PHILIPPINE BIDDING DOCUMENTS

Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution

Government of the Republic of the Philippines

Bidding No. 20-021
28 October 2020

Table of Contents

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.

Section I. Invitation to Bid

Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution

1. The Department of Trade and Industry, through the General Appropriation Act for CY 2020 and/or continuing appropriations intends to apply the sum of **Eight Million Pesos (PhP8,000,000.00)** being the ABC to payments under the contract for the **Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution (Bidding No. 20-021)**. Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The Department of Trade and Industry now invites bids for the above Procurement Project. Delivery of the Goods is required by within **thirty (30) calendar days**. Bidders should have completed, within **three (3) 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).

3. Bidding will be conducted through open competitive bidding procedures using a non- discretionary "*pass/fail*" criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.

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

4. Prospective Bidders may obtain further information from Department of Trade and Industry and inspect the Bidding Documents at the address given below during office hours from 8 AM to 5 PM, Monday to Friday.

5. A complete set of Bidding Documents may be acquired by interested Bidders on **29 October 2020** 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 **Ten Thousand Pesos (PhP10,000.00)**. The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person or via electronic mail.

6. The Department of Trade and Industry will hold a Pre-Bid Conference on **05 November 2020, 9:30AM** through video conferencing or webcasting via Zoom, which shall be open to prospective bidders. Zoom Meeting link is contained in Section III (Bid Data Sheet).

7. Bids must be duly received by the BAC Secretariat through (i) manual submission at the office address indicated below, (ii) online or electronic submission as indicated below, or (iii) both on or before **9 AM of 18 November 2020**. Late bids shall not be accepted.

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

9. Bid opening shall be on **18 November 2020, 9:30AM** at the Center Conference Room, Trade & Industry Building, 361 Sen. Gil Puyat Avenue, Makati City and/or via Zoom. Zoom Meeting link is contained in Section III (Bid Data Sheet). Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

10. The bidders may submit their bids in any of the following form:
    10.1. Physical submission of the documents on the address stated below; or
    10.2. Electronic submission of bids with the following guidelines:
        10.2.1. The Bidder shall submit three (3) set of files of the same documents in PDF format, NOT EDITABLE, with different individual password before the set deadline. The Encryption Key and Password shall be submitted during the opening of the bids of the concerned bidder.
        10.2.2. The Bidder shall have the full responsibility on securing the files submitted are not corrupted. The DTI-BAC shall have three (3) attempts to open the submitted files.
            - If the first file was successfully opened, the two (2) remaining files shall be disregarded.
            - If the first file was corrupted, the DTI-BAC shall open the second file. If the second file was successfully opened, the first and third file shall be disregarded.
            - If the first and second file were corrupted, the third file shall be opened.
            - If the third file was corrupted, the bidder shall be automatically disqualified.

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

12. For further information, please refer to:

Maynard R. Peralta
Chief, Procurement Management Division
Human Resource and Administrative Service
Department of Trade and Industry
G/F, Trade and Industry Building
361 Sen. Gil Puyat Avenue, Makati City
Tel. No: +63 (2) 7791-3363/3367, Fax No: +63 (2) 895-3515
Email: **MaynardPeralta@dti.gov.ph**

Website: **www.dti.gov.ph**

13. You may visit the following websites:

For downloading of Bidding Documents:
https://notices.philgeps.gov.ph/
https://www.dti.gov.ph/good-governance-program/transparency-seal/bac-resources/

For online bid submission:

BACSecretariat@dti.gov.ph

28 October 2020

SGD.

MARY JEAN T. PACHECO
Assistant Secretary
Chairperson
DTI-Bids and Awards Committee

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, Department of Trade and Industry, wishes to receive Bids for the **Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution**, with identification number **20-021**.

The Procurement Project (referred to herein as "Project") is composed of one (1) lot, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

a. The GOP through the source of funding as indicated below for 2020 in the amount of **Eight Million Pesos (PhP 8,000,000.00)**.

b. The source of funding is NGA, the General Appropriations Act or Special Appropriations.

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 exceeding those allowed under the rules may participate pursuant to:

i. When a Treaty or International or Executive Agreement as provided in Section 4 of the RA No. 9184 and its 2016 revised IRR allow foreign bidders to participate;

ii. Citizens, corporations, or associations of a country, included in the list issued by the GPPB, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines;

iii. When the Goods sought to be procured are not available from local suppliers; or

iv. When there is a need to prevent situations that defeat competition or restrain trade.

