PHILIPPINE BIDDING DOCUMENTS

Subscription to Endpoint Security with Managed Detection and Response

Government of the
Republic of the Philippines
Insurance Commission

Project Reference Number:
2024 – 07 – 194

Sixth Edition

25 July 2024

Preface

These Philippine Bidding Documents (PBDs) for the procurement of Goods through Competitive Bidding have been prepared by the Government of the Philippines for use by any branch, constitutional commission or office, agency, department, bureau, office, or instrumentality of the Government of the Philippines, National Government Agencies, including Government-Owned and/or Controlled Corporations, Government Financing Institutions, State Universities and Colleges, and Local Government Unit. The procedures and practices presented in this document have been developed through broad experience, and are for mandatory use in projects that are financed in whole or in part by the Government of the Philippines or any foreign government/foreign or international financing institution in accordance with the provisions of the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184.

The Bidding Documents shall clearly and adequately define, among others: (i) the objectives, scope, and expected outputs and/or results of the proposed contract or Framework Agreement, as the case may be; (ii) the eligibility requirements of Bidders; (iii) the expected contract or Framework Agreement duration, the estimated quantity in the case of procurement of goods, delivery schedule and/or time frame; and (iv) the obligations, duties, and/or functions of the winning bidder.

Care should be taken to check the relevance of the provisions of the PBDs against the requirements of the specific Goods to be procured. If duplication of a subject is inevitable in other sections of the document prepared by the Procuring Entity, care must be exercised to avoid contradictions between clauses dealing with the same matter.

Moreover, each section is prepared with notes intended only as information for the Procuring Entity or the person drafting the Bidding Documents. They shall not be included in the final documents. The following general directions should be observed when using the documents:

a. All the documents listed in the Table of Contents are normally required for the procurement of Goods. However, they should be adapted as necessary to the circumstances of the particular Procurement Project.

b. Specific details, such as the "*name of the Procuring Entity*" and "*address for bid submission*," should be furnished in the Instructions to Bidders, Bid Data Sheet, and Special Conditions of Contract. The final documents should contain neither blank spaces nor options.

c. This Preface and the footnotes or notes in italics included in the Invitation to Bid, Bid Data Sheet, General Conditions of Contract, Special Conditions of Contract, Schedule of Requirements, and Specifications are not part of the text of the final document, although they contain instructions that the Procuring Entity should strictly follow.

d. The cover should be modified as required to identify the Bidding Documents as to the Procurement Project, Project Identification Number, and Procuring Entity, in addition to the date of issue.

e. Modifications for specific Procurement Project details should be provided in the Special Conditions of Contract as amendments to the Conditions of Contract. For easy completion, whenever reference has to be made to specific clauses in the Bid Data Sheet or Special Conditions of Contract, these terms shall be printed in bold typeface on Sections I (Instructions to Bidders) and III (General Conditions of Contract), respectively.

f. For guidelines on the use of Bidding Forms and the procurement of Foreign-Assisted Projects, these will be covered by a separate issuance of the Government Procurement Policy Board.

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 projects, 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

INVITATION TO BID

SUBSCRIPTION TO ENDPOINT SECURITY WITH MANAGED DETECTION AND RESPONSE
(PROJECT REFERENCE NO. 2024 – 07 – 194)

1. The **Insurance Commission,** through the **Government of the Philippines (GOP) under 2024 Special Account in the General Fund (SAGF) 151,** intends to apply the sum of **Eight Million Pesos (Php8,000,000.00), inclusive of 12% VAT,** being the Approved Budget for the Contract (ABC) to payments under the contract for the **Subscription to Endpoint Security with Managed Detection and Response** with **Project Reference No. 2024-07-194**. Bids received more than the ABC and late bids shall be automatically rejected at bid opening.

2. The Insurance Commission (IC), through its Bids and Awards Committee, now invites bids for the **Subscription to Endpoint Security with Managed Detection and Response**. Delivery of the Goods is required as indicated in the **Bid Data Sheet**. Bidders should have completed, **within five (5) years from the date of submission and receipt of bids, a contract similar to the Project**. The description of an eligible bidder is contained in the Bidding Documents, particularly in Section II. Instructions to Bidders.

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) 9184, otherwise known as the "Government Procurement Reform Act." 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 citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

4. Prospective Bidders may obtain further information from the IC-BAC Secretariat at Telephone No. (02) 8523-8461 local 107 or through email (bacsec@insurance.gov.ph) and inspect the Bidding Documents at the address given below from **9:00 A.M. to 4:00 P.M., Monday to Friday.**

5. A complete set of Bidding Documents may be acquired by interested Bidders starting **26 July 2024** from the given address and the IC website (https://www.insurance.gov.ph/public-bidding/) 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 through electronic means.

Moreover, starting **26 July 2024**, the Bidding Documents may also be downloaded free of charge from the website of the Philippine Government Electronic Procurement System (PhilGEPS), and the IC website (**https://www.insurance.gov.ph/public-bidding/**) provided that Bidders shall pay the nonrefundable fee for the Bidding Documents not later than the submission of their bids.

6. The Insurance Commission will conduct a **Pre-Bid Conference** on **05 August 2024, at 2:00 P.M**. This conference will take place both **onsite** at the **IC Function Room, Insurance Commission, 1071 United Nations Avenue, Ermita, Manila**, and **online** via **Cisco WebEx,** per Section 22.3 of revised IRR of RA 9184. Prospective bidders are welcome to attend.

   Interested bidders should email their request to participate in the Pre-Bid Conference, including the company name, full name, designation, and email addresses of the company representatives, to bacsec@insurance.gov.ph. Each company may send up to **two (2) representatives** and must specify their preferred mode of attendance (onsite or online).

7. Bids must be duly received by the BAC Secretariat manual submission at the office address indicated below on or before **19 August 2024, 09:00 AM**. 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 **19 August 2024, 10:00 A.M.** at the **IC Function Room, Insurance Commission, 1071 United Nations Avenue, Ermita Manila.** Bids will be opened in the presence of the bidders' representatives who choose to attend at the given address. Late bids shall not be accepted.

   Interested bidders may send their request to participate in the Bid Opening through e-mail. Kindly indicate the company name, full name, designation, and e-mail addresses of the company representatives and send the request to **bacsec@insurance.gov.ph.** The procuring entity shall only accept a **maximum of two (2) company representatives** for the Bid Opening.

10. Each Bidder shall submit one (1) original and two (2) copies of the First and Second components of its bids: A three-envelope system. In addition, bidders are required to include a soft copy in the original bid submission. Kindly refer to **Section II, item 15.**

11. The **Insurance Commission** 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:

MR. ARTURO S. TRINIDAD II
BAC Chairperson
Insurance Commission
1071 United Nations Avenue, Ermita, Manila
8523-8461 local 107
Email address: bacsec@insurance.gov.ph

You may visit the following websites:

For downloading Bidding Documents:
https://www.insurance.gov.ph/public-bidding

[ORIGINAL SIGNED]
ARTURO S. TRINIDAD II
BAC Chairperson

25 July 2024

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, **INSURANCE COMMISSION,** wishes to receive Bids for the **Subscription to Endpoint Security with Managed Detection and Response**, with identification number **Project Reference No. 2024-07-194.**

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

2.1. The GOP through the source of funding as indicated below **2024 Special Account in the General Fund (SAGF) 151** in the amount of **Eight Million Pesos (Php8,000,000.00), inclusive of 12% VAT.**

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:

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

b. 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;

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

d. 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:

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**.

7.2. Subcontracting any portion of the Project does not relieve the Supplier of any liability or obligation under the Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants, or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants, or workmen.

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time and at its address as indicated in **Paragraph 6** of the **IB.**

9. Clarification and Amendment of Bidding Documents

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

10. Documents comprising the Bid: Eligibility and Technical Components

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

10.2. The Bidder's SLCC, as indicated in **ITB** Clause 5.3, should have been completed **within five (5) years from the date of submission and receipt of bids, a contract similar to the Project** 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, they 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 the delivery of the Goods to their final destination; and

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

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[1] 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**.

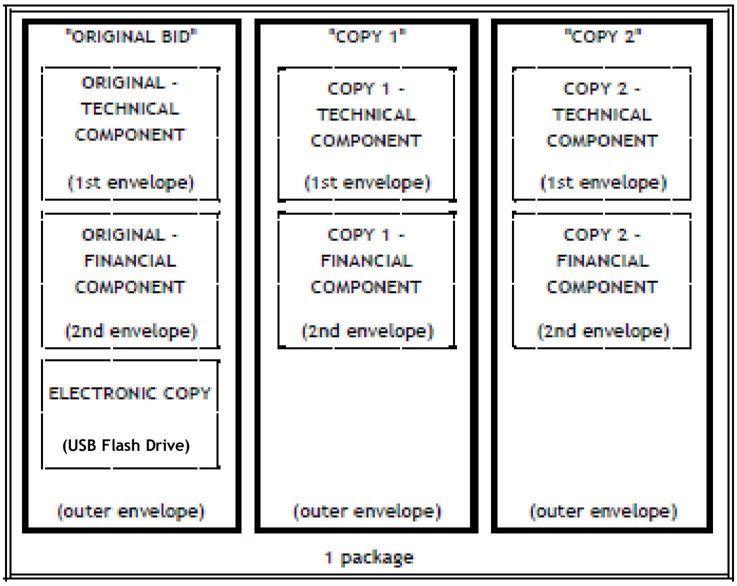
14.2. The Bid and bid security shall be valid until **17 December 2024**. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

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.

