BIDDING DOCUMENTS FOR THE

SUPPLY AND DELIVERY OF MAINTENANCE FIREYE MANAGE DEFENSE, EMAIL THREAT PROTECTION AND NX APPLIANCE

Project ID No.: BOC-GOODS-2021-08
June 2021

TABLE OF CONTENTS

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

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

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

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

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

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

CDA - Cooperative Development Authority.

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

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

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

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

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

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

GFI – Government Financial Institution.

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

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

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

Infrastructure Projects – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste

management systems, shore protection, energy/power and electrification facilities, national buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

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

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

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

UN – United Nations.

Section I. Invitation to Bid

SECTION I. INVITATION TO BID
"Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance"

1. The Bureau of Customs (BOC) through the authorized appropriations under the CY 2021 General Appropriations Act intends to apply the sum of Eighteen Million Two Hundred Thirty Thousand Eight Hundred Twenty-Five Pesos (Php18,230,825.00) being the Approved Budget for the Contract (ABC) to payments under the contract for the "Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance". Bids received in excess of the ABC shall be automatically rejected at the bid opening.

2. The Bureau of Customs now invites bids for the above Procurement Project. Delivery of the Goods for the period of July 2021 to December 31, 2021 is required specified in the Technical Specification. Bidders should have completed, within three (3) years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

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

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

4. Prospective bidders may obtain further information from the BOC Bids and Awards Committee (BAC) Secretariat and inspect the Bidding Documents at the address given below during office hours from 8:00 a.m. to 5:00 p.m.

5. A complete set of Bidding Documents may be acquired by interested Bidders on June 23, 2021 from the given address and website below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest guidelines issued by the GPPB, in the amount of Twenty Five Thousand Pesos (P25,000.00). The Procuring Entity shall allow the bidder to present its proof of payment for the fees to be presented in person.

6. The BOC will hold a Pre-Bid Conference on July 30, 2021, 2:00 p.m. at the GSD Conference Room, Ground Floor, OCOM Building, South Harbor, Gate 3, Port Area, Manila, and/or through videoconferencing/webcasting via Microsoft Teams, which shall be open to prospective bidders. Sent a Letter of Intent through email and we will send the link via Microsoft Teams.

7. Bids must be duly received by the BAC Secretariat through manual submission at the office address as indicated below on or before July 12, 2021, 1:30 a.m. 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 July 12, 2021, 2:00 p.m. at the given address below. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

10. The BOC 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 Section 41 of RA 9184 and its IRR, without thereby incurring any liability to the affected bidder or bidders.

11. For further information, please refer to:

    BOC-BAC Secretariat
    General Services Division
    OCOM Bldg., South Harbor, Gate 3, Port Area, Manila
    Telefax No. 527-9757
    Email address: **bacsecretariat@customs.gov.ph**

12. You may visit the following websites:

    For downloading of Bidding Documents: **https://customs.gov.ph/bid-opportunities/**

Date issued: June 23, 2021

ATTY. ALVIN H. EBREO, CESE
Chairperson, BOC-BAC

Section II. Instructions to Bidders

TABLE OF CONTENTS

1. Scope of Bid

The Procuring Entity, Bureau of Customs-Bids and Awards Committee (BOC-BAC) wishes to receive Bids for the "Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance" with identification number BOC-GOODS-2021-08.

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 Government of the Philippine (GOP) through the source of funding as indicated below for FY 2021 General Appropriations Act in the amount of Eighteen Million Two Hundred Thirty Thousand Eight Hundred Twenty-Five Pesos (Php18,230,825.00).

2.2. The source of funding is:

a. NGA, the General Appropriations Act or Special Appropriations.

3. Bidding Requirements

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

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

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

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

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

5. Eligible Bidders

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

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

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

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:

a. Subcontracting is not allowed.

7.2. Subcontracting of 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 either at its physical address and/or through videoconferencing/webcasting as indicated in paragraph 6 of the **ITB.**

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 **ITB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

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

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within three (3) years as provided in paragraph 2 of the **ITB** prior to the deadline for the submission and receipt of bids.

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

11. Documents comprising the Bid: Financial Component

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

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

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

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

12. Bid Prices

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

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

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

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

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

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

b. For Goods offered from abroad:

i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

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

13. Bid and Payment Currencies

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

13.2. Payment of the contract price shall be made in:

a. 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 November 9, 2021. 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

15.1 Bidders shall enclose their original eligibility and technical documents described in **ITB** Clause 10 in one sealed envelope marked "ORIGINAL - TECHNICAL COMPONENT", and the original of their financial component in another sealed envelope marked "ORIGINAL - FINANCIAL COMPONENT", sealing them all in an outer envelope marked "ORIGINAL BID".

15.2 Each copy of the first and second envelopes shall be similarly sealed duly marking the inner envelopes as "COPY NO. ___ - TECHNICAL COMPONENT" and "COPY NO. ___ – FINANCIAL COMPONENT" and the outer envelope as "COPY NO. ___", respectively. These envelopes containing the original and the copies shall then be enclosed in one single envelope.

