normal safe mode, USB drives shall be blocked as well.		
			The proposed solution should be able to carry out deep level inspection in compressed files on the end points.		
			The proposed solution should be able to monitor and log user activities including access, modifications and transfers on the end points.		
		Anti-Virus Protection	a. Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.		
			b. Have the capability to detect all in-the-wild viruses		
			c. Must have the capability to detect and block files with malicious executable content and embedded/compressed executables that use real-time compression algorithms.		
			d. Must have the capability to detect and remove rootkits.		
			e. Must have the capability to detect and quarantine suspicious files.		
			f. Must have the capability to detect malware by behavioral detection techniques.		
			g. Must have the capability to detect and remove rogue wares.		
			h. Must have the capability to detect and block ransomware attacks.		
			i. Must have the Terminal service Protection Module		
			j. Must have the capability to backup and restore data so that in case of ransomware attack data can be easily retrieved.		
			k. Must have the capability to identify source of infection i.e. from where the infection has originated in the network.		
			l. Must have the capability to restore a file from quarantine if the file is deemed safe.		
			m. Must provide Virus Outbreak Prevention mechanism, which should be activated based on threshold of detected malware.		
			n. Should have anti malware protection and cleanup capability.		
			o. Ordinary Users should not be able to modify AV settings except for those in special groups as deemed necessary by the Administrators.		

			p. Update Managers: Should have the capability to create multiple update servers to distribute updates load in large network environment that reduce bandwidth consumed during definition updates.	
			q. Must have the capability to scan compressed, archived, and packed files.	
			r. Must have the capability to scan and disinfect infections from mobile phones.	
			s. Must have the capability to scan plug and play USB storage drives as soon as they are connected.	
			t. Must have the capability to terminate virus program threads in memory, repair registry, remove any malicious OS processes created by trojans.	
			u. Must have the capability to disconnect infected endpoints from the network.	
			v. Must have the capability to scan and repair OLE (Object Linking and Embedded) files.	
			w. Must have capability to disconnect endpoint from the network in case if virus/suspicious file is active in memory.	
			x. Must have the capability to exclude file types/extensions and folders from real-time scanning.	
			y. Must have provision to send Email Notification with list of unprotected systems in the network.	
			z. Must have the capability to specify file type to take critical data backup in case of ransomware attack.	
			Must have AV Test certification	
		Device Control	a. Must have the capability to grant allow, block, read-only access to various devices.	
			b. Must have the capability to grant access rights for storage devices such as USB, CD/DVD, Card Reader, Floppy Drive etc.	
			c. Must have the capability to regulate the use of Wi-Fi and Bluetooth connections.	
			d. Must have the capability to retain control over interfaces such as Firewire Bus, Serial Port, SATA Controller, Thunderbolt, etc.	
			e. Must have the capability to control and regulate the use of printers, scanners, web cameras, and network shares.	
			f. Must have the capability to exclude any particular device from device control policies.	

			g. Must have the capability to exclude any particular devices based on Model Name.	
			h. Must have the capability to encrypt USB Pen Drive contents and make it accessible only on endpoints where Endpoint Security client is installed.	
			i. Must have the capability to allow access of USB Pen drives temporarily to some authorized users using OTP	
			j. Must have the capability to completely block USB Interfaces to deny access to all USB devices (except Keyboard and Mouse and mass storage devices)	
			k. Must have the capability to support NTFS & FAT formatted devices for authorization.	
			l. Must have the capability to identify source of infection i.e. from where the infection has originated in the network.	
			m. Must have the capability to exclude USB devices based on serial number	
			n. Must have the capability to control USB Tethering from the connected devices	
			o. Must have the capability to alert USB Access Violations in near realtime	
		Vulnerability Scan	a. Must have capability to scan and report vulnerabilities present in installed applications.	
			b. Must have capability to schedule vulnerability scan periodically in order to get latest reports of vulnerabilities present in the network.	
		File Activity Monitoring	a. Must have the capability to monitor activities related to file handling such as copy, delete, move on local drives, removable drives and network drives.	
			b. Must have the capability to monitor certain file types.	
			c. Must have the capability to exclude certain files/folders/paths from monitoring procedures.	
		Asset Management	a. Must have the capability to collect system and hardware information related to remote endpoints.	
			b. Must have the capability to obtain a summary report of various software's/updates installed on endpoints.	
			c. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.	

			d. Must have the capability to display complete license key for Windows OS		
			e. Must have the capability to display license key for MS Office		
			f. Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.		
			g. Solution should have the capability to track hardware changes on system with automated notification to the administrator		
			h. Solution should have the capability to track software changes on system		
			i. Must have the capability to detect hardware changes on the clients and display the number of changes.		
			j. Must have the capability to detect software changes on the clients and display the number of changes.		
			k. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.		
			l. Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.		
		IDS/IPS	a. Must have the capability to detect, and prevent network based and host-based intruder attempts on the home networks.		
			b. Must have the capability to generate reports for potential security breaches, policy violations, and suspicious traffic flow.		
			c. Must have the capability to prevent port scanning attacks.		
			d. Must have the capability to prevent DDOS attacks.		
			e. Prevents unauthorized changes and detects anomalies in system behavior, files, or registries.		
		Web Security and Web Filtering	a. Must have the capability to block user access to malicious and phishing websites from configured endpoints.		
			b. Must have the capability to block user access to websites based on their categories e.g. Social Networking, News, etc.		

			c. Must have the capability to block entire domain or a particular website/URL	
			d. Must have provision to exclude certain websites or entire domains.	
			e. Must have the capability to block https sites.	
			f. Must have the capability to schedule internet access time.	
			g. Must have the capability to control default behavior for Unknown or yet to categorize Websites/URLs.	
			h. Controls and monitors inbound/outbound network traffic at the endpoint level.	
		Application Control	a. Must be able to block applications based on application categories. E.g. Download Managers, File sharing applications, Games, etc.	
			b. Must have ability to add custom applications to the blocked application list.	
			c. Provision to block applications based on application name.	
			d. Must have ability to create Safelist for Applications to be allowed on the Endpoints.	
			e. Must have ability to add manage Application Safelists	
		Firewall	a. Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.	
			b. Must have the capability to examine and control all incoming and outgoing traffic per configured settings for ports, source, or origin or destination address.	
			c. Must have the capability to monitor Wi-Fi Networks and send alerts when a client connects to unsecured Wi-Fi Network.	
			d. Provision to Allow/Dis-allow applications.	
		Email Protection	a. Must have the capability to block infected and spam mails.	
			b. Must have the functionality to sender policy framework	
			c. Must have the capability to block attachments in incoming emails having multiple extensions (ex -doc.exe).	
			d. Must have the capability to block emails which try to exploit vulnerabilities in the email client.	
			e. Must have the capability to block all or user specified attachments in incoming emails.	