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:

For the procurement of Non-expendable Supplies and Services: The Bidder must have completed a single contract that is similar to this Project, 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 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 **three (3) 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**. 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 its 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 follows:

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

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**.

Section III. Bid Data Sheet

Bid Data Sheet

ITB Clause	
5.3	For this purpose, contracts similar to the Project shall be: a. **Supply and Delivery of Anti-Virus or Endpoint Security.** b. completed within **three (3) years** prior to the deadline for the submission and receipt of bids. For the procurement of Non-expendable Supplies and Services: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.
7.1	Subcontracting is not allowed.
8	The Department of Trade and Industry will hold a Pre-Bid Conference on **05 November 2020, 9:30AM** through video conferencing or webcasting via Zoom, which shall be open to prospective bidders. Zoom Meeting Details: https://zoom.us/j/92458485360?pwd=R05QcG1zWE1xWXIzamp4V2poZnRaUT09 Meeting ID: 924 5848 5360 Passcode: 743002
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 **One Hundred Sixty Thousand (PhP160,000.00)**, 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 **Four Hundred Thousand Pesos (PhP400,000.00)** if bid security is in Surety Bond.
15	a. Physical Submission: Each Bidder shall submit **one (1)** original and **five (5)** copies of the first and second components of its bid. b. Electronic Submission: Please refer to Section I (Invitation to Bid Clause 10).

17	Bid opening shall be on **18 November 2020, 9:30AM** at the Center Conference Room, Trade & Industry Building, 361 Sen. Gil Puyat Avenue, Makati City and/or via Zoom. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity. Zoom Meeting Details: https://zoom.us/j/93555563433?pwd=Q2M0SkFaZ1AzNnlmRDZqTXFHemFaQT09 Meeting ID: 935 5556 3433 Passcode: 907998
19.3	The lot*(s)* and reference is/are: One (1) lot is **Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution.**

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 at the Project Site is*:* **Director Laudemer G. Solidum** **Information Systems Management Service** **Trade & Industry Building** **361 Sen. Gil Puyat Avenue, Makati City** **Tel. No: +63 (2) 791-3226** **Fax No: +63 (2) 751-3138** **Email: LaudemerSolidum@dti.gov.ph** **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:

a. performance or supervision of on-site assembly and/or start-up of the supplied Goods;
b. furnishing of tools required for assembly and/or maintenance of the supplied Goods;
c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods;
d. 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

e. training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.

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.

Spare Parts –

The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:

Select appropriate requirements and delete the rest.

a. such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and

b. in the event of termination of production of the spare parts:

   i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and

   ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.

The spare parts and other components required are listed in **Section VI (Schedule of Requirements)** and the cost thereof are included in the contract price.

	The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods for a period of **one (1) year**. Spare parts or components shall be supplied as promptly as possible, but in any case, specified in **Section VII (Technical Specifications)**.
	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 promptly by the Procuring Entity, but in no case later than sixty (60) days upon completion, inspection and acceptance.
4	The inspections and tests will be conducted in DTI as stated in Section VII (Technical Specifications).

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	Quantity	Delivered, Weeks/Months	Statement of Compliance
1	**Supply, Delivery, Design, Testing and Maintenance of a Cloud-based Enterprise Endpoint Security Solution**	1 lot	30 c.d.	

Conforme:

_____
Name & Signature of the Authorized Representative

_____
Name of Company

_____
Date

Section VII. Technical Specifications

Technical Specifications

Item	Specification	Statement of Compliance
	DESCRIPTION: **Advance Endpoint Protection (AEP)** provides automatic threat protection and threat event reporting capabilities for servers, workstations, desktops, and laptops. It is the current evolution of endpoint detection and response (EDR) technology in order to provide detection, prevention, and forensic insight.	*[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,*
	A. <u>MANAGEMENT CONSOLE</u> **1. General features. The product should offer the following capabilities:** 1.1 The proposed solution must be a cloud-based centralized management console.	
	1.2 Bundle key, single license able to manage all security services that protects both desktops, servers (physical or virtual). The license must support operating system such as Windows, Linux, and MAC OS. Servers should account for less than 35% of all units.	
	2. Management console dashboard. For monitoring and incident management, the product should offer: 2.1 Capability to add, remove, arrange, configure, and customize multiple security portlets	
	2.2 Capability to offer real-time security information with easy to read charts.	
	2.3 Capability to configure the target of reporting, background of security report type, time interval for reported and displayed information and name of the portlet.	
	3. Management console network inventory. For infrastructure security management, the product should offer:	

