



Republic of the Philippines  
Department of Justice  
**BUREAU OF CORRECTIONS**  
Muntinlupa City



## **BIDS AND AWARDS COMMITTEE**

# **BIDDING DOCUMENTS**

**For the**

## **Supply, Delivery and Installation of End-Point Security for ICT Equipment**

(Procurement/ID No.018)

**Sixth Edition**  
**July 2020**

# Table of Contents

<b>Glossary of Acronyms, Terms, and Abbreviations .....</b>	<b>2</b>
<b>Section I. Invitation to Bid.....</b>	<b>5</b>
<b>Section II. Instructions to Bidders.....</b>	<b>8</b>
1. Scope of Bid .....	9
2. Funding Information.....	9
3. Bidding Requirements .....	9
4. Corrupt, Fraudulent, Collusive, and Coercive Practices.....	9
5. Eligible Bidders.....	10
6. Origin of Goods .....	10
7. Subcontracts .....	10
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 .....	11
12. Bid Prices .....	12
13. Bid and Payment Currencies .....	12
14. Bid Security .....	12
15. Sealing and Marking of Bids .....	13
16. Deadline for Submission of Bids .....	13
17. Opening and Preliminary Examination of Bids .....	13
18. Domestic Preference .....	13
19. Detailed Evaluation and Comparison of Bids .....	14
20. Post-Qualification .....	14
21. Signing of the Contract .....	14
<b>Section III. Bid Data Sheet .....</b>	<b>15</b>
<b>Section IV. General Conditions of Contract .....</b>	<b>17</b>
1. Scope of Contract .....	18
2. Advance Payment and Terms of Payment .....	18
3. Performance Security .....	18
4. Inspection and Tests .....	18
5. Warranty .....	19
6. Liability of the Supplier .....	19
<b>Section V. Special Conditions of Contract .....</b>	<b>20</b>
<b>Section VI. Schedule of Requirements .....</b>	<b>23</b>
<b>Section VII. Technical Specifications .....</b>	<b>24</b>
<b>Section VIII. Checklist of Technical and Financial Documents .....</b>	<b>36</b>

# *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.

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 **28 September 2023 (1:30 P.M.)** at the given address below. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.
10. The *BuCor* 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.
11. For further information, please refer to:

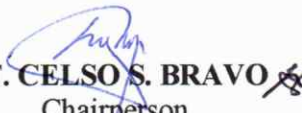
**WILLIAM M. TERRADO**

Office of the BAC Secretariat  
Supply Office, Bureau of Corrections, Muntinlupa City  
Tel # 02-8809-8587/02-8478-0907  
[bacsec2022@gmail.com](mailto:bacsec2022@gmail.com)

12. You may visit the following websites:

For downloading of Bidding Documents: *bucor.gov.ph*

**Issued on 7<sup>th</sup> day of September 2023.**

  
**CCSUPT. CELSO S. BRAVO**  
Chairperson  
Bids and Awards Committee

**CERTIFICATION**

The Schedule of Requirements and Technical Specifications are in conformity with the requirements of the end-user unit:

  
**GIL C. LLANO**  
End-User Representative

This Procurement Project is covered by an Approved Annual Procurement Plan:

  
**WILLIAM M. TERRADO**  
Head, BAC Secretariat

Prepared by:

  
**MARIA ADORACION I. VINAS**  
Member, BAC Secretariat

Approved for release by:

**CSSUPT. MELENCIO S. FAUSTINO**  
Vice-Chairperson, BAC

## ***Section I. Invitation to Bid***

**INVITATION TO BID**  
FOR THE  
**SUPPLY, DELIVERY AND INSTALLATION OF**  
**ENDPOINT SECURITY FOR ICT EQUIPMENT**  
**(BUCOR PROCUREMENT/ID NO. 018)**