		f. Must have provision for trusted email client configuration on Server	
	Groups and Policies	a. Must have the capability to create multiple user groups as per organizational structure.	
		b. Must have the capability to assign different policy configuration to each group.	
		c. Must have the capability for endpoints to synchronize with server.	
		d. Must have the capability to import group structure from Active Directory.	
		e. Must have the capability to import/export groups and policies.	
	Client Deployment	a. Must have the capability to deploy the Client software using the following mechanisms:	
		b. Client Packager (Executable & Microsoft Installer (MSI) Package Format)	
		c. Web install page	
		d. Login Script Setup	
		e. Remote installation on single endpoint or on entire IP range.	
		f. Through Active Directory and by creating group policy object	
		g. Client uninstallation should only be done by administrator.	
		h. Must have capability to create password protected client packager.	
		i. Must have provision to send Email Notification when any new endpoint security client is installed/uninstalled.	
		j. Must have capability to un-install previously installed Third Party (non Seqrite) Antivirus applications of most of the vendors from Endpoints as part of the installation	
	Server Deployment	a. Must have the facility to deploy the Endpoint Security Server on cloud-based servers on Microsoft Azure and AWS Platform	
		b. Must support installation of Endpoint Security server on dynamic (DHCP) IP address.	
		c. Must have the facility to deploy the Endpoint Security Server on Public IP/FQDN	
		d. Must have the facility to support two-tier Aggregator+Site Server deployment for increasing the limit to support more number of endpoints	

			e. Must have the ability to deploy Endpoint Security Server either on Microsoft Windows (OVA) or Linux Ubuntu OSs.	
			f. Must have the ability to deploy Site Servers in the High Availability (HA) Configuration	
		Management Features	a. Must provide a secure GUI or Web-based management console to give administrators access to all clients and servers on the network for client administration.	
			b. Must have the flexibility to roll back updates if required via the management console.	
			c. Should have role-based administration capability.	
			d. Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capability to clients and servers across the network	
			e. Must have provision for Self/Tamper Protection for Endpoint Security files/folders.	
			f. Group Administrator to manage certain groups and policies associated with the group.	
			g. Must support Multi Factor Authentication for administrators.	
		Notification, Reporting and Logging	a. Must have the capability to generate a graphical as well as tabular reports.	
			b. Must have capability to automatically purge old reports after a preconfigured duration.	
			c. Must have capability to log all activities of management server.	
			d. Must have capability to export reports in multiple formats such as PDF and CSV.	
			e. Must have capability to schedule report generation and distribution over email.	
			f. Must have capability to generate Host Integrity report showing compliant and non-compliant endpoints.	
			g. Must provide email notification for various critical events such as virus outbreak, ransomware incidents, license getting expired.etc	

			h. Must have provision to send Email Notification for status of update downloaded by Update Manager.	
			i. Must have capability to send Endpoint Reports to Security Information Event Manager (SIEM)	
			j. Must have capability to aggregate information at the aggregate server level from all the Sites when deployed in multi-site configuration	
		Roaming Client Management	a. Must have capability to configure policies for roaming clients even if it is out of network	
			b. Must have capability to get status, reports from roaming clients even if it is out of network	
			c. Must have capability to install/uninstall Endpoint Security Clients on endpoints which are outside the corporate network.	
			d. Must have capability to support all Windows, Mac, Linux endpoints in roaming configuration	
		Update Manager	a. Should have the capability to create multiple update servers to distribute updates load in large network environment that reduce bandwidth consumed during definition updates.	
			b. Must have the capability to schedule the frequency of downloading the updates.	
			c. Must have capability to allocate user-specified bandwidth to the Update Manager from the total available bandwidth.	
		Other Features	a. Must have the capability to prevent a user from accessing the operating system in safe mode.	
			b. Must have the capability to improve performance of endpoints by cleaning junk files and deleting invalid registry/disk entries.	
			c. Must have the capability to manage mobile workforce when they move out of the corporate network.	
			d. Must have capability to analyze suspicious files in the controlled environment viz. Sandbox	
			e. Must have the capability configure Full Disk Encryption on Endpoints with Windows OS	
			a. Must have the capability to Remote Monitoring Management functionality.	

	Remote Monitoring Management	b. Must have capability to provide complete access of system for troubleshooting.	
		c. Must have capability to provide functionality to Monitor user activity without knowing him.	
	MAC Features	a. Must offer comprehensive client security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.	
		b. Must have the capability to scan compressed, archived, and packed files.	
		c. Must have the capability to scan files with malicious executable content.	
		d. Must have the capability to prevent a user from accessing the operating system in safe mode.	
	Asset Management	a. Must have the capability to detect hardware changes on the clients and display the number of changes.	
		b. Must have the capability to detect software changes on the clients and display the number of changes.	
		c. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.	
		d. Must have the capability to track hardware changes happening on endpoints. E.g. RAM Changed, Processor changed, etc.	
		e. Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.	
	Advanced Device Control	a. Must have the capability to grant allow, block, read-only access to various devices.	
		b. Must have the capability to allow access of USB Pen drives temporarilty to some authorized users.	
	Client Deployment	a. Must have the capability to deploy the Client software using the following mechanisms:	
		b. Client Packager (DMG file format in a self-extracting TAR file)	
		c. Web install page	
		d. Remote installation on single endpoint or on entire IP range.	

		Roaming Client Management	a. Must have capability to configure policies for roaming clients even if it is out of network through cloud-based management platform.	
			b. Must have capability to get status, reports from roaming clients even if it is out of network through cloud-based management platform.	
		Linux Features	a. Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points	
			b. Must have the capability to scan external drives such as USB Storage, CD/DVD's	
			c. Must have the capability to define scan schedules for the clients.	
			d. Must have the capability to initiate scan remotely on clients.	
		Asset Management	a. Must have the capability to detect hardware changes on the clients and display the number of changes.	
			b. Must have the capability to detect software changes on the clients and display the number of changes.	
			c. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.	
			d. Must have the capability to track hardware changes happening on endpoints. E.g. RAM Changed, Processor changed, etc.	
			e.Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.	
		Advanced Device Control	Must have the capability to grant allow, block, access to various devices.	
		Client Deployment	Must have the capability to deploy the Client software using the following mechanisms:	
			a. Client Packager	
			b. Remote Deployment	
			c. Notify Installation	
		Web Security and Web Filtering	a. Must have the capability to block user access to malicious and phishing websites from configured endpoints.	

			b. Must have the capability to block user access to websites based on their categories e.g. Social Networking, News, etc.	
			c. Must have the capability to block entire domain or a particular website/URL.	
		Windows Platform Support	a. Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)	
			b. Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)	
			c. Microsoft Windows 2016 Server Edition	
			d. Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)	
			e. Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)	
			f. Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)	
			g. Microsoft Windows SBS 2011 Standard / Essentials	
			h. Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)	
			i. Microsoft Windows MultiPoint Server 2012 Standard (64-bit)	
			j. Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)	
			k. Microsoft Windows Server 2019 (64-bit)	
			l. Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit/64-Bit)	
			m. Microsoft Windows 11	
			n. Microsoft Windows Server 2022 Standard / Data Center / Essentials	
		MAC Platform Support	Mac OS X 10.9 to macOS Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13 and 14	
		Linux Platform Support	***Linux Platform Support - 32 Bit***	
			a. Debian 9, 10	
			b. Ubuntu 14.04,16.04	
			c. Boss 6.0	
			d. Linux Mint 19.3	
			Linux Platform Support - 64 Bit	
			a. Fedora 30, 32	
			b. Linux Mint 19.3, 20	
			c. Ubuntu 16.04, 18.04, 20.4, 22.04	
			d. Debian 9, 10	
			e. CentOS 7.8, 8.2	