Each Bidder shall submit one (1) original and two (2) copies of the technical and financial components of its bid as illustrated below:

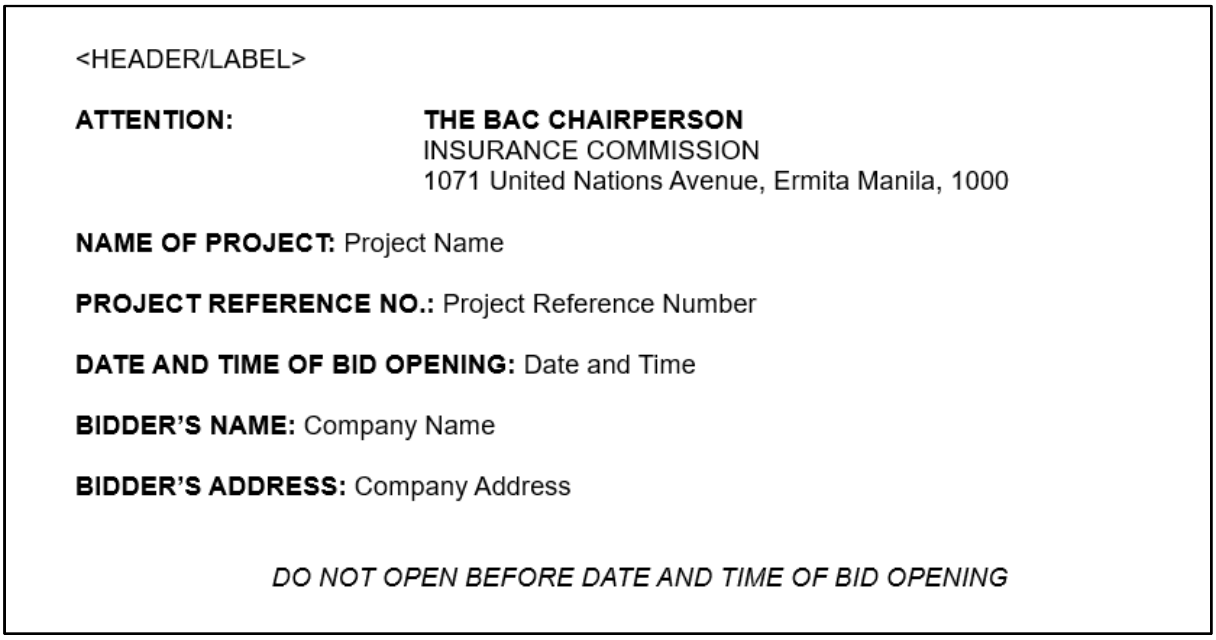

"ORIGINAL BID"
ORIGINAL - TECHNICAL COMPONENT (1st envelope)
ORIGINAL - FINANCIAL COMPONENT (2nd envelope)
ELECTRONIC COPY (USB Flash Drive)
(outer envelope)
"COPY 1"
COPY 1 - TECHNICAL COMPONENT (1st envelope)
COPY 1 - FINANCIAL COMPONENT (2nd envelope)
(outer envelope)
"COPY 2"
COPY 2 - TECHNICAL COMPONENT (1st envelope)
COPY 2 - FINANCIAL COMPONENT (2nd envelope)
(outer envelope)
1 package

In addition, all documents comprising the Technical and Financial Components shall be electronically scanned and recorded in a USB Flash Drive. The Flash Drive shall be marked as "ELECTRONIC COPY" and shall be put inside the sealed envelope labeled "ORIGINAL BID".

All submissions must be contained and sealed in one (1) package.

[1] 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.

Each sealed Bid shall be labeled as follows:



<HEADER/LABEL>

ATTENTION: **THE BAC CHAIRPERSON**
INSURANCE COMMISSION
1071 United Nations Avenue, Ermita Manila, 1000

NAME OF PROJECT: Project Name

PROJECT REFERENCE NO.: Project Reference Number

DATE AND TIME OF BID OPENING: Date and Time

BIDDER'S NAME: Company Name

BIDDER'S ADDRESS: Company Address

DO NOT OPEN BEFORE DATE AND TIME OF BID OPENING

<HEADER/LABEL> shall be:

1. **"ORIGINAL BID PLUS TWO COPIES INSIDE"** – for the bid package

2. **"ORIGINAL BID"** – for the 1st outer envelope
   a. **"ORIGINAL - TECHNICAL COMPONENT"** – for the 1st envelope inside the 1st outer envelope
   b. **"ORIGINAL - FINANCIAL COMPONENT"** – for the 2nd envelope inside the 1st outer envelope
   c. **"ELECTRONIC COPY"** – USB Flash Drive

3. **"COPY 1"** – for the 2nd outer envelope
   a. **"COPY 1 - TECHNICAL COMPONENT"** – for the 1st envelope inside the 2nd outer envelope
   b. **"COPY 1- FINANCIAL COMPONENT"** – for the 2nd envelope inside the 2nd outer envelope

4. **"COPY 2"** – for the 3rd outer envelope
   a. **"COPY 2 - TECHNICAL COMPONENT"** – for the 1st envelope inside the 3rd outer envelope
   b. **"COPY 2- FINANCIAL COMPONENT"** – for the 2nd envelope inside the 3rd outer envelope

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 the procuring entity's physical address 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, the 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:

The Project shall be awarded One (1) 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, 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

<table>
<tr><th>ITB Clause</th><th></th></tr>
<tr><td>5.3</td><td>For this purpose, contracts similar to the Project shall be:
a. **The Bidder must have completed a single contract that is similar to this Project: Subscription to Endpoint Security with Managed Detection and Response equivalent to at least fifty percent (50%) of the ABC.**
b. Completed within **Five (5) years** prior to the deadline for the submission and receipt of bids.</td></tr>
<tr><td>7.1</td><td>Subcontracting is not allowed</td></tr>
<tr><td>12</td><td>The price of the Goods shall be quoted **Delivery Duty Paid (DDP)** to *1071 United Nations, Ermita Manila, Philippines,* or the applicable **International Commercial Terms (INCOTERMS)** for this Project.</td></tr>
<tr><td>14.1</td><td>The bid security shall be in the form of a **Bid Securing Declaration** or any of the following forms and amounts:
<table>
<tr><th>Approved Budget for the Contract
(₱)</th><th>Amount Cash, Cashier's/ Manager's Check, Bank Draft/ Guarantee/ Irrevocable Letter of Credit (2%) (₱)</th><th>Surety Bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission (5%) (₱)</th><th>Bid Securing Declaration (Pursuant to GPPB Resolution No. 03-2012</th></tr>
<tr><td>**8,000,000.00**</td><td>**160,000.00**</td><td>**400,000.00**</td><td>**No required Amount**</td></tr>
</table>
1. The amount of not less than ***One Hundred Sixty Thousand Pesos (Php160,000.00)***, if bid security is in cash, cashier's/manager's check, bank draft/guarantee, or irrevocable letter of credit; or
2. The amount of not less than ***Four Hundred Thousand Pesos (Php400,000.00)***, if bid security is in Surety Bond;
If the Bid Security is in the form of a cashier's/manager's check, the payee shall be "**INSURANCE COMMISSION**."</td></tr>
<tr><td>15</td><td>Additional instructions were stated in ITB Number 15 (Sealing and Markings of Bid).</td></tr>
<tr><td>19.3</td><td>The Project will be awarded in One (1) Lot:</td></tr>
</table>

Lot No.	Quantity		Item/Description	Approved Budget for the Contract
1	1	lot	Subscription to Endpoint Security with Managed Detection and Response	**₱8,000,000.00**

20.2 **Post Qualification:** Within a non-extendible period of **five (5) calendar days** from receipt by the supplier of the Notice from the BAC that the supplier has the Single/Lowest Calculated Bid (S/LCB), the Supplier shall present original copy and submit a certified true copy of the following for post qualification:

1. Photocopy/ies of Contract/s or Purchase Order/s of one of the following:
    a. A single contract that is similar to the project and whose value must be at least fifty percent (50%) of the ABC to be bid; **OR**
    b. At least two (2) similar contracts:
        i. the aggregate amount of which should be equivalent to at least fifty percent (50%) of the ABC; **AND**
        ii. the largest of these similar contracts must be equivalent to at least twenty-five percent of the percentage of the ABC as required above (i.e., twenty-five percent [25%]).