15.3 The original and the number of copies of the Bid as indicated in the **BDS** shall be typed or written in ink and shall be signed by the Bidder or its duly authorized representative/s.

All envelopes shall:

(a) contain the name of the contract to be bid in capital letters;

(b) bear the name and address of the Bidder in capital letters;

(c) be addressed to the Procuring Entity's BAC;

(d) bear the specific identification of this bidding process indicated in the **ITB** Clause 1; and

(e) bear a warning "DO NOT OPEN BEFORE…" the date and time for the opening of bids.

(f) Each envelope must be duly signed by the authorized representative.

15.4 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.

[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.

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

16. Deadline for Submission of Bids

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

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 **ITB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

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

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

18. Domestic Preference

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

19. Detailed Evaluation and Comparison of Bids

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

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

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

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

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

20. Post-Qualification

20.1. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, that it is one of the eligible bidders who have submitted bids that are found to be technically and financially compliant,}the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**. The LCB shall likewise submit the required documents for final Post Qualification.}

21. Signing of the Contract

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

Section III. Bid Data Sheet

ITB Clause	
1	The Procuring Entity is the Bureau of Customs. The name of the Contract is "Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance" The identification number of the Contract is BOC-GOODS-2021-08
2	The Funding Source is The Government of the Philippines (GOP) through the authorized appropriations under the CY 2021 General Appropriations Act in the amount of Eighteen Million Two Hundred Thirty Thousand Eight Hundred Twenty-Five Pesos (Php18,230,825.00).
5	Only Bids for Bidders found to be legally, technically, and financially capable will be evaluated as defined in ITB Clause 5.1.
5.2	Foreign bidders are not allowed.
5.3	The bidder must have completed, three (3) years prior to July 12, 2021 single contract that is similar to the project at hand and whose value must be at least fifty percent (50%) of the ABC to be bid. Bidders shall include in their Bid a photocopy of Single Largest Completed Contract, Notice of Award (NOA), Notice to Proceed (NTP), Technical Inspection and Acceptance Committee (TIAC) Report or Certificate of Final Acceptance Report or equivalent in the Private Sector. Failure to submit a copy of Single Largest Completed Contract with proof of Completion or a failure against the veracity of such shall be a ground for disqualification of the bidder for award and forfeiture of the bid security. For this purpose, similar contract shall refer to "Provision of Cyber Security Service and Support"
5.4	Joint Venture is not allowed.
7.1 (a)	Subcontracting is not allowed.
8	The BOC will hold a Pre-Bid Conference on July 30, 2021, 2:00 p.m. at the GSD Conference Room, Ground Floor, OCOM Building, South Harbor, Gate 3, Port Area, Manila, and/or through videoconferencing/webcasting via Microsoft Teams, which shall be open to prospective bidders.
14.1	The bid security shall be in the form of a Bid Securing Declaration or any of the following forms and amounts:

	1. The amount of not less than **P364,616.50** or 2% of the ABC if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; 2. The amount of not less than **P911,541.25** 5% of the ABC if bid security is in Surety Bond.
15	Each Bidder shall submit one (1) original and two (2) copies of the first and second components of its bid with proper tabs. All papers/pages of the Bid (Original and Photocopies), including attachments thereto such as brochures, shall be countersigned/initialed each page by the bidder or his/her duly authorized representative. "Failure to comply with the above instructions would rate the bids as failed"
19.2	Partial bid is not allowed. The goods are grouped in a single lot and the lot shall not be divided into sub-lots for the purpose of bidding, evaluation, and contract award.
20.1	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 the following documents: 1. Latest Income Tax Return and business Tax Return with proof of payment *(filed and paid through BIR Electronic Filing and Payment System (eFS)*; *2.* VAT Returns (Form 2550M and 2550Q) or Percentage Tax Returns (2551M) with proof of payment covering the last 6 months; and 3. Other appropriate licenses and permits required by law. 4. A certification that they are a FireEye Affiliate or an Authorized/Licensed Vendor to carry their services in the country.
21.1	No further instruction

Section IV. General Conditions of Contract

TABLE OF CONTENTS

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

GCC Clause	
1	**Delivery and Documents –** The Goods shall only be delivered by the supplier as indicated in Section VI. Schedule of Requirements. Moreover, the delivery schedule as indicated in Section VI. Schedule of Requirements may be modified at the option of the Procuring Entity, with prior due notice, written or verbal, to the Supplier.
2.2	Payment shall be made only upon submission of the required Documents. Partial Payment is not allowed.
3	No further instructions.
4	Inspections and Tests Complete Goods shall be inspected and/or tested by the End User based in Section VII. Technical Specifications
5	Six (6) months upon receipt of Notice to Proceed
6	No additional provision.

Section VI. Schedule of Requirements

Item	Description	Delivery Date
1 lot	Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance	Deliver within five (5) calendar days after receipt of Notice to Proceed to be delivered in ICT Office, G/F ICT Bldg., South Harbor, Port Area Maila

I hereby commit to comply and deliver the above requirements.