		f. RHEL 7.5, 7.8, 8.2 & 8.6 Enterprise, 9.0, 9.1, 9.2, 9.3	
		g. SUSE Linux 12. SP4 / Enterprise Desktop 15	
		h. Rocky Linux 8.4	
		i. Boss 6.0, 8.0, 9.0	
		j. Oracle Linux 7.1, 7.9 and 8.1	
	Preferred Criterion	a. ISO 27001 & ISO 20000 certified Technical Support	
		b. The solution should consolidate EDR, EPP, and RMM functionalities into a single agent.	
		c. The centralized management console for the EDR solutions should be deployed on a dedicated single server.	
	BIDDER'S QUALIFICATIONS 1. The bidder must be an authorized partner of the Anti-Virus Solution. A Certification must be provided by the Manufacturer in the Technical Proposal. 2. The bidder must provide a Manufacturer's Authorization Form (MAF) addressed to the Procuring Entity. The MAF must be included in the Technical Proposal. 3. The bidder should have at least two (2) certified technical engineers for endpoint solution, with corresponding certificate. The certificate must be included in the Technical Proposal.		
	SUPPORT LEVEL AGREEMENT (SLA) 1. The winning bidder must provide 24/7 technical support through phone, email, and remote assistance to all PPA Offices (Head Office, Port Management Officers. & Terminals) for all issues related to the deployed security software. 2. All support requests must receive an initial response within four (4) hours. 3. If a critical issue is identified, onsite support must be available during regular business hours (8 hours per day, 5 days a week), and a technical engineer must be dispatched on the same day the issue is confirmed as critical or if the problem can't be solved remotely. (Head Office only)		

	4. Critical issues include, but are not limited to, system or service downtime, major security threats, and failures in the software that impact business operations. 5. The winning bidder must perform scheduled preventive maintenance twice a year, which includes system log checks, cleaning of devices if applicable, configuration backup, and overall software health assessment. 6. The bidder is responsible for advising and applying all relevant security patches, firmware updates, and software upgrades released by the vendor to address bugs or vulnerabilities. 7. If any issue is determined to be caused by a vendor-side problem such as a software bug, the bidder must coordinate directly with the solution vendor to resolve it and ensure that all necessary fixes are properly implemented. 8. The bidder must provide documentation including incident reports for critical issues, maintenance reports after each scheduled check-up, and update logs for all applied patches or software updates. 9. The winning bidder shall establish a Group Chat (e.g. Viber) including all PPA Technical Personnel nationwide to facilitate the prompt reporting of issues and concerns.	
	TRAINING 1. The winning bidder must provide free classroom training to fifteen (15) technical personnel of PPA on the installation, configuration, management, monitoring and maintenance of the solution. A Certificate of Completion must be provided after the training has been completed. 2. Submit the following documents • Training Syllabi and Materials • Installation, Troubleshooting, Monitoring and Management Procedure Manual. 3. The winning bidder shall shoulder all expenses (parking, venue, meals, etc.) during the training. 4. The winning bidder shall conduct one (1) online cybersecurity awareness and/or technical training session	

	annually for all PPA employees throughout the duration of the project.	
	All other provisions stated in the Terms of Reference not included herein.	

TERMS OF REFERENCE

Supply, Delivery and Installation of a Corporate Anti-Virus with Endpoint Detection and Response (EDR) for Three (3) Years at the PPA Head Office and Port Management Offices Nationwide.
ASD 126-2025

I. INTRODUCTION

This document has been provided to give the prospective bidder a general understanding of the requirements for the Supply, Delivery and Installation of a Corporate Anti-Virus with Endpoint Detection and Response (EDR) for Three (3) Years at the PPA Head Office and Port Management Offices nationwide.

II. OBJECTIVE

- To Protect PPA IT resources (desktops, servers and laptops), systems, and data against Cyber Threats such as viruses, malware, ransomware, and other security threats.
- To improve cost savings by preventing financial losses due to cyberattacks, data recovery, and reputational damage.
- To keep PPA IT resources (desktops, servers and laptops), systems, and data healthy by ensuring that both the software and the virus signature files are up to date.
- To avoid penalties imposed by the anti-virus vendors for usage of unrenewed/unlicensed software.
- To ensure that PPA complies with the requirements of Republic Act 8942 or the Intellectual Property Code of the Philippines.

III. SCOPE OF BID

- The bid proposal would be for the provision of **Four Thousand (4000)** licenses for PPA's Head Office and Project Management Offices' Desktop Computers, Servers and Laptops.

- Upgrade of the PPA's existing corporate Anti-Virus from Endpoint Protection to Endpoint Detection and Response (EDR).

- The proposal shall include the installation, setup and configuration of the Corporate Anti-Virus with EDR Client and Server at the Head Office and Remote Sites.

IV. SPECIFICATIONS

Bidders must be able to supply the Corporate Anti-Virus with EDR that meets the following technical specifications:

Technical Specification	
Endpoint Detection and Response (EDR)	
General Features	a. The solution should have all its components deployed on-premises
	b. Solution should NOT share any data of endpoints i.e. telemetry details in public cloud.
Management Console	a. The solution should provide a unified web-based console for all functionalities and should allow administrators to access the management interface from any authorized machine, without installing additional software.
	b. The solution should support multi-site configuration.
	c. The solution should provide the flexibility to have individual rules/policies for every group. The solution should also support policy inheritance from Account to Site to Group with the ability to break inheritance if required.
	d. Solution should provide a console easy to understand and to navigate with common workflows.
	e. The proposed solution must have the option to create role-based access/view(s) of the management console.
	f. Solution should support multi-factor authentication for the management console
	g. The solution should offer centralized auditing of incident response activities, accessible through the management console.
Agent Capabilities	a. The solution should deliver both Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities through a single agent, eliminating the need for multiple software installations. Additionally, all other security features—such as Firewall, Host Intrusion Prevention System (HIPS), Threat Intelligence, Device Control, Application Control, real-time analysis, and threat hunting—must also be integrated and accessible via the same unified agent.
	b. Solution should provide strong anti-tamper capabilities, to ensure that an end user can not remove, disable or modify the product in any way.
	c. Solution should have ability to trigger/schedule on-demand scans (from console and/or endpoint) to look for malware or ensure a threat has been remediated.
	d. Solution should have ability to upgrade agents with no impact to the end users.
	e. All the features of the solution should be functional even if license count is exceeded.
	f. Agent to be uninstalled remotely from the management console.
	g. Solution must allow to export device inventories.