	3.1 Integration with Microsoft Active Directory in order to import the inventory and information from these platforms.	*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.]*
	3.2 Network discovery for non-integrated machines in Microsoft Active Directory for both physical and virtual workstations and servers.	
	3.3 Remote deployment capabilities and uninstall of the existing antimalware product.	
	3.4 Manual and configurable installation packages for the antimalware product.	
	3.5 Capability to configure and run remote scanning tasks.	
	3.6 Capability to view centralized task results section with detailed info for every subtask.	
	3.7 Capability to assign policies at every level of management	
	3.8 Capability to configure policies inheritance and force policies configuration.	
	3.9 Capability to view detailed properties of managed endpoints such as name, IP, operating system, group, assigned policy, latest malware status, latest scan logs.	
	4. Management console policies. For infrastructure security management, the product should offer: 4.1 Capability to apply a policy to a specific endpoint or a group of endpoints.	
	4.2 One single policy template for physical and virtual machines.	
	4.3 Each security service has its configurable policy template with specific options to activate/ deactivate and configure functionalities like antimalware scanning, machine learning options, firewall, network access control, application blacklisting, web access control, device control, device location, and actions to be taken in case of malware.	
	4.4 A rule-based policy automatically assigned to the endpoints if it matches the given condition such as Location Rule through Network setting and User Rule through Active Directory.	

	5. Management Console Reports: 5.1 Large number of reports.	
	5.2 Easy to use from one view: summary and details in the same page, active summary section (filters details by clicking on summary section).	
	5.3 Filters for scheduled reports in order to receive by mail only relevant information for each user.	
	5.4 Archive with all the generated instances of a scheduled report.	
	6. Quarantine: 6.1 Remote restores, with configurable location and delete.	
	6.2 Customize the time the files are stored in quarantine up to 180 days.	
	7. Users: 7.1 Role based administration.	
	7.2 Detailed configuration for administrative target rights, to select which services and objects a user is allowed to manage.	
	8.1 Detailed logs for every user action.	
	9. API Keys 9.1 The solution must allow administrators to use API call.	
	9.2 The solution must include methods for managing companies, user accounts, configuring notifications, managing groups, folders and endpoints, managing policies, generating reports through API keys.	
	B. <u>PROTECTION FOR PHYSICAL WORKSTATIONS AND SERVERS</u> **1. Minimal and eliminatory features:** 1.1 The existence of a single antimalware engine.	
	1.2 To minimize resource consumption, antimalware products should allow custom modules installation (e.g. installing the	

antimalware product without the web access control module or without Firewall module).	
2. System requirements: 2.1 Workstation operating systems: Windows 10, Windows 8.1, Windows 8, Windows 7	
2.2 Tablet and embedded operating systems: Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded Compact 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7	
2.3 Server operating systems: Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2	
3. Management and remote installation: 3.1 Before installation, the administrator can customize installation packages including only the desired modules: behavior-based analysis, firewall, content control, device control, application control.	
3.2 The installation on machines from a remote location will be performed using an existing installed client in these locations to minimize WAN traffic.	
3.3 The management console will report the number of workstations that have the antimalware installed and the number of the workstations that are unprotected.	
3.4 The management console will include detailed information about workstations/servers: name, IP, operating system, installed modules, applied policy, update information etc.	
3.5 The management console will allow the administrator to send a policy to configure the entire antimalware product, for both workstations and servers.	
3.6 The management console will permit two types of accounts, Network Administrator and Security Analyst, that may be assigned to what groups of users they can change the settings for or generate reports.	

	3.7 The management console will include a logging section where all actions will be mentioned, with detailed information: login, edit, create, logout, moved etc.	
	3.8 The management console will allow the possibility of creating a single package, used for both 32-bit operating systems and 64-bit, MAC and Linux.	
	3.9 Have the possibility to select which client will discover the other computers in the network.	
	4. The main features and functionality of antimalware and antispyware module:	
	4.1 Automatic real-time scanning can be set to not scan archives or files larger than "x" MB file size by the administrator of the solution.	
	4.2 Automatic real-time scanning can support scanning archives with up-to 16 levels of depth.	
	4.3 Behavioral heuristics scanning and process monitoring.	
	4.4 Must have an integrated Sandbox Analyzer that provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not yet signed.	
	4.5 Must have an integrated Hyperdetect Tunable protection against targeted attacks, suspicious files and network traffic, exploits, ransomware, or grayware.	
	4.6 Cloud scanning and Machine Learning technology.	
	4.7 Anti-ransomware and anti-exploit technology.	
	4.8 On-demand and on-access scanning of any information storage media (CDs, external hard drives, shared drive). Also, the scanning process can be stopped if the storage media devices contain information more than "x" MB.	
	4.9 Automatic scanning of emails at the workstation level, regardless of the email client, for SMTP and POP3 protocols.	
	4.10 Configuring the paths to be scanned, up to file level.	
	4.11 The antimalware product will allow defining the scan exclusion list, for both "on-access" and "on-demand" scan, for certain folders, disks, files, extensions or processes.	