1. The *Bureau of Corrections*, through the *General Appropriations Act for 2023* intends to apply the sum of being One Million One Hundred Thirty-Two Thousand Pesos Only (Php 1,132,000.00) to payments under the contract for **018**. Bids received in excess of the ABC shall be automatically rejected at bid opening.
2. The *BuCor* now invites bids for the above Procurement Project. Delivery of the Goods is required ***within Thirty (30) calendar days from the receipt of the Notice to Proceed***. 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.
  - a. 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 *BuCor BAC Secretariat* and inspect the Bidding Documents at the address given below during Mondays to Fridays (8:00 to 5:00 P.M.).
5. A complete set of Bidding Documents may be acquired by interested Bidders on **07 September 2023 (8:00 A.M. to 5:00 P.M.) to 28 September 2023 (1:29 P.M.)** 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 Php 5,000.00*. The Procuring Entity shall allow the bidder to present its proof of payment for the fees *to be presented in person at the BuCor BAC Secretariat*.
6. The BuCor will hold a Pre-Bid Conference<sup>1</sup> on **14 September 2023 (1:30 P.M.)** at *BuCor Supply Division Conference Room* which shall be open to prospective bidders.
7. Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below. Late bids shall not be accepted.

---

<sup>1</sup> May be deleted in case the ABC is less than One Million Pesos (PhP1,000,000) where the Procuring Entity may not hold a Pre-Bid Conference.



## ***Section II. Instructions to Bidders***

## 1. Scope of Bid

The Procuring Entity, **Bureau of Corrections** wishes to receive Bids for the **Supply, Delivery and Installation of Endpoint Security for ICT Equipment with identification number 018**.

*[Note: The Project Identification Number is assigned by the Procuring Entity based on its own coding scheme and is not the same as the PhilGEPS reference number, which is generated after the posting of the bid opportunity on the PhilGEPS website.]*

The Procurement Project (referred to herein as “Project”) is composed of [*indicate number of lots or items*], the details of which are described in Section VII (Technical Specifications).

## 2. Funding Information

2.1. The GOP through the source of funding as indicated below for *GAA 2023* in the amount of **One Million One Hundred Thirty Two Thousand Pesos (Php 1,132,000.00)**.

2.2. 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.
- a. 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:
  - a. 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 ***BuCor Supply Division Conference Room*** 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 the **BDS**.
- 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 the **BDS**.

## **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<sup>2</sup> 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 until **28 January 2024**. 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.

---

<sup>2</sup> In the case of Framework Agreement, the undertaking shall refer to entering into contract with the Procuring Entity and furnishing of the performance security or the performance securing declaration within ten (10) calendar days from receipt of Notice to Execute Framework Agreement.

## 19. Detailed Evaluation and Comparison of Bids

- 19.1. The Procuring Entity's 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 may be. In this case, the Bid Security as required by **ITB** Clause 14 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

- 20.2. 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, *{[Include if Framework Agreement will be used:]}* or in the case of multi-year Framework Agreement, that it is one of the eligible bidders who have submitted bids that are found to be technically and financially compliant, *}* 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**. *{[Include if Framework Agreement will be used:]}* For every mini-competition in Framework Agreement, the LCB shall likewise submit the required documents for final Post Qualification. *}*