_____
Name of Company (in print)

_____
Signature of Company Authorized Representative

_____
Name & Designation (in print)

_____
Date

Section VII. Technical Specifications

STATEMENT OF COMPLIANCE
TO TECHNICAL SPECIFICATIONS

The bidder must state in the last column opposite each parameter and required specifications either **"Comply" or "Not Comply".** All pages shall be properly signed. Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate.

SPECIFICATION	STATEMENT OF COMPLIANCE
1. Components: 1.1. Six (6) months renewal of the existing FireEye Managed Defense subscription: 1.1.1. Security Event Monitoring and Analysis 1.1.2. Historical Detections 1.1.3. MDR Portal 1.1.4. Threat Intelligence Portal 1.1.5. Threat Hunting Services 1.1.6. Rapid Response Services 1.1.7. Assigned MDR Consultant 1.2. Six (6) months renewal of maintenance support and subscription license of the following existing FireEye Network Security Solution deployed in seven (7) identified port offices. 1.2.1. Product code, Product name, Qty: 1.2.1.1. RN-2500NX1-PTM-1Y, Sppt 2500 NX 50Mbps PTM, Qty=5 1.2.1.2. RN-2500NX1-2WDTI-1Y, DTI 2500 NX 50Mbps 2- way, Qty=5 1.2.1.3. RN-2500NX2-PTM-1Y, Sppt 2500 NX 100Mbps PTM, Qty=2 1.2.1.4. RN-2500NX2-2WDTI-1Y, DTI 2500 NX 100Mbps 2- way, Qty=2 1.2.2. Device Serial Numbers: 1.2.2.1. AD1824AQ097 1.2.2.2. AD1830AQ061 1.2.2.3. AD1830AQ053 1.2.2.4. AD1822AQ018 1.2.2.5. AD1824AQ100 1.2.2.6. AD1824AQ099 1.2.2.7. AD1824AQ098 1.3. Six (6) months renewal of maintenance support and subscription license for the existing FireEye Email Security Cloud Edition (Email Threat Protection- ETP) with 1000 mailbox licenses. 1.3.1. Product Code, Product Name, Qty:	

1.3.1.1. RN-ETP-AVAS-PTM-1999-1Y, Email Threat Prevention Cloud w/ AV/ AS PTM, Qty=1000	
2. Technical Specifications: 2.1. Manage Defense and Response (MDR) Service In this section, the following items indicate the technical capabilities and functions of the existing Managed Detection and Response Subscription that need to be renewed. 2.1.1. The service must provide continuous compromise assessment thru threat hunting and response using the existing Network advanced threat protection, Email security cloud edition, Endpoint detection and response (EDR), Network Forensics platform, and central management device of the Bureau of Customs (BoC) to early detect signs of intrusion, rapidly investigate and provide the answers needed to respond effectively. 2.1.2. The service must be familiar with and be able to perform forensics/investigation and threat hunting using the existing Endpoint Detection & Response (EDR) solution. 2.1.3. The service must be able to perform forensics/investigation using the existing Network Forensics / Packet Capture solution. 2.1.4. The MDR service provider must be able to assists and resolve any technical issues (both hardware or software issues) related to the existing Network Forensics/Packet Capture solution. 2.1.5. The MDR service provider must be able to manage the administration and maintenance of the existing Network Forensics/Packet Capture solution. 2.1.6. The MDR service provider must provide device management of the existing Network Forensics/Packet capture solution. The device management must include monitoring the device baseline configuration and features, after-sales support, and software upgrades to its latest maintenance release. 2.1.7. The MDR service provider should provide Return Merchandise Authorization-RMA (replacement) of the existing Network Forensics/Packet capture solution in the event of a hardware failure. 2.1.8. The MDR detection through response should occur within hours to drastically minimize the scope, impact, and cost of a breach. 2.1.9. The MDR service must be operated with security and threat intelligence experts with strong capabilities in deep analysis and forensics of advanced cyber-threats, kill-chains, and attack campaigns. 2.1.10. The MDR service must be able to monitor for advanced threat protection security alerts, breaches, anomalies, and advanced persistent threats, regardless of the number of nodes/users. 2.1.11. The MDR service must notify for critical security alerts, breaches, anomalies, and advanced persistent threats, based on assessed severity and in real-time. 2.1.12. The MDR service must provide real-time, in-depth, contextual, and non-trivial analysis of advanced and	