	h. Deployed agents must be able to communicate with central management server via a web- proxy.
Operating System Support	a. Solution must support all supported versions of Operating Systems and should continue support for a minimum period of 12 months after the OS version is end of sale/life.
	b. EDR Solution must provide prevention across all major Operating Systems – Windows, MacOS and Linux.
	c. Solution must support all the latest versions of Windows Operating Systems. Following but not limited to: Windows Server Core 2016 and 2019, Windows Server 2022, 2019, 2016, 2012 R2, Windows 10, 11, 10, 8.1, 8, 7, Vista, XP SP2.
	d. Solution should support all the latest Linux environments CentOS, Debian, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server, Ubuntu and Mint.
	e. Solution should support all the new OS Updates/Versions within 60 days of release.
Threat Prevention	a. The proposed solution should offer context-aware Endpoint Detection and Response (EDR) capabilities, including comprehensive recording and detailed reporting of system-level activities. This will enable threat analysts to quickly assess the nature and extent of an attack. Additionally, the solution must support custom detection, threat intelligence integration, and advanced control mechanisms.
	b. Blocks attempts to exploit software or system vulnerabilities before they can be executed.
	c. EDR Solution must have capability to protect the system against known and unknown malwares.
	d. EDR solution should ensure that every read, write and execute operations on files is checked for malware
	e. Solution should be effective against sophisticated attacks by analyzing Behaviors on an endpoint, along with signature-based approach.
	f. The solution should incorporate robust mechanisms to protect endpoints from malware even in offline environments. The agent must operate in a fully autonomous manner, without dependency on a management server, cloud infrastructure, or any external resources. It should be capable of independently detecting and responding to advanced threats, including zero-day attacks, file-less malware, memory-based exploits, ransomware, crypto miners, lateral movement, and advanced persistent threats (APTs), in real time as they occur.
	g. EDR solution should leverage Artificial Intelligence or Machine Learning to analyze files pre-execution as well as analyze behaviors while a file is running.
	h. The solution should allow the user to perform threat hunting to detect dormant threats as well.
	i. The EDR solution should support protection capabilities across Windows, Mac, Linux

	j. Solution must provide prevention across ALL major Operating Systems – Windows, MacOS and Linux.
	k. The solution should protect endpoints from malicious documents and scripts.
	l. The solution should monitor and protect the system from lateral movements & insider threats.
	m. The EDR solution should monitor and protect from exploits and file-less attacks.
	n. The EDR solution should identify and block potentially unwanted programs on the systems.
	o. The solution should provide the flexibility to safely download malicious or convicted file from the management console
Response & Remediation Capabilities	a. The proposed solution should be able to perform threat sweeping based on the threat feeds (Files, URLs) or from intelligence received from the integrated on-premises sandbox solution.
	b. The proposed solution be able to perform sweeps across endpoints using rich search criteria
	c. The proposed solution will be able to Real time response on MITRE specific threat detection.
	d. The proposed solution should provide option to sweep and assess the current (point in time/Live) state of the devices.
	1. Scan disk Files
	2. Scan in memory process
	3. Search registry"
	e. The proposed solution to provide the advance response capabilities as mentioned below
	1. Kill process
	2. Isolate device
	3. Block process
	f. The proposed solution shall allow ingestion of IOCs (Indicators of compromise) like URLs, file-hashes and shall also allow blocking of the files/file-hashes
	g. The proposed solution can take risk-based response on the endpoint based on endpoint characteristics and reputation. The reputation of the endpoint is computed based on unusual or malicious behaviour of endpoint over time.
	h. The proposed solution provide remediation console which provide functionality to access end user systems process, services, Task Manager, Registry, Active connection, cmd, application in startup, Directory etc.
	i. Solution should detect and log all remote shell commands in a remote shell session.
	k. Solution should alert on both suspicious and malicious threat behavior.
	l. Solution should have ability to kill and quarantine an offending process.
	m. Solution should support backup and restoration of files in order to reverse destructive data events that occur during attacks such as ransomware attack.

	n. Solution should provide option to network quarantine a device and provide flexibility to configure the same.
	o. Threat response capabilities offered by the solution should be easily automated.
	p. Solution should provide a mechanism to take remedial actions on multiple systems at once.
Policy & Installation	a. Tool should provide Ability to support policy propagation across site or group of devices
	b. Tool should have the option to provide dynamic policy assignment based on device attributes
	c. Devices should be installed and placed directly into a specific device group at time of installation
	d. Policy modifications should be applied in near real time
	e. The product should have predefined list of known or recommended exclusions
	f. Tool should include clauses to easily exclude false positives
	g. Tool should provide the option for the administrators to make policy exclusions of the console at multiple levels? (Account, Group)
	h. Provide exclusions set at process level
Device Control and Application Visibility	a. Tool to have the capability to control external USB media and fine tun policy to allow read only access
	b. Tool should have the capability to control external Bluetooth devices
	c. Solution should have granular USB and Device control to apply to a model, specific serial number or type of device.
	d. Device control capabilities should be available on Mac, Linux and Windows
	e. Solution should identify unpatched 3rd party software apps that may have vulnerabilities
	f. The product must provide a software inventory for the environment
Firewall Control	a. The solution should provide Firewall Control
	b. Single firewall rule should apply to multiply operating systems
	c. Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups)
Integrations	a. The solution must Integrate with Active Directory for automatic Agent to Group Mappings and policy association.
	b. The product should support grouping by Active Directory
	c. The product should require AD configuration in order to have functionality with Active Directory
	d. Active Directory should not require an agent to be installed on domain controllers for integration to work
	e. Solution should be capable of identifying the following devices: Windows, Linux, Mac
Dashboards & Reporting	The Solution should have capability to report all known vulnerabilities in programs installed on an endpoint, along with export option.

	Proposed solution should be able to monitor, log and block all application network activity
	Once deployed, proposed solution should be able to scan, inventorize, categorize and list all applications running in the organization environment (including all running versions) for identification of any rogue applications
	Proposed solution should be able to block all rogue applications from making a network connection by way of an essential application whitelisting method.
	Proposed solution should be able to monitor, log and block all browser/URL activities
	Proposed solution should support pre-defined and categorized web/URL list as per industry standards.
	Proposed solution should support additions, changes, removals or customization of web categorization lists.
	Proposed system should support creation of custom web categorization Lists.
	Proposed solution should enable blocking or allowing of web/URLs/IPs based on whitelisting or blacklisting approaches.
	Proposed solution should present flexible deployment options for On-Premises server with support for DC and DR.
	Proposed solution must support all required features to be handled by a single endpoint agent.
	Proposed solution must perform all monitoring and block activities at the endpoint continuing to perform those actions irrespective of if user is connected to internal/private VPN network or offline (only blocking) and store the logs offline and send to the server once its connected back
	All modules of the proposed solution must be centrally configurable from central management dashboards.
	Proposed solution should be password protected from being uninstalled and should be tamper proof
	Proposed solution should be able to implement temporary policies for uplifting the user privileges for a defined duration.
	Proposed solution should support sub-admin accounts with different privileges/user groups/views and different user groups.
	Proposed solution should support data export facility to SIEM Solutions.
	Proposed solution should be capable of being deployed in stealth mode at the endpoints.
	Proposed solution should offer a globally adjustable sync interval for policy and log synchronization
	Proposed solution should support agent installation via manual or automated (silent/verbose) methods
	Proposed solution console should in real time indicate agent connectivity status, last connected time and agent version
	Proposed solution should support future agent update deployments via the console

	Proposed solution should also support a CSV based Organization/Group/User Information imports and manual workgroup user creation
	Proposed solution must support LDAP based authentication mapping for admins & sub-admin accounts
	Proposed solution must have 2FA for administrator login and password enforcement for admin and sub-admin logins and automatic period-based password expiry
	The solution should allow user to define a single set of policies once and deploy across all products
	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident
	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation and incident viewing for data at rest in motion or at the endpoint.
	The unavailability of a management component/server in no way shall impact the functioning of a client.
	Proposed solution should have dashboard notifications for each incident or violation.
	Proposed solution incident summary dashboard should detail counts of each violation and a comparative analysis of previous period performance vis-a-vis present period performance.
	Proposed solution should have an executive dashboard that summarizes overall organizational health scores and areas of concern
	Proposed solution's executive dashboard should provide easy navigation and drill down capabilities to investigate areas of concerns - department, region, zone to user level.
	Proposed solution should be capable of filtering activity reports by user/or by device.
	Proposed solution should also log and support audit of all admin and sub-admin activities
	Proposed solution should support extraction of raw data logs or filtered reports via CSV/PDF formats
	Proposed platform should be capable of generating alerts on any policy changes or agent uninstallation/ deletion performed by an admin or a sub-admin.
	The solution should provide built-in reports and dashboards to analyze user behaviour and system health.
	The solution should integrate with third-party reporting tools to provide meaningful reports on user activity and deployment.
	The solution should be able to block outbound emails sent via SMTP if it violates the policy
	The solution should provide a centralized, web-based administration console for classification, configuration and policy management.