## 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	<p>For this purpose, contracts similar to the Project shall be:</p> <p style="padding-left: 40px;">a.) considered “similar” to the contract to be bid if it involves goods and services of the same nature and complexity as the subject matter of the project being procured (<i>GPPB Non-Policy Matter No. 150-2017</i>); and</p> <p style="padding-left: 40px;">b.) completed within <b>three (3) years</b> prior to the deadline for the submission and receipt of bids.</p>
7.1	Subcontracting is not allowed.
12	No further instruction.
14.1	<p>The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts:</p> <p style="padding-left: 40px;">The amount of not less than the amount equivalent to two percent (2%) of the ABC, if bid security is in cash, cashier’s/manager’s check, bank draft/guarantee or irrevocable letter of credit; or</p> <p style="padding-left: 40px;">The amount of not less than the amount equivalent to five percent (5%) of total ABC, if bid security is in Surety Bond.</p>
19.3	The Approved Budget for the Contract for one (1) lot for the Supply, Delivery and Installation of Endpoint Security for ICT Equipment is <b>One Million One Hundred Thirty-Two Thousand Pesos (Php 1,132,000.00)</b>
20.2	<p>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;</p> <ol style="list-style-type: none"> <li>1. Latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS)</li> <li>2. Supporting Documents for the SLCC (Sales Invoice or Official Receipt or End-users Acceptance)</li> <li>3. Valid and Current Registration Certificate (SEC Certificate of Registration for Corporation or DTI Certificate of Registration for Sole Proprietorship or CDA Certificate of Registration for Cooperative)</li> <li>4. Valid and Current Mayor’s or Business Permit</li> <li>5. Valid and Current Tax Clearance</li> <li>6. Audited Financial Statement</li> </ol>
21.2	No further instruction.

## ***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 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. *{[Include if Framework Agreement will be used:]} In the case of Framework Agreement, the Bidder may opt to furnish the performance security or a Performance Securing Declaration as defined under the Guidelines on the Use of Framework Agreement.*

## 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 *{[Include if Framework Agreement will be used:]} or Framework Agreement* specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC, Section VII (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	<p><b>Delivery and Documents –</b></p> <p>Delivery of the Goods/Security Services shall be made by the Service Provider within <b>Thirty (30) calendar days</b> from receipt of notice to proceed by the winning bidder, in accordance with the terms specified in Section VI (Schedule of Requirements).</p> <p>For purposes of this Clause the Procuring Entity’s Representative at the Project Site is, <b>Ms. Gil Llano</b>, NBP, Muntinlupa City.</p> <p><b>Incidental Services –</b></p> <p>The Supplier/Service Provider is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements.</p> <p>The Contract price for the Goods/ and Services 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.</p> <p><b>Packaging –</b></p> <p>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.</p> <p>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.</p> <p>The outer packaging must be clearly marked on at least four (4) sides as follows:</p> <p>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</p>

	<p>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.</p> <p><b>Transportation –</b></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
2.2	No further instructions.
4	The inspections and tests that will be conducted at the project site and actual inspection of the goods/services shall be done as required under 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.

<b>Item Number</b>	<b>Description</b>	<b>Quantity</b>	<b>Delivered, Weeks/Months</b>
1	Supply, Delivery and Installation of Endpoint Security for ICT Equipment	1 Lot	<b>30 calendar days from receipt of Notice to Proceed</b>

Terms and Conditions:

Mode of Payment: Lump Sum (Subject for approval by end-user and upon issuance of Certificate of Acceptance by the End-User and Inspection and Acceptance Committee)



## ***Section VII. Technical Specifications***

# Technical Specifications

Item	Specification	Statement of Compliance
700 lics	<b>SUPPLY, DELIVERY AND INSTALLATION OF ENDPOINT SECURITY</b>	
	<i>System Requirements</i>	
	* Windows 7 to windows 11 Home / Professional / Ultimate / Enterprise	
	* Windows Server 2008 to 2022 R2 Foundation / Standard / Enterprise	
	<i>Functional Requirements</i>	
	* Detect following types of threat:	
	- Viruses (including polymorphic), Worms, Trojans, Backdoor, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software.	
	* Support Anti-malware Scan Interface (AMSI).	
	* Provide next gen protection technologies:	
	- Protection against file-less threats	
	- Provision of multi-layered Machine Learning (ML) based protection and behavioral analysis during different stages of the kill-chain	
	* Provide Memory Scanning for Windows workstation	
	* Provide the ability to switch to cloud mode for threat protection decreasing RAM and hard disk drive resource-limited machine.	
	* Have dedicated components to monitor detect and block activities on Windows, Linux and Windows servers and endpoints, to protect against remote encryption attack.	
	* Include signatureless components to detect threats even without frequent updates. Protection must be powered by Static ML for pre-execution and Dynamic ML for post-execution stage of the kill-chain on endpoints and in the cloud for Windows servers an workstations.	
	* Provide behavioral analysis based on ML.	
* Provide the ability to integrate with the vendor’s own Endpoint Detection and Response (EDR) and Anti-APT solutions, for active threat hunting and automated incident response.		
* The suggested solution must support integration with Sandbox with ability to automatically scan endpoints and apply responses in case if suspicious activity has been detected by the Sandbox.		
* The suggested solution must support integration with APT solution.		