zero-day threats with highly actionable mitigation, to protect from Advanced Persistent Threat (APT) attacks or determine if such attacks are currently occurring or have occurred in the past. 2.1.13. When the investigation reveals a compromise, the vendor should send a compromise report related to that activity within one (1) hour from the time the vendor makes that determination. 2.1.14. In addition to asset details, summary, threat context, and attacker details, the compromise report must also provide recommended actions, Analysis, Investigation findings, and evidence. 2.1.15. The investigation report must include asset details such as the type of asset (ie. endpoint), IP address, Agent ID, domain, Operating System, Agent version, etc. 2.1.16. When a more comprehensive investigation is necessary, the service must be able to pivot into remote live response or incident response seamlessly using the existing EDR solution to determine the full extent of attacker activity in the customer environment and to provide complete recommendations and remediation actions. 2.1.17. The MDR service must proactively hunt for signs and indicators of compromise and pursue adversaries in the network and endpoints using advanced analytical techniques. 2.1.18. The MDR service must include proactive hunting of new tactics, techniques, and procedures (TTPs) that may evade traditional detection or prevention mechanisms. 2.1.19. The MDR service must have defined hunting techniques, both in-network and endpoint, that are implemented using the capabilities from the existing Network Anti-APT/Forensic solution and existing EDR. 2.1.20. The service must provide Hunting services mapped to the MITRE ATT&CK Framework. 2.1.21. The service must provide daily Hunting services based upon a collection of one or more missions, run on a defined interval, targeting a specific data source or sources. 2.1.22. The service must provide Hunting services that minimize endpoint performance impact. 2.1.23. The service must provide daily hunts, providing a greater opportunity to identify suspicious behavior and disrupt Threat Actors as early as possible, reducing dwell time. 2.1.24. The service must deliver responsive timely hunting that can rapidly incorporate emerging TTPs. 2.1.25. The service must provide visibility and transparency into the Hunting service with detailed information about missions, techniques, and completion status provided in a portal. 2.1.26. The service should provide a threat hunting report every month providing the ff. details: 2.1.26.1. Hunting results per month providing the threats identified and investigated; 2.1.26.2. Details about the specific MITRE ATT&CK Techniques/sub-techniques that the service	

provider needs to hunt in the customer's environment; 2.1.26.3. Hunting hypothesis; 2.1.26.4. Forensic evidence needs to be analyzed; 2.1.26.5. Threat and relevant intelligence about the techniques/sub-techniques; 2.1.26.6. What threat actors have been associated with the activity; 2.1.27. The service must include reporting of endpoint coverage every month. The report should include the number of checked-in endpoints for the past month. 2.1.28. The service must employ an arsenal of technologies and methodologies to investigate system artifacts, perform full-packet capture, conduct NetFlow analysis, reverse-engineer malware, and inspect emails to detect indicators of compromise. 2.1.29. The service must be able to identify data that was stolen or offer insight into the intellectual property that the attackers are targeting, where possible. 2.1.30. The service must be able to contain compromised devices using the existing endpoint detection and response technology. 2.1.31. The vendor must have the capability to detect lateral movement by attackers on the internal network even if such lateral movement is purely internal and not visible on Internet egress link. 2.1.32. The service must include extended investigation to identify any evidence of previously unknown attacker activity, attacker lateral movement, and data staging/theft. 2.1.33. The service must include the status report of the security events (or alerts) if the events have been under review, being reviewed, or being reported. The status report should be available and viewable via the MDR service web portal. 2.1.34. The service must have exceptional threat intelligence to threat actor tactics, modus operandi, and geopolitical context gleaned from front-line incident response work. The service must also have the ability to foresee and predict attacker trends based on gathered intelligence. 2.1.35. The MDR vendor must have an established track record in performing large-scale cyber forensic investigations, specifically involving cyber criminals and nation-state attackers. 2.1.36. The MDR vendor must have deep intelligence of cyber threat actors especially those related to cyber espionage. 2.1.37. The MDR service must fulfill the role of a trusted advisor, engage in information sharing against advanced threat actors through regular contact, and offer service performance feedback and reports, customized risk analyses, and routine delivery of intelligence reports. 2.1.38. The MDR service must provide access to a trusted security advisor, who acts as the go-to security and incident response subject matter expert and specialist who handles all aspects of customer communication and service delivery.	

2.1.39. The MDR service must include community protection with industry experts who are constantly scanning for and reacting to the emerging threats, latest attacks, geopolitical triggers, and cyber events across multiple countries and industries. 2.1.40. The MDR service must be available 24x7 using a follow-the-sun model for global coverage, with Security Operations Centers (SOC) in the major geographies viz. Americas, Europe, and the Asia Pacific. 2.1.41. The MDR service must monitor system health for the existing advanced threat protection solutions, Network Forensics, and EDR solution. The monitoring includes aspects like power supply and fan failure, Redundant Array of Independent Disks (RAID) abnormalities, high system temperature, and excessive disk space usage. The vendor should provide Customers with notifications of system health issues such as connectivity problems. 2.1.42. The MDR service provider must provide an MDR service web portal that contains compromise reports with the functionality to perform remote containment of hosts (servers/PCs/Laptops). 2.1.43. The MDR service must have an assigned trusted security advisor who will be the primary point of contact and provide context on the threats that have been reported as well as provide recommendations on how to increase their security posture. Their threat briefings must contain: 2.1.43.1. Current Engagement Status 2.1.43.2. Investigations / Reporting Q&A 2.1.43.3. Appliance & Device Health 2.1.43.4. News / Outstanding Items 2.1.43.5. Hunting statistics or results from the previous month 2.1.43.6. Recent Intel on threat actors impacting the financial sector 2.1.43.7. Tales from the Trenches 2.1.44. The MDR service upon confirmation of the compromise report must answer: 2.1.44.1. What happened within the environment that prompted them to be notified? 2.1.44.2. What do other technologies tell them about the activity? 2.1.44.3. What alerts, if any, did other appliances generate? 2.1.44.4. What other data, if any, did our investigative appliances log? 2.1.44.5. Did the event activity result in a compromise? 2.1.44.6. Why do they think the event is malicious or suspicious? 2.1.44.7. What do they know about the threat actors associated with the event? 2.1.44.8. What is recommended to do about the activity? 2.1.45. The MDR service must provide access to the threat intelligence portal that contains detailed information on TTPs for advanced threat actors. 2.1.46. The MDR service provider must have operational advanced SOCs in different locations throughout the world, delivering 24x7.	