2. The corresponding proof/s of completion, could either be:
    a. Certificate/s of Final Acceptance/Completion from the bidder's client/s; **OR**
    b. Official Receipt/s or Sales Invoice/s of the bidder covering the full amount of the contract/s.

3. Latest Income and Business Tax Returns, filed and paid through the Electronic Filing and Payment System (EFPS), consisting of the following:
    a. 2023 Income Tax Return with proof of payment; **AND**
    b. Latest Income Tax Returns per Revenue Regulations 3-2005; Tax returns filed through the Electronic Filing and Payments System (EFPS). The latest income and business tax returns are those within the last six months preceding the date of bid submission (including copy of VAT returns and corresponding payments for the last 6 months);

4. Registration certificate from SEC, Department of Trade and Industry (DTI) for sole proprietorship, or CDA for cooperatives;

5. Valid and current Business/Mayor's Permit issued to bidder by the city or municipality where the principal place of business of the bidder is located or the equivalent document for Exclusive Economic Zones or Areas;

	6. Valid and current Tax Clearance per E.O. 398, series of 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR); 7. Certification from the manufacturer or distributor (provide official certificate of distributorship) that they are certified reseller or partner of the proposed software and managed services; 8. Certification to provide Technical/Software Service Support from the manufacturer or distributor (provide official certificate of distributorship); **AND** 9. Brochures/Manuals *(In case of a Joint Venture between local companies, both partners must present/submit above item. In case of a foreign partner, must present/submit a Corporate Financial Statement or Annual Report)* ***N.B. Documents submitted during post-qualification as part of post-qualification documents must be certified by the authorized representative to be true copy/ies of the original.***
21.2	No further instructions

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	The Project Site is: **INSURANCE COMMISSION** 1071 United Nations Avenue Ermita, Manila **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: The delivery terms applicable to this Contract are delivered to **Insurance Commission, 1071 United Nations Avenue, Ermita, Manila**. 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 Representatives at the Project Site are **JUAN CARLO R. FLORENCIO AND JOEL LORENZO L. MALING** of the Information Technology Division.
	Incidental Services – The Supplier is required to provide all 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 the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:

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

Insurance –

The Goods supplied under this Contract shall be fully insured by the Supplier in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery. The Goods remain at the risk and title of the Supplier until their final acceptance by the Procuring Entity.

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 in accordance with GCC Clause 22. 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 the use of the Goods or any part thereof.
2.2	Payment shall be made in accordance with Section VII. Technical Specifications and upon completion of the contract and submission of complete documentary requirements in accordance with prevailing accounting and auditing rules and regulations.
4	The inspections and tests that will be conducted are: (a) Inspection conducted by the Internal Control Unit of the Procuring Entity; (b) IT Personnel of the Insurance Commission

Section VI. Schedule of Requirements

The delivery schedule expressed as days stipulates hereafter as delivery period, which is the date of delivery to the project site.

The delivery schedule shall be as indicated below:

ITEM	**IT EQUIPMENT**	**Qty**	**U/M**	**Delivered, Weeks/Months**
1	Subscription to Endpoint Security with Managed Detection and Response	1	lot	*Within Fifteen (15) Calendar Days from the receipt of the Notice to Proceed*

1. **Service Level Agreement/Warranty Certificate**
   The winning bidder must submit implementation Schedule indicating the required activities and the date of implementation, Sales/Service Invoice, and Service Level Agreement (SLA)/Warranty Certificate.

2. **Acceptance**
   Acceptance shall be issued upon compliance of the foregoing. All deliverables mentioned above shall be checked by IC and complied by the winning bidder before the final acceptance and turnover of the project.

3. **Liquidated Damages**
   - Liquidated Damages will be imposed if the delivery of the required documents and/or any deliverables will not be accomplished by the winning bidder after fifteen (15) days upon receipt of the Notice to Proceed.
   - The applicable rate for the liquidated damages is one tenth (1/10) of one (1) percent of the total bid price of the winning bidder for every day of delay.

4. **Payment Terms**
   Payment shall be made thirty (30) days after issuance of Certificate of Final Acceptance by the Procuring Entity subject to the submission of complete supporting documents.

I hereby certify to comply with and deliver all the above requirements.

____

Name of Company

____

Address

Signature over Printed Name (Duly authorized to sign the Bid)

Telephone/Fax Number

Section VII. Technical Specifications

DETAILED TECHNICAL SPECIFICATIONS

1. **Project Title**

   Subscription to Endpoint Security with Managed Detection and Response (Project Reference No. 2024-07-194)

2. **Objective**

   The objective of this procurement project is to secure a subscription for Endpoint Security with Managed Detection and Response (MDR) to enhance our organization's protection against cyberattacks. This subscription aims to safeguard our endpoints and servers from evolving and sophisticated threats by providing comprehensive threat detection, advanced analytics, and rapid incident response. It will ensure continuous monitoring, proactive threat hunting, and immediate response capabilities, thereby minimizing potential risks, reducing downtime, and protecting critical data and infrastructure. This investment is crucial for maintaining the integrity, confidentiality, and availability of our systems, ensuring compliance, and supporting overall service continuity.

3. **Subscription Period**

   The Subscription to Endpoint Security with Managed Detection and Response shall cover Two (2) years of **Supply, Renewal, Delivery, Installation and Configuration.**

4. **Number of Users/Endpoints**
   Endpoint Security for Workstations: 318
   Endpoint Security for Servers: 32
   Email Security: 350
   Cloud-based Phishing Simulation and Campaigns: 318
   Managed Risk: 350

5. **Endpoint Security for Workstations**
   a) Integrated Management
      i. Must have a unified console for managing multiple products from the same vendor
      ii. The ability to manage security policies and administer multiple products from a single web interface.
   b) Multi-Platform Management
      i. Windows, Mac, and Linux machines must be managed from one management console.
   c) Updating and Deployment Options
      i. Must be able to configure the bandwidth limit for updating
      ii. Must have the option to enable devices to get updates from the security vendor from a cache device and communicate all policy
      iii. Deploying the endpoint agent must support the following methodology:
         1) Email setup link
         2) Installer link

3) Scripted Installation
4) Inclusion on an Image

6. API and SIEM Integration

a) Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM
b) Allow integration with SIEM solutions

7. Role Management

a) Must have the capability to divide security administration by responsibility level and includes predefined roles including:
   i. Super Admin
   ii. Admin
   iii. Help Desk
   iv. Read-Only

8. AD Synchronization

a) Must have the capability to implement a service that maps users and groups from Active Directory to the security vendor cloud console and keeps them synced.
b) Must have the capability to synchronized with Azure Active Directory
c) Must have the capability to Auto synchronization that happens every 6 hours for Azure AD

9. Tamper Protection

a) Must have the capability to prevent the following actions on the endpoint protection solution:
   i. Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or security vendor live protection
   ii. Disable tamper protection
   iii. Uninstall the security vendor agent software

10. Threat Protection

a) Must have the capability to protect against malware, risky file types and websites, and malicious network traffic.
b) Must have the capability to have security vendor settings recommendation to provide best protection a computer can have without complex configuration
c) Must have the capability to Check suspicious files against the latest information in security vendor database
d) Must have the capability to automatically submit malware samples to security vendor online for analysis
e) Must have the capability to do real-time scanning of local files and network shares the moment the user tries to access them. Access must be denied unless the file is clean.
f) Must have the capability to do real-time scanning internet resources as users attempt to access them
g) Must have the capability to protect against threats by detecting suspicious or malicious behavior or traffic on endpoint computers:
   i. Documents from Ransomware
   ii. Critical functions in web browsers

iii. Mitigate exploits in vulnerable applications
iv. Application hijacking
v. Detect network traffic to command-and-control servers

11. Suspicious Behavior Detection

a) Must be able to monitor the behavior of code to stop malware before a specific detection update is released
b) Must be able to have both pre-execution behavior analysis and runtime behavior analysis
c) Must be able to have a technology that is used to identify specific characteristic of files before they run, to determine whether they have malicious intent

12. Advance Deep Learning Mechanism

a) The system shall be light speed scanning; within 20 milliseconds, the model shall able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes.
b) Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes.
c) Must be able to protect the system even with offline and will not rely on signatures
d) Must be able to classify files as malicious, potentially unwanted apps (PUA) or benign.
e) Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.
f) Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up to date.
g) Must Lighter - model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance.
h) The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, Tensorflow, and Scikit-learn.