	<p>* The suggested solution must support integration with Managed Detection and Response service.</p>	
	<p>* The suggested solution must support integration with threat intelligence portal, which contains and displays information about the reputation of files and URLs</p>	
	<p>* The suggested solution must support integration with cloud reputation service.</p>	
	<p>* The suggested solution must support central management and analytics through on-prem Web console and cloud management console. (Incident related data, System status and health check data, Settings, etc.)</p>	
	<p>* EDR agent must have integration with Endpoint Protection application (Single agent).</p>	
	<p>* EDR and Endpoint Protection solutions must have unified console for administrators and analysts</p>	
	<p>* EDR should support standalone agent installation (without Endpoint Protection application).</p>	
	<p>* Hardware platform where the solution is installed should be flexible for any upgrade include network interfaces, RAM and CPU</p>	
	<p>* Ability to configure and manage firewall settings built into the Window Server, through its management console.</p>	
	<p>* Provide Application and Device Controls for Windows workstations.</p>	
	<p>* Protection for servers and workstations must include a dedicated component for protection against ransomware/cryptor virus activity on shared resources</p>	
	<p>* On detecting ransomware/cryptor-like activity, automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type.</p>	
	<p>* Provide a pre-defined list of scan exclusions for Microsoft applications and services.</p>	
	<p>* The installation of endpoint protection on servers without the need to restart.</p>	
	<p>* Enable the following for endpoints:</p>	
	<ul style="list-style-type: none"> <li>- Manual Scanning, On-Access Scanning, On-Demand Scanning, Compressed File Scanning, Scan Individual File, Folder and Drive, Script Blocking and Scanning, Registry Guard, Buffer Overflow Protection, Background/Idle Scanning, Removable Drive Scanning on connection with system</li> <li>- The ability to detect and block untrusted hosts on detection of encryption-like activities on server shared resources.</li> </ul>	

<p>* It have password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.</p>	
<p>* Must have both local and global reputation databases.</p>	
<p>* Must be able to scan HTTPS, HTTP and FTP traffic against viruses and spyware, or any other malware.</p>	
<p>* Include a personal firewall capable, as an absolute minimum, of an :</p>	
<ul style="list-style-type: none"> <li>- Blocking network activates of applications based on their categorization.</li> <li>- Blocking/allowing specific packets, protocols, IP addressse ports and traffic direction.</li> <li>- The automatic and manual addition of network subnets, and modification of network activity permissions.</li> </ul>	
<p>* It prevent the connection of reprogrammed USB device emulating keyboards, and enable control of the use of onscreen keyboards for authorization.</p>	
<p>* Be able to block network attacks and report the source of the infection</p>	
<p>* Must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files must be stored in a specific format that ensures they cannot pose any threat.</p>	
<p>* Have a proactive approach to preventing malware from exploiting existing vulnerabilities on servers and workstations.</p>	
<p>* Support AM-PPL (Anti-Malware Protected Process Light) technology for protection against malicious actions.</p>	
<p>* Provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections.</p>	
<p>* Include a dedicated component for scanning encrypted connection.</p>	
<p>* Able to decrypt and scan network traffic transmitted over encrypted connections supported by the following protocols; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.</p>	
<p>* Have the ability to automatically exclude web resources when a scan error occurs while performing an encrypted connection scan. This exclusion must be unique to the host and must not be shared with other endpoint.</p>	
<p>* Include functionality to remotely wipe data on the endpoint</p>	