	The solution should support the ability to save configurations in a single configuration file irrespective of multiple AD group specific policies.
	The solution should provide the ability to deploy in silent mode either natively or using third party software distribution tools so that software can be deployed and enabled in different phases.
	Proposed solution should support Windows (7, 8.1, 10, 11), MacOS (Big Sur. Catalina, Monterey) and Linux OS (Ubuntu 18 L TS GUI and 20 L TS GUI) Desktop endpoints.
	The unavailability of a management component server in no way shall impact the functioning of a client
	The solution should provide flexibility to send user logs to SIEM, syslog server, text file and Windows event logs as per the need
	The solution should be able to block booting operations in windows networking safe mode. In windows normal safe mode, USB drives shall be blocked as well.
	The proposed solution should be able to carry out deep level inspection in compressed files on the end points.
	The proposed solution should be able to monitor and log user activities including access, modifications and transfers on the end points.
Anti-Virus Protection	a. Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.
	b. Have the capability to detect all in-the-wild viruses
	c. Must have the capability to detect and block files with malicious executable content and embedded/compressed executables that use real-time compression algorithms.
	d. Must have the capability to detect and remove rootkits.
	e. Must have the capability to detect and quarantine suspicious files.
	f. Must have the capability to detect malware by behavioral detection techniques.
	g. Must have the capability to detect and remove rogue wares.
	h. Must have the capability to detect and block ransomware attacks.
	i. Must have the Terminal service Protection Module
	j. Must have the capability to backup and restore data so that in case of ransomware attack data can be easily retrieved.
	k. Must have the capability to identify source of infection i.e. from where the infection has originated in the network.
	l. Must have the capability to restore a file from quarantine if the file is deemed safe.
	m. Must provide Virus Outbreak Prevention mechanism, which should be activated based on threshold of detected malware.
	n. Should have anti malware protection and cleanup capability.
	o. Ordinary Users should not be able to modify AV settings except for those in special groups as deemed necessary by the Administrators.

	p. Update Managers: Should have the capability to create multiple update servers to distribute updates load in large network environment that reduce bandwidth consumed during definition updates.
	q. Must have the capability to scan compressed, archived, and packed files.
	r. Must have the capability to scan and disinfect infections from mobile phones.
	s. Must have the capability to scan plug and play USB storage drives as soon as they are connected.
	t. Must have the capability to terminate virus program threads in memory, repair registry, remove any malicious OS processes created by trojans.
	u. Must have the capability to disconnect infected endpoints from the network.
	v. Must have the capability to scan and repair OLE (Object Linking and Embedded) files.
	w. Must have capability to disconnect endpoint from the network in case if virus/suspicious file is active in memory.
	x. Must have the capability to exclude file types/extensions and folders from real-time scanning.
	y. Must have provision to send Email Notification with list of unprotected systems in the network.
	z. Must have the capability to specify file type to take critical data backup in case of ransomware attack.
	Must have AV Test certification
Device Control	a. Must have the capability to grant allow, block, read-only access to various devices.
	b. Must have the capability to grant access rights for storage devices such as USB, CD/DVD, Card Reader, Floppy Drive etc.
	c. Must have the capability to regulate the use of Wi-Fi and Bluetooth connections.
	d. Must have the capability to retain control over interfaces such as Firewire Bus, Serial Port, SATA Controller, Thunderbolt, etc.
	e. Must have the capability to control and regulate the use of printers, scanners, web cameras, and network shares.
	f. Must have the capability to exclude any particular device from device control policies.
	g. Must have the capability to exclude any particular devices based on Model Name.
	h. Must have the capability to encrypt USB Pen Drive contents and make it accessible only on endpoints where Endpoint Security client is installed.
	i. Must have the capability to allow access of USB Pen drives temporarily to some authorized users using OTP
	j. Must have the capability to completely block USB Interfaces to deny access to all USB devices (except Keyboard and Mouse and mass storage devices)

	k. Must have the capability to support NTFS & FAT formatted devices for authorization.
	l. Must have the capability to identify source of infection i.e. from where the infection has originated in the network.
	m. Must have the capability to exclude USB devices based on serial number
	n. Must have the capability to control USB Tethering from the connected devices
	o. Must have the capability to alert USB Access Violations in near realtime
Vulnerability Scan	a. Must have capability to scan and report vulnerabilities present in installed applications.
	b. Must have capability to schedule vulnerability scan periodically in order to get latest reports of vulnerabilities present in the network.
File Activity Monitoring	a. Must have the capability to monitor activities related to file handling such as copy, delete, move on local drives, removable drives and network drives.
	b. Must have the capability to monitor certain file types.
	c. Must have the capability to exclude certain files/folders/paths from monitoring procedures.
Asset Management	a. Must have the capability to collect system and hardware information related to remote endpoints.
	b. Must have the capability to obtain a summary report of various software's/updates installed on endpoints.
	c. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.
	d. Must have the capability to display complete license key for Windows OS
	e. Must have the capability to display license key for MS Office
	f. Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.
	g. Solution should have the capability to track hardware changes on system with automated notification to the administrator
	h. Solution should have the capability to track software changes on system
	i. Must have the capability to detect hardware changes on the clients and display the number of changes.
	j. Must have the capability to detect software changes on the clients and display the number of changes.
	k. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.
	l. Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.
IDS/IPS	a. Must have the capability to detect, and prevent network based and host-based intruder attempts on the home networks.

	b. Must have the capability to generate reports for potential security breaches, policy violations, and suspicious traffic flow.
	c. Must have the capability to prevent port scanning attacks.
	d. Must have the capability to prevent DDOS attacks.
	e. Prevents unauthorized changes and detects anomalies in system behavior, files, or registries.
Web Security and Web Filtering	a. Must have the capability to block user access to malicious and phishing websites from configured endpoints.
	b. Must have the capability to block user access to websites based on their categories e.g. Social Networking, News, etc.
	c. Must have the capability to block entire domain or a particular website/URL
	d. Must have provision to exclude certain websites or entire domains.
	e. Must have the capability to block https sites.
	f. Must have the capability to schedule internet access time.
	g. Must have the capability to control default behavior for Unknown or yet to categorize Websites/URLs.
	h. Controls and monitors inbound/outbound network traffic at the endpoint level.
Application Control	a. Must be able to block applications based on application categories. E.g. Download Managers, File sharing applications, Games, etc.
	b. Must have ability to add custom applications to the blocked application list.
	c. Provision to block applications based on application name.
	d. Must have ability to create Safelist for Applications to be allowed on the Endpoints.
	e. Must have ability to add manage Application Safelists
Firewall	a. Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.
	b. Must have the capability to examine and control all incoming and outgoing traffic per configured settings for ports, source, or origin or destination address.
	c. Must have the capability to monitor Wi-Fi Networks and send alerts when a client connects to unsecured Wi-Fi Network.
	d. Provision to Allow/Dis-allow applications.
Email Protection	a. Must have the capability to block infected and spam mails.
	b. Must have the functionality to sender policy framework
	c. Must have the capability to block attachments in incoming emails having multiple extensions (ex -doc.exe).
	d. Must have the capability to block emails which try to exploit vulnerabilities in the email client.
	e. Must have the capability to block all or user specified attachments in incoming emails.