13. Exploit Prevention/Mitigation must detect and stop the following known exploits:

a) Enforcement of Data Execution Protection (DEP)
b) Mandatory Address Space Layout Randomization (ASLR)
c) Bottom-up ASLR
d) Null Page (Null Dereference Protection)
e) Heap Spray Allocation
f) Dynamic Heap Spray
g) Stack Pivot
h) Stack Exec (MemProt)
i) Stack-based ROP Mitigations (Caller)
j) Branch-based ROP Mitigations (Hardware Augmented)
k) Structured Exception Handler Overwrite Protection (SEHOP)
l) Import Address Table Access Filtering (IAF) (Hardware Augmented)
m) LoadLibrary API calls

n) Reflective DLL Injection
o) Shellcode monitoring
p) VBScript God Mode
q) WoW64
r) Syscall
s) Hollow Process Protection
t) DLL Hijacking
u) Application Lockdown
v) Java Lockdown
w) Squiblydoo AppLocker Bypass

14. Policies

a) Selected policies should be able to be applied to either users or devices.
b) Policies must have the capability to be enforced and whether it expires.

15. Data Loss Prevention (DLP)

a) Must be able to monitor and restrict the transfer of files containing sensitive data.
b) Must be able to Specify conditions for data loss prevention to detect, action to be taken if the rules are matched, any files to be excluded from scanning
c) Must have two types of rules: File & Content

16. Peripheral Control

a) Must be able to control access to peripherals and removable media
b) Must be able to exempt individual peripherals from that control

17. Application Control

a) Must be able to detect and block applications that are not a security threat but lets the administrator decide if its unsuitable for office use.

18. Web Control

a) Must be able to block by category of the site
b) Must be able to block specific file types or specific websites
c) Must be able to prevent access to sites that increase the risk to the organization
d) Must be able to help improve productivity and potentially limit bandwidth

19. Root Cause Analysis

a) Must be able to allow investigation on the chain of events surrounding a malware infection and pinpoint areas where you can improve security
b) Must be able to Must have the following list for each case that is being created:
   i. Priority
   ii. Summary
   iii. Status
   iv. Time Created
   v. User
   vi. Device

20. Remediation

a) Detected malware are cleaned up automatically

b) If a cleanup is successful, the malware detected is deleted from the Alerts list. The malware detection and cleanup are shown in the "Events" list

21. Extended Detection and Response

i. Data lake

   i. Must have the capability to out-of the-box and fully customizable SQL queries

   ii. Must have the capability to store and access critical information from endpoints, servers, firewall and email

   iii. Must have the capability to utilize device information even when the device is offline

b) IT Operations

   i. Why a machine is running slowly.

   ii. Devices that have known vulnerabilities, unknown services or unauthorized browser extensions.

   iii. If there are programs running that should be removed.

   iv. Identify unmanaged, guest, and IoT devices

   v. Why network connection is slow and what application is causing it.

   vi. Look back 30 days for unusual activity on a missing or destroyed device

c) Critical IT Operations

   i. Find out what processes are trying to make a network connection on non-standard ports

   ii. Show processes that have recently modified files or registry keys

   iii. List detected IoCs mapped to the MITRE ATT&CK framework

   iv. Extend investigations to 30 days without bringing a device back online

   v. Use ATP and IPS detections from the firewall to investigate suspect hosts

   vi. Compare email header information, SHAs, and other IoCs to identify malicious traffic to a domain

d) Remote Access

   i. Must have the capability to connect to devices and investigate and remediate possible security issues

   ii. Must have the capability to stop suspicious processes, restart devices with pending updates, browse folders, and delete files

   iii. Must have the capability to see when sessions started and ended, the admin who started the session, the device that the session accessed, and the "Purpose" given when the session was started

e) Synchronized Security

   - Security products of the same vendor actively work together, responding automatically to incidents and delivering enhanced security insights

   i. Endpoint security + Email Security

      - Automatically isolate compromised mailboxes, and clean up infected computers sending outbound spam and malware

   ii. Email + Phishing

- One-click enrollment of risky users in targeted user education training programs

f) Managed Threat Response
   i. Must have advanced threat hunting, detection, and response capabilities delivered as a fully- managed service.
   ii. Must have a team of threat hunters and response experts available 24/7
   iii. Must be able to hunt and validate potential threats and incidents proactively
   iv. Must be able to use all available information to determine the scope and severity of threats
   v. Must be able to apply the appropriate business context for valid threats
   vi. Must be able to initiate actions to remotely disrupt, contain, and neutralize threats.
   vii. Must be able to provide actional advice for addressing the root cause of recurring incidents.

g) Managed Threat Response Operations Team
   i. Must have a team of security professionals: analysts, engineers, ethical hackers, specialists, and inventors. Backgrounds of personnel must be comprised of but not limited to armed forces, law enforcement, intelligence, and public and private enterprise.
   ii. Team must work 24/7 to hunt and neutralize threats that cannot be detected or neutralized by technology solutions alone.
   iii. Team must drive continuous improvement. In addition to neutralizing threats, we will provide detailed recommendations for improving your overall security posture
   iv. Must use a proprietary Investigative Framework that provides structure to guide analysts while investigating Cases
   v. The framework must enable the ops team to construct an attack narrative which aids them in concluding whether malicious activity is present within a customer environment (provided data coverage and data quality are at their maximum)
   vi. Must perform validation by applying the data points to the MITRE ATT&C Matrix, the Cyber Kill Chain, and an analyst’s tribal knowledge

h) Threat Hunting Data

   Must use the following data as the foundation from which the Ops team performs threat hunts:
   i. Device data
      i. Process execution: Contains information on processes run on specific hosts
      ii. Registry data: Contains data related to registry objects, including key and value metadata
      iii. File artifacts: Information on stored files and artifacts kept on a local host
   ii. Network data
      i. Session data: Information regarding network connections between hosts
      ii. DNS logs: Data related to DNS resolution

iii. IDS data
iv. Traffic information from all devices on the network
v. Firewall logs
vi. Connection data on the edge of the network (allowed and blocked)

iii. Security Data
i. Security alerts: Automated alerts from security tools
ii. Threat intelligence: Data that contains indicators and known tactics, techniques, and procedures (TTPs) used by attackers
iii. CVE vulnerability disclosures

i) Machine-Accelerated Human Response
Must be able to fuse machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats with speed and precision.

j) Complete Transparency and Control
i. Must have response actions that the customer can choose from to manage how the threat response team will work with them during incidents.
ii. Must have the following response modes to choose from:
i. Notify - The threat response team will notify you about the detection and provide detail to help you in prioritization and response.

ii. Collaborate - The threat response team will work with your internal team or external point(s) of contact to respond to the detection.

iii. Authorize - The threat response team will be handling the containment and neutralization actions and will inform you of the action(s) taken

k) Service Tiers - Must have service tiers available that can provide a comprehensive set of capabilities for organizations of all sizes and maturity levels.

l) Standard Tier
i. Must have 24/7 Lead-Driven Threat Hunting - Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated, freeing up threat hunters to conduct lead-driven threat hunts. This type of threat hunt involves the aggregation and investigation of causal and adjacent events (weak signals) to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.
ii. Must be able to conduct Security Health Check - Keep your security products operating at peak performance with proactive examinations of your operating conditions and recommended configuration improvements.
iii. Must have Activity Reporting - Must be able to provide summaries of case activities to enable prioritization and communication, so your

team knows what threats were detected and what response actions were taken within each reporting period

iv. Must have Adversarial Detections - The threat response team must be able to determine the difference between legitimate behavior and the tactics, techniques, and procedures (TTPs) used by attackers.

m) Advance Tier – Includes all Standard features, plus the following:

i. Must have 24/7 Leadless Threat Hunting - Enhanced Threat Hunting by utilizing methods such as data science, threat intelligence, and the intuition of veteran threat hunters to anticipate and identify Indicators of Attack (IoA) and compromise based on factors specific to the Customer's environment.

ii. Must have Enhanced Telemetry - Threat investigations must be supplemented with telemetry from other security products extending beyond the endpoint to provide a full picture of adversary activities.

iii. Must be able to conduct Proactive Posture Improvement - Proactively improve your security posture and harden your defenses with prescriptive guidance for addressing configuration and architecture weaknesses that diminish your overall security capabilities

iv. Must have a Dedicated Threat Response Lead - When an incident is confirmed, a dedicated threat response lead must be provided to directly collaborate with your on-premise resources (internal team or external partner) until the active threat is neutralized.

v. Must have Direct Call-In Support - Must have direct call-in access to the Security Operations Center (SOC). The Threat Response Operations Team should be available around-the-clock.

vi. Must have Asset Discovery - From asset information covering OS versions, applications, and vulnerabilities to identifying managed and unmanaged assets, the threat response team must be able to provide valuable insights during impact assessments, threat hunts, and as part of proactive posture improvement recommendations.

n) Service Level Targets - The following service level targets are utilized to provide Customers with guidelines around timing expectations for Case creation and Response Actions resulting from investigations but excluding Threat Hunting:

i. Target time for Case creation must be 2 minutes from Detection.

ii. Target time for initial Response Action must be 30 minutes from Case Creation.