2.1.47. The MDR service must include investigation of ongoing or historical evidence of attacker activity in the environment, determining the scope of affected networks, systems, users, applications, or data. 2.1.48. The MDR service must include an investigation of any evidence of previously unknown attacker activity. 2.1.49. The MDR service must include investigation of any evidence of attacker activity affecting more than one endpoint. 2.1.50. The MDR service must include investigation of any evidence of attacker lateral movement or data staging/theft. 2.1.51. The MDR service provider must be able to leverage and use the existing EDR solution to rapidly identify systems that had been accessed by threat actors using legitimate but compromised domain credentials. 2.1.52. The MDR service provider must be able to leverage and use the existing EDR solution to investigate the lateral movement of threat actors within the windows enterprise environments by aggregating historical logon activity and able to monitor the threat actor activity. 2.1.53. The MDR service must have a web portal that allows interaction on reported threats between the customer and the MDR service provider. 2.1.54. The MDR service must offer a portal that is intuitive and user-friendly and allows an unlimited number of user accounts. The vendor should ensure the portal availability for 99.9% of the time during each calendar month. 2.1.55. The service portal must support native two-factor authentication (2FA) to verify user account and access privileges. 2.1.56. The service portal must include SMS messaging for two-factor authentication (2FA). 2.1.57. The service portal must support the restriction of user access using an email domain whitelist, allowing only a specific email domain to access the portal. 2.1.58. The service portal must support a notification feature that allows users to receive important communications about investigations, appliance health, service announcements, and endpoint containment. 2.1.59. The service portal dashboard must display the hunting techniques applied by the MDR service provider in the customer's environment. 2.1.60. The service portal must have a dashboard that provides visibility into how many endpoints are connected to the MDR service and provides endpoint service status in real-time. 2.1.61. The service portal must provide system health information on all of the appliances/technologies supported by the MDR service, including license and software status and the location of any appliance that requires provisioning or is listed in critical condition. 2.1.62. The service portal must provide access to investigations and incident reports performed by the MDR service provider. 2.1.63. The service portal must provide information and visibility of the number of endpoints/hosts that have	

checked in and that were successfully tasked for the past 30, 60, or 90 days. 2.1.64. The service portal must display the number of network sensors that are online, offline, in a degraded state, or in transit. It must also provide sensor location information, visibility on Web, DNS, email traffic, data transfer rate metrics, and details about any investigations associated with the network sensors. 2.1.65. The service portal must support appliance Health visibility of all the network/email/endpoint security appliances connected to the MDR service provider. 2.1.66. The service portal must include an announcement page about important information such as Intel Highlights, Intel insights, and analysis about new cybersecurity threat trends, protection and prevention recommendations 2.1.67. The MDR service provider should include operational Intelligence reports which include the ff: 2.1.67.1. High-level technical reports on specific malware families. These reports may include technical indicators, behavioral information, known campaigns where the malware has been previously used, and attributed actors or groups that have been known to use the malware. 2.1.67.2. High-level overviews of threat actors known and reported by the MDR service provider. 2.1.67.3. The number of investigations by source (network/endpoint/other). 2.1.67.4. Extended, relevant intelligence when a threat actor has been attributed in an incident. 2.1.68. The MDR service portal must have seamless integration with the following existing solution: Network Advanced Threat Protection, Email Security Cloud Edition, Network Forensic, Endpoint Detection & Response (EDR), and Central Management device. The MDR service provider must be responsible for the support, maintenance, and management of the integration of the mentioned existing solution with the provided MDR service portal. Please provide evidence or documentation (ie. user guides) that the existing solution can seamlessly integrate with the provided MDR service portal. 2.1.69. The service must include an intelligence portal that contains at least 10 years' worth of intelligence on financial and nation-state (APT) threat actors, as well as hacktivists and other cybercriminals. 2.1.70. The MDR service provider must include operational threat intelligence to leverage and use to contextualized the security events coming from the existing advanced threat protection, Email Security Cloud Edition, Network Forensic, and EDR solution. 2.1.71. The MDR service provider must include operational threat intelligence to leverage and use in threat hunting. 2.1.72. The service must include operational intelligence providing access to malware intelligence reporting, including malware profiles, malware quarterly industry reports, actor overviews, and indicator reporting. 2.1.73. The service must include an intelligence portal that allows analysis of suspicious domains and IP	

addresses and submission of suspicious files for an on-demand and automated analysis.