	f. Must have provision for trusted email client configuration on Server
Groups and Policies	a. Must have the capability to create multiple user groups as per organizational structure.
	b. Must have the capability to assign different policy configuration to each group.
	c. Must have the capability for endpoints to synchronize with server.
	d. Must have the capability to import group structure from Active Directory.
	e. Must have the capability to import/export groups and policies.
Client Deployment	a. Must have the capability to deploy the Client software using the following mechanisms:
	b. Client Packager (Executable & Microsoft Installer (MSI) Package Format)
	c. Web install page
	d. Login Script Setup
	e. Remote installation on single endpoint or on entire IP range.
	f. Through Active Directory and by creating group policy object
	g. Client uninstallation should only be done by administrator.
	h. Must have capability to create password protected client packager.
	i. Must have provision to send Email Notification when any new endpoint security client is installed/uninstalled.
	j. Must have capability to un-install previously installed Third Party (non Seqrite) Antivirus applications of most of the vendors from Endpoints as part of the installation
Server Deployment	a. Must have the facility to deploy the Endpoint Security Server on cloud-based servers on Microsoft Azure and AWS Platform
	b. Must support installation of Endpoint Security server on dynamic (DHCP) IP address.
	c. Must have the facility to deploy the Endpoint Security Server on Public IP/FQDN
	d. Must have the facility to support two-tier Aggregator+Site Server deployment for increasing the limit to support more number of endpoints
	e. Must have the ability to deploy Endpoint Security Server either on Microsoft Windows (OVA) or Linux Ubuntu OSs.
	f. Must have the ability to deploy Site Servers in the High Availability (HA) Configuration
Management Features	a. Must provide a secure GUI or Web-based management console to give administrators access to all clients and servers on the network for client administration.
	b. Must have the flexibility to roll back updates if required via the management console.
	c. Should have role-based administration capability.
	d. Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and

	time needed to deploy new security capability to clients and servers across the network
	e. Must have provision for Self/Tamper Protection for Endpoint Security files/folders.
	f. Group Administrator to manage certain groups and policies associated with the group.
	g. Must support Multi Factor Authentication for administrators.
Notification, Reporting and Logging	a. Must have the capability to generate a graphical as well as tabular reports.
	b. Must have capability to automatically purge old reports after a preconfigured duration.
	c. Must have capability to log all activities of management server.
	d. Must have capability to export reports in multiple formats such as PDF and CSV.
	e. Must have capability to schedule report generation and distribution over email.
	f. Must have capability to generate Host Integrity report showing compliant and non- compliant endpoints.
	g. Must provide email notification for various critical events such as virus outbreak, ransomware incidents, license getting expired.etc
	h. Must have provision to send Email Notification for status of update downloaded by Update Manager.
	i. Must have capability to send Endpoint Reports to Security Information Event Manager (SIEM)
	j. Must have capability to aggregate information at the aggregate server level from all the Sites when deployed in multi-site configuration
Roaming Client Management	a. Must have capability to configure policies for roaming clients even if it is out of network
	b. Must have capability to get status, reports from roaming clients even if it is out of network
	c. Must have capability to install/uninstall Endpoint Security Clients on endpoints which are outside the corporate network.
	d. Must have capability to support all Windows, Mac, Linux endpoints in roaming configuration
Update Manager	a. Should have the capability to create multiple update servers to distribute updates load in large network environment that reduce bandwidth consumed during definition updates.
	b. Must have the capability to schedule the frequency of downloading the updates.
	c. Must have capability to allocate user-specified bandwidth to the Update Manager from the total available bandwidth.
Other Features	a. Must have the capability to prevent a user from accessing the operating system in safe mode.
	b. Must have the capability to improve performance of endpoints by cleaning junk files and deleting invalid registry/disk entries.

	c. Must have the capability to manage mobile workforce when they move out of the corporate network.
	d. Must have capability to analyze suspicious files in the controlled environment viz. Sandbox
	e. Must have the capability configure Full Disk Encryption on Endpoints with Windows OS
Remote Monitoring Management	a. Must have the capability to Remote Monitoring Management functionality.
	b. Must have capability to provide complete access of system for troubleshooting.
	c. Must have capability to provide functionality to Monitor user activity without knowing him.
MAC Features	a. Must offer comprehensive client security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.
	b. Must have the capability to scan compressed, archived, and packed files.
	c. Must have the capability to scan files with malicious executable content.
	d. Must have the capability to prevent a user from accessing the operating system in safe mode.
Asset Management	a. Must have the capability to detect hardware changes on the clients and display the number of changes.
	b. Must have the capability to detect software changes on the clients and display the number of changes.
	c. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.
	d. Must have the capability to track hardware changes happening on endpoints. E.g. RAM Changed, Processor changed, etc.
	e. Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.
Advanced Device Control	a. Must have the capability to grant allow, block, read-only access to various devices.
	b. Must have the capability to allow access of USB Pen drives temporarilty to some authorized users.
Client Deployment	a. Must have the capability to deploy the Client software using the following mechanisms:
	b. Client Packager (DMG file format in a self-extracting TAR file)
	c. Web install page
	d. Remote installation on single endpoint or on entire IP range.
Roaming Client Management	a. Must have capability to configure policies for roaming clients even if it is out of network through cloud-based management platform.
	b. Must have capability to get status, reports from roaming clients even if it is out of network through cloud-based management platform.

Linux Features	a. Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points
	b. Must have the capability to scan external drives such as USB Storage, CD/DVD's
	c. Must have the capability to define scan schedules for the clients.
	d. Must have the capability to initiate scan remotely on clients.
Asset Management	a. Must have the capability to detect hardware changes on the clients and display the number of changes.
	b. Must have the capability to detect software changes on the clients and display the number of changes.
	c. Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.
	d. Must have the capability to track hardware changes happening on endpoints. E.g. RAM Changed, Processor changed, etc.
	e.Must provide comprehensive asset management reports based on following parameters: Operating System, Application Name, System Manufacturer, Installed Physical RAM, Processor and Last Shutdown time.
Advanced Device Control	Must have the capability to grant allow, block, access to various devices.
Client Deployment	Must have the capability to deploy the Client software using the following mechanisms:
	a. Client Packager
	b. Remote Deployment
	c. Notify Installation
Web Security and Web Filtering	a. Must have the capability to block user access to malicious and phishing websites from configured endpoints.
	b. Must have the capability to block user access to websites based on their categories e.g. Social Networking, News, etc.
	c. Must have the capability to block entire domain or a particular website/URL.
Windows Platform Support	a. Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
	b. Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
	c. Microsoft Windows 2016 Server Edition
	d. Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
	e. Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
	f. Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
	g. Microsoft Windows SBS 2011 Standard / Essentials
	h. Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
	i. Microsoft Windows MultiPoint Server 2012 Standard (64-bit)