22. Endpoint Security for Server

a) Server Protection Features

i. Must have the capability to enable computers to get updates from a cache on a server on the network, rather than directly from internet or security vendor.

ii. Must have the capability to only applications you have approved can run on a server.

iii. Must have the capability to file Integrity Monitoring
iv. Must have the capability to secure cloud, on-premises and virtual server deployments
v. Must have the capability to be managed via the security vendor cloud management platform for all the same security vendor solutions

b) Email Security (Microsoft and Google compatible)
i. Must be compatible with Microsoft Exchange Online and Microsoft Office 365
ii. Must be compatible with Microsoft Exchange 2003 or later
iii. Must be compatible with G Suite from Google Cloud
iv. Must be compatible with any service where you own the domain and control the associated DNS records.

c) Cloud Management
i. Must protect and manage emails in the cloud through an intuitive cloud-based console, providing access to the entire range of vendor products through one interface, including web, endpoint, mobile, and server.
ii. Must be able to create unique email security policies for individuals, groups or the whole domain

d) Active Directory Sync and Azure Active Directory Sync
i. Must have the capability to synchronize with Microsoft Active Directory
ii. Must have the capability to synchronize with Microsoft Azure Active Directory
iii. Must be able to keep users automatically synchronized with the product
iv. Must provide the administrator the capability to manually add mailboxes or import mailboxes and aliases.

e) Self-service portal for end-users
i. Must have a self-service portal for end-users
ii. The self-service portal must allow users to manage quarantined emails
iii. The self-service portal must allow users to edit the allow/block rules
iv. The self-service portal must allow users to view messages in the event of an outage using the emergency inbox

f) Data Center Location
i. Must meet data compliance regulations
ii. Must have a choice of global data centers for message processing

g) Business Continuity
i. Must have email spooling that ensures no email is lost.
ii. In the event of a disruption to your Microsoft or Google Cloud email service, the product must have the capability to automatically queue the recipient’s emails then deliver once the service is restored with a five day retry period"
iii. Must provide read access to queued email from a 24/7 Emergency Inbox inside the end-user portal

iv. Must have the capability to send administrator alerts when mail can't be delivered to a server/service in the event of third-party cloud email service provider outages

h) Protection from Spam and Malware
   i. Must have live threat updates to stop the latest attacks
   ii. Must have anti-spam, anti-virus, and anti-phishing detection
   iii. Must have reputation filtering that can block up to 90% of spam
   iv. Must have next-generation reputation filtering technology that eliminates botnet spam at the IP-connection level by monitoring connection requests and rejects those showing evidence of botnet connections
   v. Must protect against snowshoe spam

i) Block Phishing Imposters
   i. Must use a combination of authentication techniques to identify and allow legitimate emails from trusted partners and block imposters
   ii. Must use Sender Policy Framework (SPF) check to identify IP addresses authorized to send email from the domain
   iii. Must use Domain Keys Identified Mail (DKIM) check to provide cryptographic proof that a message was sent from a specific sender and hasn’t been tampered with
   iv. Must use Domain Message Authentication Reporting & Conformance (DMARC) check to determine what to do when messages fail SPF or DKIM checks from the sender
   v. Must have Header anomaly detection to identify if the sender's display name is the same as one of your internal usernames
   vi. Must be able to compare the display name of inbound emails to the display name of commonly abused cloud service brand names and VIPs within the organization to check for matches
   vii. Must be able to do an analysis of look-a-like domains to identify domain names similar to the corporate domain
   viii. Suspicious messages should have an option to be blocked, quarantined, tagged with a subject line warning, or have a banner added with a direct link to the user-level block list
   ix. Must have an Allow and Blocked senders policy that allows administrators to restrict messages to or from specific email addresses, IP addresses, and domains, including support for wildcards (*), allowing you to block country-level TLDs

j) Prevent Data Loss
   i. Must automatically scan message bodies and attachments for sensitive data to easily establish policies to block or encrypted messages
   ii. Must give users the capability to encrypt emails using the product's O365 add-in
   iii. Must have push-based encryption that protects the entire email or attachments only
   iv. Must have enforced TLS encryption that prevents eavesdropping when messages are in transit

v. Must protect sensitive information with the discovery of financials, confidential contents, health information, and PII in all emails and attachments

vi. Must be able to create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs

vii. Must have granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption"

viii. Must have a single console, managing data loss prevention for email, alongside next-gen endpoint protection

k) Active Threat Protection

i. Must have URL re-writing capability to check the website reputation of email links before delivery and at the time you click – blocking stealthy, delayed attacks

ii. Must have a cloud-based Sandbox that can detect zero-day malware and unwanted applications.

l) Comprehensive Reporting

i. Must provide statistics reports within the console in the form of tables and graphs with custom date ranges.

ii. Must have the following reports available:

a. Message history (messages deleted, quarantined, processing, delivered successfully, delivery failed, and queued for delivery)

b. Message details (sender/recipient info, status, raw header details, and attachments)

c. Message summary (message direction, # scanned, # Legitimate, # spam, # virus, # DLP policy violations, # advanced threat, # realtime blocklist, # company blocklist, # authentication failures)

d. Message volume analyzed by sandbox

e. Top 100 URLs scanned

23. Cloud-based Phishing Simulation and Campaigns

a) Integrated Management

i. Must have a cloud-based unified console for managing multiple products such as Phishing Simulation, Advanced Endpoint Protection, Email Gateway, Server Security, Mobile Control, etc.

ii. All settings for these products MUST be configured from a Central Dashboard without the need to access additional consoles.

b) Attack Simulations

i. Must be able to emulate a range of phishing attack types to help you identify areas of weakness in your organization's security posture and empower users through engaging training to strengthen your organization's defenses.

ii. Must have over 500 customizable, realistic, and challenging phishing attacks.

iii. Email simulations must support 10 languages:

a. English;

b. German;

c. French;

d. Dutch;

e. Italian;
f. Spanish;
g. Portuguese;
h. Korean;
i. Japanese;
j. Traditional Chinese

iv. Campaigns should have the following template categories:
   a) *Phishing:* This simulates a phishing attack against your users. It encourages your users to click a link in an email.
   b) *Credential Harvesting:* This simulates an attack designed to obtain login ids and passwords. It encourages your users to enter credentials into a fake website. No passwords are collected.
   c) *Attachment:* This simulates an attack designed to deploy malicious attachments on your system. It encourages your users to open an attachment in an email.
   d) *Training:* This allows you to send anti-phishing training to your users without a simulated attack.

c) Training

i. Must have over 60 interactive training modules that will educate users about specific threats, such as suspicious emails, credential harvesting, password strength, and regulatory compliance.
ii. Training campaigns without attack simulation should be available.
iii. Must have the option to redirect caught users to your own hosted training material.

d) Customization and Scheduling

i. Must have Email Template User Variables
ii. Must have Training Reminder Emails
iii. Must have customizable Landing Pages
iv. Must have Immediate or Scheduled Campaign Broadcast options
v. Must have the capability to conduct Distributed Broadcast across user list

e) Reporting and Management

i. Must have an Outlook add-in that enables users to report suspected phishing and spam messages with one click right from within Outlook.
ii. The Outlook Add-in should work for Office 365 Business subscription (Exchange online) mail accounts.
iii. The solution dashboard should provide at-a-glance campaign results on user susceptibility and allows you to measure overall risk levels across your entire user group with live Awareness Factor data, including:
iv. Top level campaign results
v. Organizational trend of caught employees and reporters
vi. Total users caught
vii. Testing coverage
viii. Days since last campaign

ix. Drill–down reports should give deeper insight into performance at an organizational or individual user level.
x. Reports must have an option to export to a CSV file.
xi. The solution should be easy to use and can be easily accessed on any supported browser.
xii. Must have an option to import users manually, from Active Directory or from a CSV file.
xiii. Should have a section that lists the domains and IP addresses that the solution uses to send campaign emails.
xiv. Should have an automated report on phishing and training results

f) Synchronized Security

i. Must be able to connect to vendor's Email Gateway solution to identify users who have been warned or blocked from visiting a website due to its risk profile.
ii. Must be able to enroll risky users in targeted user education training programs with one click.