2.1.74. The service must include a daily email summary highlighting cyber threats observed or reported on by public resources, with an assessment of accuracy from the MDR service provider's Intel analysts.

2.1.75. The service must include an intelligence portal that has a dashboard providing the actor, malware, and vulnerabilities activity trends globally.

2.1.76. The intelligence portal must provide access to near real-time trending data on adversary behavior, attacks, and other threat activity.

2.1.77. The intelligence portal must provide access to details of malware, malware families, and malicious tools used by threat actors.

2.1.78. The intelligence portal must provide access to an indicator of compromises, and other observables (both proprietary and open-source), along with associated actors and malware.

2.1.79. The MDR service provider (the principal) should be included in the lists of lists of the participated vendors from the previous MITRE ATT&CK evaluation both for APT3 and APT29.

2.1.80. The MDR service provider (the principal) must be Service Organization Controls (SOC 2) Type II certified. The vendor must be able to provide a report of its compliance (SOC2 Type II report), that includes a description of the control environment, and the external audit result and opinion of its controls that meet the American Institute of Certified Public Accountants (AICPA) Trust Services Security, Availability, and Confidentiality Principles and Criteria.

2.1.81. The PRINCIPAL (Manufacturer) represented by the BIDDER (Vendor/Partner) must have multiple SOC's delivering MDR service capable of remote investigation and response 24x7x365.

2.1.82. The PRINCIPAL (Manufacturer) represented by the Bidder (Vendor/Partner) must be named as Leading vendor in External Threat Intelligence Services by Forrester.

2.1.83. To show the capability of the MDR service provider threat research or labs team, the vendor must have a research team that has published a paper on an APT Threat Actor and must provide a sample published paper on APT Threat Actor from the Principal or Manufacturer. The paper should not be focused on a specific attack, but rather focused on attribution around a specific attack group.

2.2. Email Security Cloud Edition

In this section, the following are the functions and technical capabilities of the existing Email Security Cloud Edition solution that needs to be renewed. The renewal should include maintenance support and license subscription for 1000 mailboxes.

2.2.1. Email Security Cloud Edition must provide the capabilities of a fully secure email gateway that can detect, isolate, and immediately stop URL, impersonation, and attachment-based attacks before they enter an organization’s environment.

2.2.2. The existing Email Security Cloud Edition must seamlessly be integrated with the MDR service portal that contains compromised/investigation reports. The MDR service provider must be responsible for the maintenance of the integration of the mentioned existing solutions with the provided MDR web service portal. 2.2.3. The solution must support supply chain impersonation detection, which provides protection from fraudulent activity between an organization and its vendors. This feature should apply behavioral analysis patterns alongside threat intelligence. 2.2.4. The solution must support various signature, analytics, and machine learning capabilities to detect URL-based email phishing attacks. 2.2.5. The solution must support deep learning capabilities that compile and compare screenshots of trusted and commonly targeted brands against web and login pages referenced by URLs contained within an email. 2.2.6. The solutions must support seamless API integration with Office 365 for auto-remediation. Auto-remediation for the Office 365 is necessary to remove the emails from the user's inbox when a retroactive alert is generated by the solution. 2.2.7. The solutions must support an auto-remediation policy to either quarantine, move to an administrator-defined folder, or permanent deletion. 2.2.8. The solution must able to extract suspicious URLs that are embedded in a PDF file within an email message body. If the embedded URL that is extracted from the PDF file is detected as malicious, the solution should immediately block the email from being delivered to the recipient and marks the malicious email for quarantine. 2.2.9. The solution must have protection from advanced evasion techniques (AETs) that use malformed email as the attack vector. This attack attempts to bypass detection by using emails that have non-compliant headers or non-compliant Multipurpose Internet Mail Extensions (MIME) attachment header formats. 2.2.10. The solution must support retroactive alerting. If the solution delivers an email to end users containing a URL not currently known to be malicious, and the URL is later determined to be malicious, a retroactive alert should be generated by the solution. 2.2.11. The solution must support native dashboard statistics that include a threat map that displays threat locations. 2.2.12. The solution must support integration with Microsoft O365 in inline mode for protection against advanced threats and targeted email attacks. 2.2.13. The cloud solution should be able to retain quarantined emails within 15 days (including the current day). 2.2.14. The cloud solution must be able to retain the alerts within 90 days (including the current day). 2.2.15. The cloud solution must be able to retained events within 31 days (including the current day). 2.2.16. The cloud solution must be able to retain Dashboard Data within 3 months (including the current month). 2.2.17. The cloud solution must be able to retain email trace within 31 days (including the current day).	