4.12 With a comprehensive database of spyware signatures and heuristic detection of these programs, the product will have to offer antispyware protection.	
4.13 In order not to overload system resources, antimalware product must contain a single scan engine. He will be able to run scheduled scans with low priority and can automatically shut down after scanning the workstation.	
4.14 For greater protection, antimalware should have 4 types of detection: signature-based, heuristic based, processes continuous monitoring and cloud scanning.	
4.15 For greater protection, antimalware should be able to scan HTTP and SSL as well.	
4.16 For a better management of antimalware installed on workstations, the product will include the option of setting a password for uninstallation protection.	
4.17 For user safety, the client will include antiphishing module that will have the option of checking links searched with the search engines (Search Advisor).	
4.18 The antimalware application should offer on-access for Linux OS.	
5. Firewall: 5.1 The ability to set the "stealth mode" at the local network level or the Internet level.	
5.2 The module can be installed/uninstalled according to administrator preferences.	
6. Quarantine: 6.1 The antimalware product must allow automatic sending of the quarantined files to the virus lab.	
6.2 Sending quarantined files will be automatically done in a predefined time interval (number of hours) set by the administrator.	
6.3 Antimalware product must allow automatic deletion of quarantined files older than a certain period, not occupying unnecessary storage space.	

6.4 The quarantine will allow objects to be scanned after each signature update.	
6.5 The antimalware product must be able to save a copy of a malware file and send it to quarantine before taking Delete or Disinfect actions.	
7. Data Protection: 7.1 Allows blocking confidential data (pin card, bank account, etc.) for both HTTP and SMTP, by creating specific rules.	
8. User Control: 8.1 The product will have integrated a user control module with the following features: a. Blocking Internet access for specific clients or client groups. b. Blocking access to certain applications. c. Blocking Internet access for certain periods of time. d. Blocking web pages that contain certain keywords. e. Allowing access to specific web pages specified by the administrator. f. Restricting access to certain websites by some predetermined categories (e.g. online dating, violence, etc.).	
10. Device Control: 10.1 Prevent sensitive data leakage and malware infections via attached devices.	
10.2 Apply blocking rules and exclusions via policy to a vast range of devices and types.	
10.3 Will send information like device name, class ID, connection date and time.	
10.4 Have predefined types of devices like: CDROM, Imaging Devices, Tapes Drives, COM/LPT Ports, SCSI Raid, Printers, NICs, Internal and External storage etc…	
10.5 Support different configuration and privileges like Allowed, Blocked or Custom	
10.6 Support Read-Only mode for storage devices.	

	10.7 Ability to block only USB and allow all the other ports to be used.	
	10.8 Allow setting exclusions for different types of devices	
	10.9 Support to define devices exclusions: a. By Product ID b. By Device ID, Hardware ID c. Ability to discover devices.	
	11. Update: 11. 1 Ability to wait for computer restart after the update, without notifying the user.	
	11.2 Cascaded update system using a local update server.	
	11.3 Update clients in a remote location through an existing client with update server role built-in.	
	11.4 The client update server role must be available for Windows and Linux operating systems.	
	12. Endpoint Risk and Analytics (ERA): 12.1 The endpoint security must have an integrated Endpoint Risk Analytics (ERA) that identifies, assesses and remediates Windows endpoints weaknesses via security risk scans (on-demand or scheduled via policy), taking into account a vast number of indicators of risk.	
	13. Automatic Sandbox analysis of suspicious files 13.1 The solution must have an integrated Sandbox analysis and the ability to perform in-depth analysis of suspicious files.	
	13.2 The solution must have the ability to automatically or manually submit files to sandbox servers.	
	13.3 The solution can be configured to allow submitted objects to be accessed by users or block them until the analysis is returned.	
	13.4 The solution must allow different remediation actions if a submitted file is a threat.	
	13.5 The solution must have the ability to use a proxy server to the sandbox traffic.	