24. Managed Detection and Response

a) 24/7 Threat Detection and Response

- Must be a fully managed 24/7 service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

b) Ransomware and Breach Prevention Services

i. Must have an expert team that stops advanced human-led attacks and can take action to neutralize threats before they can disrupt your business operations or compromise your sensitive data.
ii. Must be customizable with different service tiers, and can be delivered via vendor-proprietary technology or using your existing cybersecurity technology investments.

c) Cybersecurity Delivered as a Service

Enabled by extended detection and response (XDR) capabilities that provide complete security coverage wherever your data reside, the MDR Service must be able to:

i. Detect more cyber threats than security tools can identify on their own
ii. Must have tools that automatically block 99.98% of threats, which enables MDR analysts to focus on hunting the most sophisticated attackers that can only be detected and stopped by a highly trained human.
iii. Take action on your behalf to stop threats from disrupting your business
iv. MDR analysts detect, investigate, and respond to threats in minutes — whether you need a full-scale incident response or help making accurate decisions.
v. Identify the root cause of threats to prevent future incidents

vi. Must be able to proactively take action and provide recommendations that reduce risk to your organization. Fewer incidents mean less disruption for your IT and security teams, your employees, and your customers.

vii. Vendor must have 500+ threat detection and response experts backed by seven global security operations centers (SOCs).

viii. MDR analysts must execute threat response actions on your behalf to disrupt, contain, and eliminate attackers with an industry-leading average threat response time of 38 minutes—96% faster than the industry benchmark.

d) Machine-Accelerated Human Response

Must be able to fuse machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats with speed and precision.

e) Service Level Targets

i. Must have established Service Level Targets (SLTs) to ensure that the team is meeting your expectations and providing the best security service to protect your business. SLTs are designed to provide guidelines around timing expectations for case creation and response actions resulting from investigations.

ii. Must have the following SLTs:

   a. Target time for Case Creation - 2 minutes from Detection

   b. Target time for initial Response Action - 30 minutes from Case creation

f) Managed Detection and Response Dashboard

i. Must have dashboard that shows a summary of threats recently detected and investigated.

ii. Must have an Action required banner on the dashboard that is shown when there is a notification about an incident or incidents.

iii. The dashboard must have a Cases section where notification details can be reviewed.

iv. The dashboard should also include the following:

v. Detections by time of day (UTC) heat map that shows the level of detections each hour.

vi. Total detections by operating system that shows the number of detections for each OS.

vii. MITRE ATT&CK techniques chart that shows a breakdown of attacks according to the classifications used in the MITRE knowledge base.

viii. Detections classification summary that lists the five most frequently-detected types of malicious behavior, along with the number of each.

ix. Most investigated devices that shows the devices we've investigated most frequently.

x. Active cases that lists Managed Threat Response cases (investigations into potential threats) that are currently active.

xi. Must have a Report History section where Weekly and Monthly reports can be accessed and provide insights into security investigations, cyber threats, and security posture.

g) Threat Response Mode

i. Must let you decide and control how and when potential incidents are escalated, what response actions (if any) you want us to take, and who should be included in communications.

ii. There are 2 Threat Response Mode options, regardless of whether you subscribed to MDR or MDR Complete:

a. *Collaborate* - The Collaborate Threat Response Mode must send you notifications of observed activities, and corresponding recommendations. The MDR Ops team will investigate but no response actions will be taken without your consent or active involvement. Selecting Collaborate gives you the option to have some response actions performed by the MDR Ops team and others to be performed by your team or another partner (e.g. an IT managed service provider).

In this mode, the MDR Ops team must receive written authorization before performing response actions. We're your co-pilot and you're the captain.

An option exists under Collaborate that authorizes the MDR Ops Team to operate in Authorize mode in the event that we do not receive an acknowledgment after attempting to reach all your defined contacts by phone.

b. Authorize - The Authorize Threat Response Mode must send notifications of observed activities, but the MDR Ops team will proactively manage all containment actions (with full neutralization for MDR Complete customers) on your behalf and inform you of the action(s) taken. Selecting Authorize means you want us to handle as much workload as possible, notify you of the response actions taken, and only escalate things that require specific actions from you or your team that we are unable to take. In this case, we act as the captain.

h) Service Tiers

Must have service tiers available that can provide a comprehensive set of capabilities for organizations of all sizes and maturity levels.

i) MDR Essentials

a. 24/7 expert-led threat monitoring and response
b. Compatible with third-party security products
c. Weekly and monthly reporting
d. Monthly intelligence briefing that provides insights into the latest threat intelligence and security best practices
e. Account Health Check
f. Expert-led threat hunting

g. Threat containment: attacks are interrupted, preventing spread
h. Uses full vendor XDR agent (protection, detection, and response) or vendor XDR Sensor (detection and response)
i. Direct call-in support during active incidents

j) MDR Complete - Includes all features above, plus the following:

i. Full-scale incident response: threats are fully eliminated
ii. Requires full vendor XDR agent (protection, detection, and response)
iii. Root cause analysis
iv. Dedicated Incident Response Lead
v. Breach Protection Warranty (Covers up to $1 million in response expenses)

k) Integrations

Security data from the following sources can be integrated for use by the MDR operations team at no additional cost. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

Vendor Endpoint Protection*
Vendor Workload Protection*
Vendor Mobile Security**
Vendor Firewall**
Vendor Email Protection**
Vendor Cloud Security**
Vendor Zero Trust Network Access**
Microsoft Security Tools
Microsoft Defender for Endpoint
Microsoft Defender for Cloud
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Entra ID
Microsoft Azure Sentinel
Office 365 Security and Compliance Center

** included with the MDR service*
*** must be purchased and deployed prior to integration with the MDR service*

a. **Microsoft Audit Logs**
Provides information on user, admin, system, and policy actions and events ingested via the Office 365 Management Activity API

b. **Google Workspace**
Ingests security telemetry from the Google Workspace Alert Center API

c. **Third-Party Endpoint Protection – compatible with:**
Microsoft

CrowdStrike
SentinelOne
Trend Micro
Blackberry (Cylance)
Broadcom (Symantec)

l) **90-Days Data Retention**
Retains data from vendor products and third-party solutions in the vendor Data Lake.

m) **Add-On Integrations**
Security data from the following third-party sources can be integrated for use by the MDR operations team via the Purchase of Integration Packs. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

a. **Vendor Network Detection and Response (NDR)**
   1. Continuously monitor activity inside your network to detect suspicious actions occurring between devices that are otherwise unseen
   2. Compatible with any network via SPAN port mirroring

b. **Firewall – compatible with:**
Check Point
Cisco Firepower
Cisco Meraki
Fortinet
Palo Alto Networks
SonicWall
WatchGuard

c. **Public Cloud – compatible with:**
AWS Security Hub
AWS CloudTrail
Orca Security

d. **Identity – compatible with:**
Auth0
Duo
ManageEngine
Okta

e. **Network – compatible with:**
Cisco Umbrella
Darktrace
Secutec
Skyhigh Security
Thinkst Canary

f. **Email – compatible with:**
Proofpoint
Mimecast

g. **Backup and Recovery – compatible with:**
Veam Backup & Replication

h. **1-Year Data Retention**
Retains data from vendor products and third-party solutions in the vendor Data Lake.

n) **MDR Guided Onboarding**
For an additional purchase, MDR Guided Onboarding is available for remote onboarding assistance. The service provides hands-on support for a smooth and efficient deployment, ensures best practice configurations, and delivers training to maximize the value of your MDR service investment. You are provided a dedicated contact from the vendor Professional Services organization, who will be with you through your first 90 days to make sure your implementation is a success.

MDR Guided Onboarding includes:

i. *Day 1 - Implementation:*
- Project kickoff
- Configure vendor web console and review of features
- Configure MDR integrations
- Configure vendor NDR sensor(s)
- Enterprise-wide deployment

ii. *Day 30 - XDR Training:*
- Learn to think and act like a SOC
- Understand how to hunt for indicators of compromise
- Gain an understanding of using our MDR platform for administrative tasks
- Learn to construct queries for future investigations

iii. *Day 90 Security Posture Assessment*
- Review current policies for best practice recommendations
- Discuss features that are not in use that could provide additional protection
- Security assessment following NIST framework
- Receive summary report with recommendations from our review

o) **Breach Protection (MDR Complete)**
- Must be included in the MDR Complete service tier
- Must not have a geographical restrictions

p) **Security posture requirements for qualified reimbursement:**
- Must keep devices, applications, and OS patched and up to date

- Must maintain up-to-date and properly installed and configured vendor Endpoint Protection across all eligible devices
- Must maintain MFA authentication for RDP use

25. Managed Risk

a) **Managed Service Delivered by Vulnerability Experts -** Provides a fully managed service delivered by a dedicated team of experts, including certified vulnerability analysts.
b) **Attack Surface Visibility -** discovers your internet-facing assets and analyzes your external attack surface.
c) **Continuous Risk Monitoring -** Provides expert guidance and helps set remediation priorities for your business.
d) **Prioritize Vulnerabilities -** Identifies and prioritizes exposures using extensive vulnerability coverage and risk-based prioritization.
e) **Identify New Risks Fast -** Proactively notifies your team when new critical vulnerabilities are discovered that affect your assets.
f) **Comprehensive Reporting -** Provides detailed attack surface and vulnerability reports that enables you to stay informed and gain a better understanding of your organization's digital footprint and associated risks.
g) **Collaborates with MDR -** Works seamlessly with the Managed Detection and Response service. Conveniently manage cases alongside your MDR investigations in one unified console.
h) **Service Onboarding**

Day 1 – Onboarding - will guide you through the simple steps to provide your authorized contacts, and details of your organization's domains, and schedule your automated scans.

Day 30 – Baseline Review - initial baseline review meeting enables the Managed Risk team to understand what's important to your organization and review the results of your first vulnerability scans.