2.2.18. The solution must be hosted in the cloud that provides real-time dynamic threat protection without the use of signatures to protect an organization across the email threat vector. The solution must include an end-user portal that allows quarantine management, as well as a review of malicious email and statistics. 2.2.19. The solution must support the BCC deployment mode option that provides passive (out of band) analysis of incoming email to identify advanced threats. 2.2.20. The solution must support inline deployment mode that provides active (inline) analysis of incoming email to identify advanced threats. In this mode, the malicious email should be blocked and quarantined. 2.2.21. The solution must support inline deployment mode that provides active (inline) analysis of incoming email to identify spam, known malware, and advanced threats. In this mode, the malicious email should be blocked and quarantined. 2.2.22. The cloud solution must be able to integrate with on-prem Network Advanced Threat Protection for alerts correlation between web and email vector. 2.2.23. The solution must be able to determine whether the organization's current antivirus solutions in the gateway, server, or endpoint would have detected the malware attached in emails 2.2.24. The solution must support the creation of allow rules to bypass anti-spam filtering of emails based on the following criteria: Sender Reverse Domain, sender country internet domain suffix (ie. .uk), recipient email address, the sender IP address, sender email address, and sender email domain. 2.2.25. The solution must support the creation of deny rules to reject emails based on the following criteria: Sender Reverse Domain, sender country internet domain suffix (ie. .uk), recipient email address, the sender IP address, sender email address, and sender email domain. 2.2.26. The solution must able to drop an email and not deliver it to its intended recipient based on the following criteria: email from a specific email address, email with a specific subject, email with a specific word in the subject or body, email with specific text in the header, and email with an attachment from the predefined file extension types. 2.2.27. The solution must able to quarantine emails based on the following criteria: email from a specific email address, email with a specific subject, email with a specific word in the subject or body, email with specific text in the header, and email with an attachment from the predefined file extension types. 2.2.28. The solution must able to deliver the email to the intended recipient based on the following criteria: email from a specific email address, email with a specific subject, email with a specific word in the subject or body, email with specific text in the header, and email with an attachment from the predefined file extension types. 2.2.29. The solution must able to route the email to another MTA for processing based on the following criteria:	

email from a specific email address, email with a specific subject, email with a specific word in the subject or body, email with specific text in the header, and email with an attachment from the predefined file extension types.

2.2.30. The solution must support daily digests of all the quarantined emails for specific users/recipients. If enabled by the admin, the end-user may be able to release some of the emails him/herself.

2.2.31. The solution must support a native Dashboard displaying the following information:

- 2.2.31.1. Email Traffic Volume, broken down by Received, Accepted, and Delivered
- 2.2.31.2. Chart of the types of email attachments contained in the email messages
- 2.2.31.3. Top Sender email addresses that sent the most suspicious or malicious email for the specified period, along with the total size of content sent
- 2.2.31.4. Top Recipient email addresses that received the most suspicious or malicious email, and the total size of that content
- 2.2.31.5. Top Rule Matches
- 2.2.31.6. Advanced Threats graph of the number of threats over the specified period
- 2.2.31.7. Spam count graphed over the specified time interval, percentage of all accepted emails, and trend
- 2.2.31.8. Viruses Trend information
- 2.2.31.9. Recent Alerts
- 2.2.31.10. Threat Map with a color-coded map of the world which details Countries identified as sources of suspicious emails displayed in color representing the relative threat.
- 2.2.31.11. The above information should be able to be displayed from the last few hours, a day, a week, or the last 30 days.

2.2.32. The solution must provide the following information on every Advanced Threat Alert: Alert ID, Date and Time that the malicious email was received, Sender's email address, Targeted email addresses, Malicious email subject, MD5 hash, Malicious URL, or name of the malicious attachment file, Originating email server that sent the malicious email, Email Status (ie. Quarantined, Released, Delivered, etc.), Threat classification of the malicious attachment or URL, and Severity (High, Medium, Low) of the malicious attachment or URL.

2.2.33. The solution must able to provide information about the dynamic analysis that includes the malware file type, vulnerable applications, and operating systems, whether the organization's current antivirus solution would have detected the malware, message-digest algorithm (MD5), and checksum of the malicious file.

2.2.34. The solution must be able to provide forensic evidence like the detected actual malicious file in a protected archived file and any associated network activity packet captures (VM Captures).

2.2.35. The solution must provide a Malware Communications report that includes the analysis that was performed by the system pertaining to any URL that the malware

communicated with. The information displayed in the report should include the HTTP method, hostname, and port that were used to connect to the malicious site. It should also include a copy of the raw request. 2.2.36. The solution must provide a native report that includes the analysis that was performed by the system on any operating system changes that occurred. The information displayed should include services that were started or stopped, registry keys that were modified, and other system configuration changes that occurred. 2.2.37. The solution must have a Threat Intel report that provides all the intelligence information on a threat detected, including the threat name, risk level, and type associated with a threat. It should also detail the affected software, vulnerability information, and its remediation patches if available. It should give a summary of the risk, information about how it can spread, the known targets for a specific type of malicious content or URL, and the attribution associated with the threat. 2.2.38. The solution must allow the administrator either to release or delete quarantined emails natively via the Web GUI/Portal. 2.2.39. The solution must provide an executive summary report of the email traffic during the selected dates. The report should include data about the type of traffic received and delivered, content analysis, and distribution across threat categories. The report should also include top rejection reasons and information such as the policies violated or matched by the accepted emails. 2.2.40. The solution must able to dynamically analyze the following attached file types: EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives. 2.2.41. The solution must able to dynamically analyze the attached files even with password-protected and encrypted. 2.2.42. The solution must able to detect and block the 3 primary categories of advanced threats in emails: attachment, URL, and impersonation-based attacks. 2.2.43. The vendor ensures that the cloud solution is available (i.e., not experiencing a Service Outage) for 99.9% of the time during each calendar month. 2.2.44. The cloud solution be SOC2 Type II compliant. The vendor must comply with the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC 2) Type II Certification for Security and Confidentiality. 2.2.45. The solution must be cloud-based, with no hardware or software to install. 2.3. Network Advanced Threat Protection Solution The following are the functions and technical capabilities of the existing Network Advanced Threat Protection solution that needs to be renewed. The renewal should include maintenance support and DTI license subscription. The DTI license subscription provides continuous security content updates from the global threat intelligence.	