<p>- In silent mode; On hard drives and removable drives; For all user accounts on the computer; Immediate data deletion; Postponed data deletion; Delete by using the operating resources - files are deleted but are not sent to the recycle bin; Delete completely, without recovery - making data practically impossible to restore after deletion</p>	
<p>* It include functionality to automatically delete the data if there is no connection to the endpoint management server</p>	
<p>* It support signature-based detection in addition to cloud-assisted and heuristic</p>	
<p>*Have the ability to raise an alert on, clean and delete a detected threat.</p>	
<p>*Have the ability to accelerate scanning tasks, skipping those objects that have not changed since the previous scan.</p>	
<p>*Allow the administrator to exclude specified files/ folders/ applications/ digital certificates from being scanned, either on-access (real-time protection) or during on-demand scans.</p>	
<p>* It should include the functionality to isolate infected computers.</p>	
<p>* It automatically scan removable drives for malware when they are attached to any endpoint. Scan control should be based on drive size.</p>	
<p>* Be able to block the use of USB storage devices or allow access only to permitted devices, and allow read/write access only by domain users, to reduce data theft and enforce lock policies.</p>	
<p>* Be able to differentiate between USB storage devices, printers, mobiles and other peripherals.</p>	
<p>* Be able to log file operations (Write and Delete) on USB storage devices on the endpoint. No additional license or component required to be installed on the endpoint.</p>	
<p>* Have ability to block the execution of any executable from the USB storage device.</p>	
<p>* Have ability to block/allow user access to web resources based on websites, content type, user and time of day.</p>	
<p>* Have a specific detection category to block website banners.</p>	
<p>* Provide the ability to configure WI-FI networks based on Network Name, Authentication Type, Encryption Type, so these can later be used to block or allow the Wi-Fi connections.</p>	
<p>* It support user-based policies for Device Web and Application Control</p>	
<p>* It should specifically allow the blocking of the following devices:</p>	
<p>- Bluetooth, Mobile devices, D/DVDs, Cameras and Scanners, MTPs and the transfer of data to mobile devices</p>	
<p>* It should feature cloud integration, to provide the fastest possible updates on malware and potential threats.</p>	

<p>*Ability to manage user access rights for Read and Write operations on CDs/DVDs, removable storage devices and MTP devices.</p> <hr/> <p>* Must feature firewall filtering by local address physical interface, and packet Time-To-Live (TTL)</p> <hr/> <p>*Allow the administrator to monitor the application’s use of custom/random ports after it has launched</p> <hr/> <p>* It support the blocking of prohibited (Deny-List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-list</p> <hr/> <p>* Have a cloud-integrated Application Control component for immediate access to the latest updates on application ratings and categories.</p> <hr/> <p>* It must include traffic malware filtering, web link verification and web-resource control based on cloud categories.</p> <hr/> <p>* Web Control/Restriction component must include a Cryptocurrencies and Mining category. It must also include predefined regional legal restrictions to comply with Belgian and Japanese law</p> <hr/> <p>* Have the ability to allow applications based on their digital signature certificates, MD5, SHA256, META Data, File Path, and pre-defined security categories.</p> <hr/> <p>*Have controls for the download of DLL and drivers.</p> <hr/> <p>*Support the control of scripts from PowerShell.</p> <hr/> <p>* Support Test Mode with report generation on the launch of blocked application.</p> <hr/> <p>* Have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files “HIPS functionality”</p> <hr/> <p>* Have the ability to control system/user application access to audio and video recording device</p> <hr/> <p>* Must provide a facility to check application listed n each cloud-based category.</p> <hr/> <p>* Have ability to automatically regulate the activity of programs running, including access to the file system and registry as well as interaction with other programs.</p> <hr/> <p>* Have ability to automatically categorize applications launched prior to endpoint protection installation.</p> <hr/> <p>* Must have endpoint mail threat protection with:</p> <hr/> <p>- Attachment filter and the ability to rename attachments  - Scanning of mail messages when receiving, reading and sending.</p> <hr/> <p>* Must have the ability to scan multiple redirects shortened URLs, hijacked URLs, and time-based delays.</p>	
--	--