Quarterly Reviews - Scheduled meetings with the Managed Risk team, enable you to review recent findings, learn about the current exploitation landscape, and discuss recommendations and remediation priorities.

SCOPE OF WORKS	
	1. Installation and Testing
	The winning bidder must:
	a. Supply, delivery, installation and configuration of endpoint security with manage threat response and email protection
	b. Conduct Project Management
	c. Conduct initial Project Kick Off.
	d. Create Project team for IC and winning bidder.

	e. Formulate Project Implementation Plan, Prepare, Present and Sign off Scope of Work (SOW) to IC.
	f. Conduct Final Project Kick Off
	g. Set all necessary settings and configuration of new endpoint to ensure that they are compatible and connected to existing IC setup.
	h. Provide all the needed components to complete the setup and connections.
	i. Conduct intensive testing together with IC IT personnel to achieve the functionality and benefits of the new equipment. Provide actual results of the testing of the installed endpoints.
	j. Shall be tested for Twenty-Four (24) hours of continuous use upon installation and commissioning.
	k. Corrections shall be within ten (10) working days prior to commissioning.
	l. All levels of testing shall be conducted at the site.
	m. Performance tuning shall be conducted to ensure resilient performance of the endpoint.
	2. Warranty/Maintenance/Technical Support/Availability
	a. The endpoint security with manage threat response and email protection shall cover warranty, labor, and on-site visit for two (2) years.
	b. On call support shall be available 24 hours a day, 7 days a week. A two (2) hours response from time of the call (through telephone call) shall be provided. Onsite support must have a response time of not more than four (4) hours from the time of the call-in cases where in the phone support could not solve the problem during the duration of the warranty.
	c. Warranty must include firmware updates, software patches, and driver updates, if available, during the duration of the warranty.
	d. Installation and configurations of endpoint security with manage threat response and email protection must be free of charge to procuring entity.
	e. Provide RCA (Root Cause Analysis) after solving the problem.
	f. Provide endpoint security with manage threat response and email protection reconfiguration, if needed, with no extra cost to procuring entity.
	g. Reinstall corrupted software caused by hardware failure.
	h. The warranty period for the hardware and software shall commence upon issuance of certificate of acceptance by the Procuring Entity.
	i. Provide Pro-active maintenance support that automatically generates reports and sends notification to the manufacturers 24x7 call support centers in cases of system (hardware and software) abnormality, so that components will be replaced, and errors fixed before failure occurs.
	j. Bidder must provide procedures on support and problem escalation.

	k. Bidder must have a 24 x 7 helpdesk system via phone and email support. Helpdesk system must automatically track, monitor, and escalate open case until the issue is declared resolved and closed. Vendor should be ready for a site visit and show how their current helpdesk system works.
	l. Helpdesk service facility shall include:
	i. Technical engineer dispatch facility
	ii. Case logging and monitoring
	iii. Support history and reporting
	iv. Must have proper Helpdesk Support System in place to accommodate IC technical request. Helpdesk system will provide ticket for each technical request or issues and will provide continues status and report until the resolution. Helpdesk must be available 24x7 including Saturday, Sunday and holidays. Helpdesk system should be available for site visit as IC may require.
	3. Training
	a. Must have over 60 interactive training modules that will educate users about specific threats, such as suspicious emails, credential harvesting, password strength, and regulatory compliance.
	b. Training campaigns without attack simulation should be available.
	c. Must have the option to redirect caught users to your own hosted training material.
	4. Customization and Scheduling
	a. Must have Training Reminder Emails
	b. Must have customizable Landing Pages
	5. Reporting and Management
	a. Must have an Outlook add-in that enables users to report suspected phishing and spam messages with one click right from within Outlook.
	b. The Outlook Add-in should work for Office 365 Business subscription (Exchange online) mail accounts.
	c. The solution dashboard should provide at-a-glance campaign results on user susceptibility and allows you to measure overall risk levels across your entire user group with live Awareness Factor data, including:
	i. Top level campaign results
	ii. Organizational trend of caught employees and reporters
	iii. Total users caught
	iv. Testing coverage
	v. Days since last campaign
	d. Drill–down reports should give deeper insight into performance at an organizational or individual user level.

	e. Reports must have an option to export to a CSV file.
	f. The solution should be easy to use and can be easily accessed on any supported browser.
	g. Must have an option to import users manually, from Active Directory or from a CSV file.
	h. Should have a section that lists the domains and IP addresses that the solution uses to send campaign emails.
	6. Synchronized Security
	a. Must be able to connect to vendor's Email Gateway solution to identify users who have been warned or blocked from visiting a website due to its risk profile.
	b. Must be able to enroll risky users in targeted user education training programs with one click.
	7. Virtual Training
	a. Vendor must provide appropriate level of knowledge transfer to IC support personnel operations
	8. Documentation
	The winning bidder must provide:
	a. User and system manuals
	b. Technical materials
	c. Documented step-by-step procedure
	d. Complete documentation of the endpoint security with manage threat response and email protection
	e. Network Diagram documentation of the endpoint security with manage threat response and email protection
	9. Certification
	a. The winning bidder must secure certification from the manufacturer that they are certified reseller or partner of the proposed equipment.
	b. The winning bidder must secure certification from the manufacturer that they are certified to provide technical service support.
	c. Assigned certified and experience Project Manager who will handle the project.
	d. Bidder must utilize experienced and trained technical support engineers under its direct employment and supervision in rendering the required maintenance.
	e. The solution being offered must belong to **Leader's Quadrant of Gartner's 2023 Magic Quadrant for Endpoint Protection Platforms**
	f. Vendor must be named a Leader in Frost & Sullivan’s 2024 Frost Radar for Global Managed Detection and Response
	g. Vendor must be named Customers’ Choice for Managed Detection and Response (MDR) in the Inaugural Gartner Voice of the Customer Peer Insights Report.
	h. Vendor must be named a Leader for Endpoint Protection, EDR, XDR, Firewall, and MDR in G2’s Winter 2024 (December 2023) Reports

	i. Vendor must be named a Leader in the 2024 IDC MarketScape for Worldwide Managed Detection and Response (MDR) Services.
	10. Bidder's Qualification and Certifications
	a. To ensure comprehensive support capabilities for the proposed endpoint solution, the bidder must be of **highest/tier 1/platinum partnership** with the solution manufacturer. This partnership level would ensure that the partner of the Bureau would have an in-depth technical resources, training, and support programs directly from the manufacturer.
	b. The bidder must submit a valid certification directly from the manufacturer of the proposed endpoint protection platform solution. This certification shall confirm that the bidder is a **certified reseller or authorized partner** for the offered solution.
	c. The bidder must provide a certification from the manufacturer indicating their status as a **certified provider of technical support services** for the proposed solution.
	d. Bidder must have the capability to deliver technical support services for the proposed solution. This requires the direct employment and supervision of a minimum of **four (4) experienced and fully trained technical support engineers**. A certification must be provided.
	11. Acceptance
	a. Acceptance shall be issued upon compliance of the foregoing. IC IT personnel shall review and conduct testing on the delivered endpoint security with manage threat response and email protection on its functions. All deliverables mentioned above shall be checked by IC and complied by the winning bidder before the final acceptance and turnover of the project.
	12. Delivery Address, Date, and Installation
	a. The winning bidder must deliver the goods not more than fifteen (15) days upon receipt of the **<u>Notice To Proceed (NTP)</u>** and must delivered at 1071 United Nations Avenue, Ermita, Manila City.

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 and current **Certificate of PhilGEPS Registration Certificate (Platinum Membership) (all pages) in accordance with Section 8.5.2** of the IRR (pursuant to GPPB Resolution No. 15-2021 dated 14 October 2021);

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 (**per IC Form No. 3**); **and**

□ (c) Statement of the bidder's Single Largest Completed Contract (SLCC) of similar nature within the last five (5) years from the date of submission and receipt of bids equivalent to at least fifty (50%) of the total ABC (**per IC Form No. 4**); **and**

Similar in Nature shall mean ***"Subscription to Endpoint Security with Managed Detection and Response"***

Any of the following documents must be submitted/attached corresponding to the listed completed largest contracts as per IC Form No. 4:

i. Copy of End User's Acceptance; or
ii. Copy of Official Receipt/s or Sales Invoice or Collection Receipt/s

□ (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 (**per IC Form No. 8**); **and**

□ (e) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, (**per IC Form No. 6**); **and**

□ (f) Original duly signed Omnibus Sworn Statement (OSS);
<u>and</u> 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 (**per IC Form No. 7**)

<u>Financial Documents</u>

□ (g) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);
<u>or</u>
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 (**per IC Form No. 5**);
<u>or</u>
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 (**per IC Form No. 1**); **<u>and</u>**

□ (j) Original of duly signed and accomplished Detailed Bid Price Schedule(s) (**per IC Form No. 1-A**).