	13.6 The solution must have the ability to detonate files individually or as a group.	
	13.7 The solution offers detailed report about the files submitted.	
	C. <u>PROTECTION FOR VIRTUALIZED WORKSTATIONS AND SERVERS</u> **1. Antimalware protection dedicated to virtualized environments – minimal requirements:** 1.1 For all the systems running Windows and Linux, the product includes: a. Process scanning; b. Memory scanning; c. Real-time scanning of files; d. Scan files on demand;	
	1.2 Real time and on demand scanning for Linux virtual machines.	
	1.3 Contains the antimalware signatures;	
	1.4 Provides complete protection, up to date, when opening a virtual machine;	
	1.5 Provides optimized scanning.	
	1.6 A dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware agents, acting as a scan server.	
	2. General features: 2.1 Methods for detection of viruses, spyware, rootkits, and other malicious programs.	
	2.2 The product must report the current status of security host - VMs protected/unprotected	
	3. Minimum system requirements: A. **Operating Systems for Virtual Machines (32/64 bit):** • Windows 10, 8.1, 8, Windows 7	
	• Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2	

	• Linux distributions: Red Hat Enterprise Linux 6.0 or higher, CentOS 6.0 or higher, Ubuntu 14.04 LTS or higher, SUSE Linux Enterprise Server 11 SP4 or higher, OpenSUSE Leap 42.x, Fedora 25 or higher, Debian 8.0 or higher, Oracle Linux 6.3 or higher, Amazon Linux AMI 2016.09 or higher	
	4. The main features and functionality of antimalware module: 4.1 Automatic scanning of files that are being copied on external support and from LAN or WAN.	
	4.2 Automatic real-time scanning of files can be set to scan only specific file types, with specific extensions, defined by the administrator.	
	4.3 Automatic real-time scanning of files can be set to not scan archives larger than « x » KB, file sizes can be defined by the administrator of the solution.	
	4.4 The on-demand scanning will include the following options: a. Scan any storage media connected to the virtual machine; b. Emails scanning;	
	4.5 Configuring the paths to be scanned, to file level;	
	4.6 Must allow the administrator to define certain folders, disks, files and extensions to be excluded from the real time scanning and on demand scanning.	
	4.7 In order not to overload system resources, the antivirus product can be configured to use in-the-cloud scanning and partially, the local scanning. More than that, if the system doesn't have enough hardware resources, the antivirus can be configured to offload the scan to a scanning server. <u>Three Layer of Anti-Virus Scanning</u> 1. Central Scanning (Offload Scanning) 2. Local Scanning 3. Cloud	
	5. Quarantine: 5.1 Antimalware product must allow automatic deletion of quarantined files older than a certain period, not occupying unnecessary storage space.	

	5.2 The ability to move a file from quarantine to its original location.	
	5.3 Ability to rescan quarantined files after each signature update.	
	6. Management and remote installation: 6.1 The management console will report the number of virtual machines that have installed or not installed the virus protection solution and machine status: On or Off.	
	6.2 The possibility of management console to report whether or not the antimalware module is enabled on the virtual machine.	
	D. <u>ENDPOINT DETECTION AND RESPONSE</u> The proposed endpoint security agent must have an integrated endpoint detection and response platform that supports a modular information security solution capable of protecting any enterprise environment in a scalable and highly available method. It is an event correlation component, capable of identifying advanced threats or in-progress attacks. Product provides detailed information of the detected incidents, an interactive incident map and remediation actions	
	OS Support A. Desktop Operating Systems: • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone5) • Windows 10 April 2018 Update (Redstone4) • Windows 10 Fall Creators Update (Redstone3) • Windows 10 Creators Update (Redstone2) • Windows 10 Anniversary Update (Redstone1) • Windows 10 November Update (Threshold2) • Windows 10 • Windows 8.1 • Windows 8 • Windows 7	
	B. Server operating systems: • Windows Server 2012(4) / Windows Server 2012 R2(2) • Windows Server 2008 / Windows Server 2008 R2	