	<p>* Must enable the user of the computer to perform a check on a file's reputation from the File Context menu</p> <hr/> <p>* Must include the scanning of all scripts, including those developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the internet.</p> <hr/> <p>* Provide protection against as yet unknown malware based of the analysis of their behavior and examination of changes in the system register, together with a strong remediation engine to automatically restore any system changes made by the malware.</p> <hr/> <p>* Provide protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.</p> <hr/> <p>* Must include IPv6 protocol support</p> <hr/> <p>* Offer scanning of critical sections of the computer as a standalone task.</p> <hr/> <p>* Must incorporate Application Self-Protection technology:</p> <ul style="list-style-type: none"> <li>- protecting against unauthorized the remote management of application</li> <li>- protecting access to application parameters by setting a password.</li> <li>- preventing the disabling of protection by malware, criminals or amateur users</li> </ul> <hr/> <p>* Offer the ability to choose which threats protection components to install</p> <hr/> <p>* Include the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc</p> <hr/> <p>* Include the anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.</p> <hr/> <p>* Protect against as yet unknown malware belonging to registered families, based on heuristic analysis</p> <hr/> <p>* Include multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry).</p> <hr/> <p>* Allow the administrator to create a single installer with the required configuration, for use by non-IT literate users.</p> <hr/> <p><b><i>Centralized administration, monitoring and update software requirements</i></b></p> <hr/> <p>* Must enable the installation of anti-malware software from a single distribution package</p>	
--	---	--

	<p>* Must have customizable installation profiles depending on the number of protected nodes.</p> <hr/> <p>* Must support IPv6 addresses</p> <hr/> <p>* Must support two-step verification (authentication).</p> <hr/> <p>* Ability to read information from Active Directory to obtain data about computer accounts in the organization.</p> <hr/> <p>* Include a built-in web console for the management of the endpoints, which should not require any additional installation.</p> <hr/> <p>* Web management console should be straightforward to use and must support touch screen devices.</p> <hr/> <p>* Automatically distribute computer accounts by management group if new computers appear on the network. It must provide the ability to set the transfer rules according IP address, type of the operating system and location in Organizational Units of Active Directory.</p> <hr/> <p>* Provide for the centralized installation update and removal of anti-malware software, together with centralized configuration, administration, and the information about its operation.</p> <hr/> <p>* Feature the centralized removal (manual and automatic) of incompatible applications from the administration center.</p> <hr/> <p>* Provide flexible methods for anti-malware agent installation: RPC, GPO, an administration agent for remote installation and the option to create a standalone installation package for local installation.</p> <hr/> <p>* Enable the remote installation malware software with the latest anti-malware databases.</p> <hr/> <p>* Feature the automatic update of anti- malware software and anti-malware database.</p> <hr/> <p>* Have automatic search facilities for vulnerabilities in applications and in the operating system on protected machines.</p> <hr/> <p>* Must enable the management of a component prohibiting the installation and/or running of programs.</p> <hr/> <p>* Enable the management of a component controlling work with external I/O devices.</p> <hr/> <p>* Be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization platform or hypervisory.</p> <hr/> <p>* Enable the creation of a hierarchy of administration servers at an arbitrary level and the ability to centrally managing the entire hierarchy from the upper level.</p> <hr/> <p>* Support Managed Services Mode administration servers, so that logically isolated administration server instances can be set up for different users and user groups.</p>	
--	---	--