<u>Other documentary requirements under RA No. 9184 (as applicable)</u>

(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.

BIDDING FORMS

FORM NO.	FORM TITLE
IC Form No. 1	BID FORM
IC Form No. 1-A	DETAILED BID PRICE SCHEDULE
IC Form No. 2	FINANCIAL DOCUMENTS FOR ELIGIBILITY
IC Form No. 3	LIST OF ALL ONGOING GOVERNMENT & PRIVATE CONTRACTS, INCLUDING CONTRACTS AWARDED BUT NOT YET STARTED
IC Form No. 4	STATEMENT IDENTIFYING THE BIDDER'S SINGLE LARGEST COMPLETED CONTRACT SIMILAR TO THE CONTRACT TO BE BID WITHIN THE LAST FIVE (5) YEARS
IC Form No. 5	JOINT VENTURE AGREEMENT
IC Form No. 6	CONFORMITY WITH SECTION VI (SCHEDULE OF REQUIREMENTS) AND SECTION VII (TECHNICAL SPECIFICATIONS)
IC Form No. 7	OMNIBUS SWORN STATEMENT
IC Form No. 8	BID SECURING DECLARATION

IC Form No. 1

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 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 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 : ______________________________

IC Form No. 1-A

For Goods Offered From Within the Philippines
Detailed Bid Price Schedule

Date: ______________________
Project ID No: ______________________

Project: Subscription to Endpoint Security with Managed Detection and Response

Code:
Date of Bidding: ________________
Time of Bidding: ________________

____
____
(Supplier's Name/Address/Tel. No.)

For Goods Offered From Within the Philippines

ITEM	DESCRIPTION	QTY	U/M	Unit Price	Total Price
1	Subscription to Endpoint Security with Managed Detection and Response	1	lot		
				TOTAL BID PRICE, Pesos :	
				Plus 12% RVAT :	
				TOTAL BID PRICE PHP :	

Total Amount in Words :

____

____ ***(PhP)***

Name of Bidder ____________________. ITB Number _____. Page _____ of ___.

____
Signature/Date
Authorized Official/Position

IC Form No. 2

Financial Documents For Eligibility Check

1. Summary of the Applicant Supplier's/Distributor's/Manufacturer's assets and liabilities on the basis of the attached income tax return and audited financial statement, stamped "RECEIVED" by the Bureau of Internal Revenue (BIR) or BIR authorized collecting agent, for the immediately preceding year and a certified copy of Schedule of Fixed Assets particularly the list of construction equipment.

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

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

   NFCC = 15 (current asset s– current liabilities) minus value of all outstanding works under ongoing contracts including awarded contracts yet to be started

   NFCC = PhP ____

Herewith attached are certified true copies of the income tax return and audited financial statement: stamped "RECEIVED" by the BIR or BIR authorized collecting agent for the immediately preceding year and NFCC Computation and/or certificate of commitment from a licensed bank to extend a credit line.

Submitted by:

____
Name of Supplier / Distributor / Manufacturer

____
Signature of Authorized Representative
Date : ______________________________

NOTE:

If Partnership or Joint Venture, each Partner or Member Firm of Joint Venture shall submit the above requirements.

IC Form No. 3

List of all Ongoing Government & Private Contracts including Contracts Awarded but not yet Started

Business Name : ______________________________
Business Address : ______________________________

Name of Contract/ Project Cost	1. Owner's Name 2. Address 3. Telephone Nos.	Nature of Work	Bidder's Role		1. Date Awarded 2. Date Started 3. Date of Completion	% of Accomplishment		Value of Outstanding Works / Undelivered Portion
			Description	%		Planned	Actual	
Government								

Note: The following documents shall be submitted upon post-qualification:

1. *Notice of Award and/or Contract*
2. *Notice to Proceed issued by the owner*

Submitted by : ______________________________
(Printed Name & Signature)

Designation : ______________________________
Date : ______________________________

IC Form No. 4

STATEMENT OF SINGLE (1) LARGEST COMPLETED CONTRACT OF SIMILAR NATURE WITHIN THE LAST FIVE (5) YEARS FROM DATE OF SUBMISSION AND RECEIPT OF BIDS AMOUNTING TO AT LEAST FIFTY PERCENT (50%) OF THE APPROVED BUDGET FOR THE CONTRACT (ABC)

OR

STATEMENT OF AT LEAST TWO (2) CONTRACTS OF SIMILAR NATURE WITHIN THE LAST FIVE (5) YEARS FROM THE DATE OF SUBMISSION AND RECEIPT OF BIDS, THE AGGREGATE OF WHICH SHOULD BE EQUIVALENT TO AT LEAST FIFTY PERCENT (50%) OF THE ABC, AND THE LARGEST OF THESE SIMILAR CONTRACTS MUST BE EQUIVALENT TO AT LEAST TWENTY FIVE PERCENT (25%) OF THE ABC (25%) OF THE ABC

Business Name : ____

Business Address : ____

Name of Contract	1. Owner's Name 2. *Address* 3. *Telephone Nos.*	Nature of Work	Bidder's Role		1. Amount at Award 2. *Amount at Completion* 3. *Duration*	1. Date Awarded 2. *Contract Effectivity* 3. *Date Completed*
			Description	%		
Government						

Note: *Any of the following documents shall be submitted upon post-qualification:*

a) Copy of End User's Acceptance; or
b) Official Receipt/s; or
c) Sales Invoice

Submitted by: ____
(Printed Name & Signature)
Designation: ____
Date: ____

IC Form No. 5

Joint Venture Agreement

KNOW ALL MEN BY THESE PRESENTS:

That this JOINT VENTURE AGREEMENT is entered into By and Between ___________, of legal age, __*(civil status)*__, owner/proprietor of __________________________ and a resident of _________________________.

and –

________________________, of legal age, __*(civil status)*__, owner/proprietor of ____________________ a resident of ______________________________________.

That both parties agree to join together their manpower, equipment, and what is needed to facilitate the Joint Venture to participate in the Eligibility, Bidding and Undertaking of the here-under stated project to be conducted by the Insurance Commission.

1. NAME OF PROJECT CONTRACT AMOUNT

That both parties agree to be jointly and severally liable for the entire assignment.

That both parties agree that ___________________ and/or __________________ shall be the Official Representative of the Joint Venture, and is granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the Joint Venture in the bidding as fully and effectively and the Joint Venture may do and if personally present with full power of substitution and revocation.

That this Joint Venture Agreement shall remain in effect only for the above stated Project until terminated by both parties.

Done this _____ day of ______, in the year of our Lord 20__.

ACKNOWLEDGEMENT

REPUBLIC OF THE PHILIPPINES)
______________________________)S.S.

BEFORE ME, a Notary Public for and in _______________, Philippines, this _______ day of _______________, 20__, personally appeared:

NAME	CTC NO.	ISSUED AT/ON
______________________________	_______________	_________________
______________________________	_______________	_________________

known to me and known to be the same person who executed the foregoing instrument consisting of ________ ( ) pages, including the page whereon the acknowledgment is written and acknowledged before me that the same is his free and voluntary act and deed and that of the Corporation he represents.

WITNESS MY HAND AND NOTARIAL SEAL, at the place and on the date first above written.

Notary Public
Until 31 December 20__
PTR No._______________
Issued at:_______________
Issued on:_______________
TIN No. _________________

Doc. No. _______
Page No. _______
Book No. _______
Series of 20__.

IC Form No. 6

Conformity with Section VI (Schedule of Requirements) and Section VII (Technical Specifications)

(Name of Bidder) hereby undertakes that it shall **COMPLY** with the general requirements stated in Sections VI (Schedule of Requirements) and Section VII (Technical Specifications).

____
Name and Signature of Authorized Official

____
Position

____
Date

REPUBLIC OF THE PHILIPPINES)
___________________________) S.S.

ACKNOWLEDGMENT

BEFORE ME, a Notary Public for and in _________, Philippines, this ___ day of _________________, 20__, personally appeared:

Name	Government-Issued ID & No.	Issued on	Issued at
(SUPPLIER)			

known to me and to me known to be the same person who executed the foregoing instrument consisting of ______ (__) pages, including the page whereon this Acknowledgment is written, all pages signed by both parties and their instrumental witnesses, and they acknowledged before me that the same is their free and voluntary act and deed and that of the Corporation they represent.

WITNESS MY HAND AND NOTARIAL SEAL, on the date and place first above written.

Notary Public

Doc. No. ____;
Page No. ____;
Book No. ____;
Series of 20__.

IC Form No. 7

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]

IC Form No. 8

BID SECURING DECLARATION FORM

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

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

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

To: **REYNALDO A. REGALADO**
Insurance Commissioner
2nd Floor Insurance Commission Bldg.,
1071 United Nations Avenue, Ermita, Manila 1000

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid Securing Declaration.
2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f),of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.
3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:
   a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
   b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and
   c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

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

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

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

Republic of the Philippines

gppb

Government Procurement Policy Board