	j. Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
	k. Microsoft Windows Server 2019 (64-bit)
	l. Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit/64-Bit)
	m. Microsoft Windows 11
	n. Microsoft Windows Server 2022 Standard / Data Center / Essentials
MAC Platform Support	Mac OS X 10.9 to macOS Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13 and 14
Linux Platform Support	***Linux Platform Support - 32 Bit***
	a. Debian 9, 10
	b. Ubuntu 14.04,16.04
	c. Boss 6.0
	d. Linux Mint 19.3
	Linux Platform Support - 64 Bit
	a. Fedora 30, 32
	b. Linux Mint 19.3, 20
	c. Ubuntu 16.04, 18.04, 20.4, 22.04
	d. Debian 9, 10
	e. CentOS 7.8, 8.2
	f. RHEL 7.5, 7.8, 8.2 & 8.6 Enterprise, 9.0, 9.1, 9.2, 9.3
	g. SUSE Linux 12. SP4 / Enterprise Desktop 15
	h. Rocky Linux 8.4
	i. Boss 6.0, 8.0, 9.0
	j. Oracle Linux 7.1, 7.9 and 8.1
Preferred Criterion	a. ISO 27001 & ISO 20000 certified Technical Support
	b. The solution should consolidate EDR, EPP, and RMM functionalities into a single agent.
	c. The centralized management console for the EDR solutions should be deployed on a dedicated single server.

V. BIDDER'S QUALIFICATIONS

1. Must have completed a single contract similar to the contract to be bid whose value must be at least equivalent to fifty percent (50%) of the ABC. For this purpose, a comparable contract or one with similar terminology, such as "Supply, Delivery, and Installation of Any Software Subscriptions.

2. The bidder must be an authorized partner of the Anti-Virus Solution. A Certification must be provided by the Manufacturer in the Technical Proposal.

3. The bidder must provide a Manufacturer's Authorization Form (MAF) addressed to the Procuring Entity. The MAF must be included in the Technical Proposal.

4. The bidder should have at least two (2) certified technical engineers for endpoint solution, with corresponding certificate. The certificate must be included in the Technical Proposal.

VI. SUPPORT LEVEL AGREEMENT (SLA)

1. The winning bidder must provide 24/7 technical support through phone, email, and remote assistance to all PPA Offices (Head Office, Port Management Officers. & Terminals) for all issues related to the deployed security software.
2. All support requests must receive an initial response within four (4) hours.
3. If a critical issue is identified, onsite support must be available during regular business hours (8 hours per day, 5 days a week), and a technical engineer must be dispatched on the same day the issue is confirmed as critical or if the problem can't be solved remotely. (Head Office only)
4. Critical issues include, but are not limited to, system or service downtime, major security threats, and failures in the software that impact business operations.
5. The winning bidder must perform scheduled preventive maintenance twice a year, which includes system log checks, cleaning of devices if applicable, configuration backup, and overall software health assessment.
6. The bidder is responsible for advising and applying all relevant security patches, firmware updates, and software upgrades released by the vendor to address bugs or vulnerabilities.
7. If any issue is determined to be caused by a vendor-side problem such as a software bug, the bidder must coordinate directly with the solution vendor to resolve it and ensure that all necessary fixes are properly implemented.
8. The bidder must provide documentation including incident reports for critical issues, maintenance reports after each scheduled check-up, and update logs for all applied patches or software updates.
9. The winning bidder shall establish a Group Chat (e.g. Viber) including all PPA Technical Personnel nationwide to facilitate the prompt reporting of issues and concerns.

VII. TRAINING

1. The winning bidder must provide free classroom training to fifteen (15) technical personnel of PPA on the installation, configuration, management, monitoring and maintenance of the solution. A Certificate of Completion must be provided after the training has been completed.

2. Submit the following documents

    - Training Syllabi and Materials
    - Installation, Troubleshooting, Monitoring and Management Procedure Manual.

3. The winning bidder shall shoulder all expenses (parking. venue. meals. etc.) during the training.

4. The winning bidder shall conduct one (1) online cybersecurity awareness and/or technical training session annually for all PPA employees throughout the duration of the project.

VIII. APPROVED BUDGET

The Approved Budget for the Contract is **Thirty Million and Five Hundred Thousand Pesos (30,500,000.00)** inclusive of 12% VAT.

IX. DELIVERY AND PAYMENT

The Corporate Anti-Virus with EDR should be installed and configured, and accepted within ninety (90) days upon receipt of Notice of Proceed (NTP).

The license and support period of three (3) years shall commence upon issuance of the Certificate of Acceptance by the end-user.

Payment shall be made upon issuance of Certificate of Acceptance by the end-user.

WILFRED THOMAS B. GORRE
Acting Manager
Information and Communications Technology Department

Section VIII. Checklist of Technical and Financial Documents

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

☐ (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages) in accordance with Section 8.5.2 of the IRR;

Technical Documents

☐ (b) Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; **and**

☐ (c) Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 revised IRR of RA No. 9184, within the relevant period as provided in the Bidding Documents; **and**

☐ (d) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;
Or

Original copy of Notarized Bid Securing Declaration; **and**

☐ (e) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, if applicable; **and**

☐ (f) Original duly signed Omnibus Sworn Statement (OSS); **and** if applicable, Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; 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

☐ (g) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);
or
A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

Class "B" Documents

☐ (h) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;
or

duly notarized statements from all the potential joint venture partners stating the following:

a. that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful; and

b. failure to enter into JVA in the event of a contract award shall be a ground for bid disqualification and subsequent forfeiture of the bid security.

Other documentary requirements under RA No. 9184 (as applicable)

☐ (i) *[For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos]* Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.

☐ (j) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

II. FINANCIAL COMPONENT ENVELOPE

☐ (a) Original of duly signed and accomplished Financial Bid Form; **and**

☐ (b) Original of duly signed and accomplished Price Schedule(s).

BID FORM

Date : _____
Project Identification No. : _____

To: [name and address of Procuring Entity]

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers [insert numbers], the receipt of which is hereby duly acknowledged, we, the undersigned, offer to [supply/deliver/perform] [description of the Goods] in conformity with the said PBDs for the sum of [total Bid amount in words and figures] or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: [specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties], which are itemized herein or in the Price Schedules,

If our Bid is accepted, we undertake:

a. to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);

b. to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;

c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements pursuant to the PBDs.

The undersigned is authorized to submit the bid on behalf of [name of the bidder] as evidenced by the attached [state the written authority].