<p>* Give access to the anti-malware security vendor's cloud services via the administration server.</p>	
<p>* Include the automatic distribution of licenses on client computer.</p>	
<p>* Be able to perform inventories of software and hardware installed on user computers.</p>	
<p>* Have a notification mechanism to inform users about events in the installed anti-malware software and setting and to distribute notifications about events via email.</p>	
<p>* Enable the centralized installation of third party applications on all or selected computers.</p>	
<p>* Have the ability to specify any computers in the organization as a center for relaying updates and installation packages, in order to reduce the network load on the main administration server system.</p>	
<p>* Have the ability to specify any computer the organization as a center for forwarding anti-malware agent events from the selected group of client computers to the centralized administration server, in order to reduce the network load on the main administration server system.</p>	
<p>* Be able to generate graphical reports for anti-malware software events, and data about the hardware and software inventory, licensing, etc. be able to export of reports to PDF and XML files.</p>	
<p>* Provide the centralized administration of backup storages and quarantine on all network resources where anti-malware software is installed.</p>	
<p>* Provide the creation of internal account authenticate administrators on the administration server.</p>	
<p>* Provide the creation of an administration system backup copy with the help of integrated administration system tools.</p>	
<p>* Must support Windows Failover Cluster</p>	
<p>* Must have a built-in clustering feature.</p>	
<p>* Include Role Based Access Control (RBAC), and this must allow restrictions to be replicated throughout the management servers in the hierarchy.</p>	
<p>* Management server must include pre-defined security roles for the Auditor, Supervisor and Security Officer.</p>	
<p>* Have ability manage mobile device through remote commands.</p>	
<p>* Have ability to delete downloaded updates.</p>	
<p>* Enable Administration Server updates to be managed from the application interface.</p>	
<p>* Provide the ability to select an update agent for client computers based on analysis of the network.</p>	

<p>* Clearly show information about the distribution of vulnerabilities across managed computers.</p>	
<p>* Management server must maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed.</p>	
<p>* Management server must have functionality to create multiple profiles within a protection policy with different protection settings that can be simultaneously active on a based on the following activation rules:</p>	
<p>- Device status, Tags, Active directory, Device owner, Hardware</p>	
<p>* Support following notification delivery channels:</p>	
<p>- Email, Syslog, SMS, SIEM</p>	
<p>* Have the ability to define an IP address range, in order to limit client traffic towards the management serve based on time and speed.</p>	
<p>* Have the ability to perform inventory on scripts and .dll files.</p>	
<p>* Have the ability to tag/mark computers based on:</p>	
<p>a. Network Attributes (Name, Domain and/or Domain Suffix, IP address, IP address to management server)</p>	
<p>b. Location in Active Directory (Organizational Unit, Group)</p>	
<p>c. Operating System (Type and Version, Architecture, Service Pack number)</p>	
<p>d. Virtual Architecture</p>	
<p>e. Application registry (Application name, Application version, Manufacturer)</p>	
<p>* Have the ability to create/define settings based on a computer's location in the network, rather than the group to which it belongs in the management server</p>	
<p>* Have the functionality to add a unidirectional connection mediator between the management server and the endpoint connecting over the internet/public network.</p>	
<p>* Allow the administrator to define restricted settings in policy/profile settings, so that a virus scan task can be triggered automatically when a certain number of viruses are detected over defined amount of time. The values for the number of viruses and timescale must be configurable.</p>	
<p>* Have a customizable dashboard generating and displaying real time statistics for endpoints.</p>	
<p>* Allow the administrator to customize report.</p>	
<p>* Enable the administrator to set a period of time after which a computer not connected to the management server and its related data are automatically deleted from the server.</p>	
<p>* Allow the administrator to create categories/groups of application based on:</p>	