	C. MacOS: • OS X El Capitan (10.11.x) and later	
	D. Linux • Ubuntu 14.04 or higher • CentOS 7.3 or higher	
	EDR Components There are two major components: 1. The EDR Sensor, which collects and processes data to report endpoint and application behavior data. 2. Security Analytics, a backend component used to interpret metadata collected by the EDR sensor.	
	Post-Compromise Detection of Suspicious Activity Product monitors endpoint events looking for signs of attack and raises an incident when such activity is detected. 1. Product has the capability to baseline systems based on MITRE attack indicators and has its own threat intelligence. 2. Any deviation from the baseline is reported as incident in our EDR module.	
	Incident Investigation and Visualization 1. Product provides support for incident analysis by providing tools to help filter, investigate and take actions on all security events detected by the EDR Sensor over a specific time interval.	
	2. The product assigns confidence score value indicating the degree of certainty that a security event is dangerous.	
	3. Product integrates with MITRE's ATT&CK knowledge base and tags security events appropriately.	
	4. Security events can be searched by filenames, IP addresses, hostnames, or IOCs. It also provides advanced search feature which allows the user to go through past events based on a complex criterion. Predefined queries are designed for useful security event search cases.	

	5. The product provides sophisticated security event visualization with specific information or actions with the following information: a. The Summary tab provides an overview of the event impact and detailed information about each event node. b. Timeline feature gathers information about the security event development in a chronological order. c. Remediation Actions gathers information about the blocking actions automatically taken by the product on the current security event.	
	6. Product can blocklist files/processes using the MD5/SHA256 hash values. It can be done from the security incident or imported from a CSV file.	
	Threat Containment When security threat is detected, the product provides following remediations actions for threat containment.	
	Quick Remediation: 1. Product can apply remediation actions from this section as a temporary solution to the security event. 2. Kill – Stops a process from executing in the environment. This creates a kill process task on the local endpoint. System32 and its own processes are excluded from this action.	
	3. Quarantine file – Stores the item in question and prevents it from executing its payload.	
	4. Isolate Host – Product isolates the host from the network.	
	Network Actions: Product provides this solution for attack containment across the network 1. Add file to Blocklist – The file is question can be added to a blocklist and attack can be prevented from spreading laterally in the network.	
	2. Add file as Exception – For a non-malicious file, this option can be used to exclude legitimate activity.	

Investigate Actions:

The product leverages internal components and 3rd party solutions for further investigation.

1. Virustotal
2. Sandbox
3. Google

Remote Connection

1. Product can remotely connect to host to rapidly investigate attacks, collect forensic data and remediate breaches.
2. It eliminates uncertainty and greatly reduces any downtime that results from an attack.
3. It allows an authorized user/administrator to securely access managed endpoints directly from console.
4. After successfully connecting to the remote endpoint, several custom shell commands can be executed directly on the Operating system for remediating the threat instantly or collecting data for further investigation.

F. SERVICE LEVEL AGREEEMENT (SLA)

- FREE Technical Support
  - 24x7 FREE International Online Technical Support through email.
  - 24x7 FREE Local Telephonic Technical Support, Remote Support and Email Support.

- Onsite Technical Support
  - Next Business Day (NBD) on-site support as per request by the end user during the contract period.
  - On-Site support during the deployment of the Endpoint Security.

H. IMPLEMENTATION SERVICES AGREEMENT

- The winning bidder must provide accurate Statement of Work for 2,500 endpoints.
- The Supplier shall deliver, install, and configure the proposed equipment including all components at the DTI extension offices and branches within thirty (30) working days upon receipt of Notice to Proceed (NTP).
- The Supplier shall provide documentation of all the configuration made to the proposed equipment within forty (40) calendar days upon receipt of NTP.

	• Monthly Software Maintenance and Health Check of the system. • The winning bidder must provide hardcopy or softcopy of the user's manual and continuously update if ever there's new revision in the Anti-Virus Software. • The winning bidder must provide Comprehensive Users Training for 1 day. • The winning bidder must have at least Two (2) Certified Technical Engineer of the proposed endpoint security solution provided by the Principal or the distributor.	

Conforme:

_____
Name & Signature of the Authorized Representative

_____
Name of Company

_____
Date

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);
or

☐ (b) Registration certificate from Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for cooperatives or its equivalent document,
and

☐ (c) Mayor's or Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the equivalent document for Exclusive Economic Zones or Areas;
and

☐ (d) Tax clearance per E.O. No. 398, s. 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).

Technical Documents

☐ (f) 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**

☐ (g) 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**

☐ (h) 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**

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

☐ (j) 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

☐ (k) The Supplier's audited financial statements, showing, among others, the Supplier's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission; **and**

☐ (l) 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

☐ (m) 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 that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

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

☐ (n) *[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.

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

25 FINANCIAL COMPONENT ENVELOPE

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

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

Republic of the Philippines

gppb

Government Procurement Policy Board