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Name: _____
Legal capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

Price Schedule for Goods Offered from Abroad
[shall be submitted with the Bid if bidder is offering goods from Abroad]

For Goods Offered from Abroad

Name of Bidder _____ Project ID No._____ Page ___ of ___

1	2	3	4	5	6	7	8	9
Item	Description	Country of origin	Quantity	Unit price CIF port of entry (specify port) or CIP named place (specify border point or place of destination)	Total CIF or CIP price per item (col. 4 x 5)	Unit Price Delivered Duty Unpaid (DDU)	Unit price Delivered Duty Paid (DDP)	Total Price delivered DDP (col 4 x 8)

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Price Schedule for Goods Offered from Within the Philippines
[shall be submitted with the Bid if bidder is offering goods from within the Philippines]

For Goods Offered from Within the Philippines

Name of Bidder _____ Project ID No._____ Page ___of___

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of origin	Quantity	Unit price EXW per item	Transportation and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Bid Securing Declaration Form
[shall be submitted with the Bid if bidder opts to provide this form of bid security]

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

BID SECURING DECLARATION
Project Identification No.: [Insert number]

To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid Securing Declaration.

2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f),of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.

3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:

   a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
   b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and
   c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Contract Agreement Form for the Procurement of Goods (Revised)
[Not required to be submitted with the Bid, but it shall be submitted within ten (10) days after receiving the Notice of Award]

CONTRACT AGREEMENT

THIS AGREEMENT made the _____ day of _____ 20_____ between [name of PROCURING ENTITY] of the Philippines (hereinafter called "the Entity") of the one part and [name of Supplier] of [city and country of Supplier] (hereinafter called "the Supplier") of the other part;

WHEREAS, the Entity invited Bids for certain goods and ancillary services, particularly [brief description of goods and services] and has accepted a Bid by the Supplier for the supply of those goods and services in the sum of [contract price in words and figures in specified currency] (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents as required by the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of this Agreement, viz.:

    i. Philippine Bidding Documents (PBDs);
        i. Schedule of Requirements;
        ii. Technical Specifications;
        iii. General and Special Conditions of Contract; and
        iv. Supplemental or Bid Bulletins, if any

    ii. Winning bidder's bid, including the Eligibility requirements, Technical and Financial Proposals, and all other documents or statements submitted;

        Bid form, including all the documents/statements contained in the Bidder's bidding envelopes, as annexes, and all other documents submitted (e.g., Bidder's response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;

    iii. Performance Security;

    iv. Notice of Award of Contract; and the Bidder's conforme thereto; and

    v. Other contract documents that may be required by existing laws and/or the Procuring Entity concerned in the PBDs. Winning bidder agrees that additional contract documents or information prescribed by the GPPB that are subsequently required for submission after the contract execution, such

as the Notice to Proceed, Variation Orders, and Warranty Security, shall likewise form part of the Contract.

3. In consideration for the sum of [total contract price in words and figures] or such other sums as may be ascertained, [Named of the bidder] agrees to [state the object of the contract] in accordance with his/her/its Bid.

4. The [Name of the procuring entity] agrees to pay the above-mentioned sum in accordance with the terms of the Bidding.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.

[Insert Name and Signature]	[Insert Name and Signature]
[Insert Signatory's Legal Capacity]	[Insert Signatory's Legal Capacity]
for:	for:
[Insert Procuring Entity]	[Insert Name of Supplier]

Acknowledgment
[Format shall be based on the latest Rules on Notarial Practice]

Omnibus Sworn Statement (Revised)
[shall be submitted with the Bid]

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. [Select one, delete the other:]

   [If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

   If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. [Select one, delete the other:]

   [If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

   [If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable;)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. [Select one, delete the rest:]

   [If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, Procurement Agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a partnership or cooperative:] None of the officers and members of [Name of Bidder] is related to the Head of the Procuring Entity, Procurement Agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of [Name of Bidder] is related to the Head of the Procuring Entity, Procurement Agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. [Name of Bidder] complies with existing labor laws and standards; and

8. [Name of Bidder] is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:

   a. Carefully examining all of the Bidding Documents;

   b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;

   c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and

   d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the [Name of the Project].

9. [Name of Bidder] did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any

payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 20__ at _____, Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Performance Securing Declaration (Revised)
[if used as an alternative performance security but it is not required to be submitted with the Bid, as it shall be submitted within ten (10) days after receiving the Notice of Award]

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

PERFORMANCE SECURING DECLARATION

Invitation to Bid: [Insert Reference Number indicated in the Bidding Documents]

To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, to guarantee the faithful performance by the supplier/distributor/manufacturer/contractor/consultant of its obligations under the Contract, I/we shall submit a Performance Securing Declaration within a maximum period of ten (10) calendar days from the receipt of the Notice of Award prior to the signing of the Contract.

2. I/We accept that: I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of one (1) year for the first offense, or two (2) years for the second offense, upon receipt of your Blacklisting Order if I/We have violated my/our obligations under the Contract;

3. I/We understand that this Performance Securing Declaration shall cease to be valid upon:

    a. issuance by the Procuring Entity of the Certificate of Final Acceptance, subject to the following conditions:
        i. Procuring Entity has no claims filed against the contract awardee;
        ii. It has no claims for labor and materials filed against the contractor; and
        iii. Other terms of the contract; or

    b. replacement by the winning bidder of the submitted PSD with a performance security in any of the prescribed forms under Section 39.2 of the 2016 revised IRR of RA No. 9184 as required by the end-user.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

NET FINANCIAL CONTRACTING CAPACITY (NFFC) COMPUTATION

A. The values of the bidder's current assets and current liabilities shall be based on the data submitted to the BIR, through its Electronic Filing and Payment System (EFPS).

		Year 20__
1.	Total Assets	
2.	Current Assets	
3.	Total Liabilities	
4.	Current Liabilities	
5.	Net Worth (1-3)	
6.	Net Working Capital (2-4)	

B. The Net Financial Contracting Capacity (NFCC) based on the above data is computed as follows:

NFCC = [(Current asset minus current liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started, coinciding with the contract to be bid

NFCC = Php _____

K = 15

Herewith attached are certified true copies of the income tax return and audited financial statement: stamped "RECEIVED" by the BIR or BIR authorized collecting agent for the immediately preceding year.

Submitted by:

_____
Name of Supplier/Distributor/Manufacturer

_____
Signature of Authorized Representative

STATEMENT OF THE BIDDER'S ONGOING GOVERNMENT AND PRIVATE CONTRACTS, INCLUDING CONTRACTS AWARDED BUT NOT YET STARTED

This is to certify that _____ has the following ongoing government and private contracts, including contracts awarded but not yet started:

NAME OF THE CONTRACT	DATE OF THE CONTRACT	CONTRACT DURATION	OWNER'S NAME & ADDRESS	KINDS OF GOODS/SERVICES DELIVERED	AMOUNT OF CONTRACT	VALUE OF OUTSTANDING CONTRACT	DATE OF DELIVERY

*PROOF OF CONTRACT TO BE PRESENTED AT POST-QUALIFICATION.

_____ _____

Name and Signature of Authorized Representative Date

STATEMENT OF THE BIDDER'S SINGLE LARGEST COMPLETED CONTRACT (SLCC) SIMILAR TO THE CONTRACT TO BE BID

This is to certify that _____ has completed the following:

NAME OF THE CONTRACT	DATE OF THE CONTRACT	CONTRACT DURATION	OWNER'S NAME & ADDRESS	KINDS OF GOODS	AMOUNT OF COMPLETED CONTRACT/S	DATE OF DELIVERY	END USER'S ACCEPTANCE OR OFFICIAL RECEIPT(S) OR SALES INVOICE ISSUED FOR THE CONTRACT*

*TO BE ATTACHED TO THE STATEMENT

_____
Name and Signature of Authorized Representative

_____
Date