<p>-Application Name, Application Path, Application Metadata, Application Digital certificate, Vendor pre-defined application category, SHA, Reference computer</p>	
<p>* Allow the administrator to define different status change conditions for groups of endpoints in the management server.</p>	
<p>* Allow the administrator to add custom/3rd party endpoint management tools into the management server.</p>	
<p>* Have a built-in feature/module to remotely collect the data needed for troubleshooting from the endpoints, without requiring physical access.</p>	
<p>* Allow the administrator to create Connection Tunnel between a remote client device and the management server if the port used for connection to the management server is not available on the device.</p>	
<p>* Have built-in functionality to remotely connect to the endpoint using Windows Desktop Sharing Technology. In addition the solution must be able to maintain the auditing of administrator actions during the session.</p>	
<p>* Have a feature to create a structure of administration groups using the Groups hierarchy, based on the following data:</p>	
<ul style="list-style-type: none"> <li>- structures of Windows domains and workgroups</li> <li>- structures of Active Directory group</li> <li>- contents of a text file created by the administrator manu</li> </ul>	
<p>* Be able to retrieve information about the equipment detected during a network poll.</p>	
<p>* Incorporate a single distribution/relay agent to support at least 10,000 endpoints for the delivery of protection updates, patches, and installation packages to remote site.</p>	
<p>* Incorporate a single distribution/relay agent to relay/transfer or proxy threat reputation requests from endpoints to the management server.</p>	
<p>* Support the download of differential files rather than full update packages.</p>	
<p>* Support OPEN API, and include guidelines for integration with 3rd party external system.</p>	
<p>* Include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.</p>	
<p>* Include Role Based Access Control (RBAC) with customizable predefined roles.</p>	
<p>* Master/primary/parent management server must be able to relay updates and cloud reputation services.</p>	
<p>* Reports must include information about each threat and the technology that detected it</p>	

<p>* Report must include details about which endpoints protection components are, or are not, installed on client devices, regardless of the protection profile applied/existing for these devices.</p>	
<p>* Primary management server must be able retrieve detailed information reporting on the health status etc. of managed endpoints from the secondary management servers.</p>	
<p>* Include the option for the customer to either deploy an on-premises -management console, or use the vendor provided cloud-based management console.</p>	
<p>* Be able to integrate with the vendor's cloud-based management console for endpoint management at no additional cost.</p>	
<p>* Enable swift migration from the on-premises management console to the vendor management console.</p>	
<p>* Provide anti-malware database update mechanisms including:</p>	
<p>a. Multiple ways of updating, including global communication channels over the HTTPS protocol, shared resource at local network and removable media.</p>	
<p>b. Verification of the integrity and authenticity of updates by means of an electronic digital sign</p>	
<p>* Support Single Sign On (SSO) using NTLM and Kerberos</p>	
<p><b><i>Documentation</i></b></p>	
<p>* Requirements for solution documentation. Documentation for all malware software, including administration tools, should include the following documents:</p>	
<p>a. Online Help Administrator</p>	
<p>b. Online Help for implementation best practices</p>	
<p>* The anti-malware software documentation provided should describe in detail the processes of installation, configuration and use of the anti-malware software.</p>	

**I/We hereby commit to comply and deliver all the requirement in accordance with the above stated specifications.**

**CONFORME:**

---

Name of Company in Print

---

Signature Printed Name of Authorized Representative

---

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

## II. FINANCIAL COMPONENT ENVELOPE

- (i) Original of duly signed and accomplished Financial Bid Form; **and**

- (j) Original of duly signed and accomplished Price Schedule(s).

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

- (k) *[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.
- (l) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

**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: \_\_\_\_\_



# *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: \_\_\_\_\_

**Bid Form for the Procurement of Goods**  
*[shall be submitted with the Bid]*

---

**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.

*[Insert this paragraph if Foreign-Assisted Project with the Development Partner:*

Commissions or gratuities, if any, paid or to be paid by us to agents relating to this Bid, and to contract execution if we are awarded the contract, are listed below:

Name and address Amount and Purpose of  
of agent Currency Commission or gratuity

---

---

---

(if none, state "None") ]

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: \_\_\_\_\_

## 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, 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, 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, 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]*