2.3.1.	The solution should detect zero-day, multi-flow, and other evasive attacks with dynamic, signature-less analysis in a safe and virtual environment.	
2.3.2.	The solution must stop infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.	
2.3.3.	The solution must detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights gathered on the front lines, and threat intelligence.	
2.3.4.	The solution must stop infection, compromise, and intrusion phases of the cyber-attack kill chain by identifying malicious exploits, malware, and command and control (CnC) callbacks.	
2.3.5.	The solution must allow the ingestion of third-party threat intelligence using an industry-standard format STIX to add custom threat indicators.	
2.3.6.	The solution must support analysis of over 140 different file types, including portable executables (PEs), web content, archives, images, Java, Microsoft, and Adobe applications and multimedia.	
2.3.7.	The solution must support the execution of suspicious network traffic against thousands of operating system, service pack, application type, and application version combinations.	
2.3.8.	The solution must support protection against advanced attacks and malware types that are difficult to detect via signatures: web shell uploads, web shell execution, ransomware, crypto miners.	
2.3.9.	The solution must support an Intrusion Prevention System (IPS) with sandbox engine validation which reduces the time required to triage signature-based detection that is traditionally prone to false alerts.	
2.3.10.	The solution must support riskware categorization that separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response.	
2.3.11.	The solution must support global threat intelligence providing concrete, real-time, globally-shared data to quickly and proactively stop targeted and newly discovered attacks.	
2.3.12.	The network advanced threat protection device must support a built-in sandbox engine for dynamic analysis of malicious payloads and file downloads. The sandbox engine should be built-in to each network sensor that will be deployed at the Head office and remote branches.	
2.3.13.	The network advanced threat protection device should support the option to disable the built-in sandbox engine and enable the cloud sandbox analysis instead. This is to double the throughput capacity of the network advanced threat protection device.	
2.3.14.	The solution must detect both known and unknown threats in real-time while also enabling back-in-time detection of threats.	
2.3.15.	The solution must support network outbound scanning, TLS 1.3 inspection capabilities with the SSLi feature, and ICAP blocking. Outbound scanning allows scanning file uploads to O365.	

2.3.16. The solution must include a network threat protection sensor that supports Inline blocking mode or span/tap mode. 2.3.17. Detection appliances must be capable of automatically downloading threat intel from an intelligence cloud. 2.3.18. The solution must be able to generate real-time Malware Notification Alerts via the System Console, Simple Network Management Protocol, Web Alerts via HTTP and/or HTTPS, and Email. 2.3.19. The solution must support signature-less detection that should utilize hardened Virtual Machine technology to positively identify malware, including zero-hour vulnerability exploits, polymorphic payloads, and obfuscated java-script. The virtualization solution shall not be detectable by malware in order to avoid evasion. The Hypervisor must not be an OEM solution such as from VMWare. 2.3.20. The solution must be able to detect and report web exploits by using multiple versions of web browsers and plug-ins. 2.3.21. The solution must be able to detect and report malware downloaded by users or downloaded in the context of a web exploit by using multiple client operating systems with multiple service pack levels. 2.3.22. The solution must be able to detect and prevent advanced Malware, Zero-day attack, and targeted Advanced Persistent Threats without just relying on a Signature database. 2.3.23. The solution must perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks. No information should be sent to third-party systems or cloud infrastructure systems for analysis and detection of Malware. 2.3.24. The solution must have the ability to detect multi-stage attacks and must not be a file-based Sandbox technology that is limited to examining one file at a time in isolation. 2.3.25. The solution must automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware. 2.3.26. The solution must utilize a stateful attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration. 2.3.27. The solution must have the option to share dynamically generated real-time malware intelligence with a global distribution network for detecting both known malware and zero-day, highly targeted attacks used globally. 2.3.28. The solution shall be capable of blocking reliably outgoing communications to C&C servers in order to conserve data integrity on hosts including out-of-band infections. 2.3.29. The solution must have the ability to detect client-side EXPLOITS prior to any complex malware being downloaded to the systems. Complex malware is defined as malware with complex abilities such as key-	

	logging, data-stealing, encrypting, migrating, and installing additional complex malware.	
2.3.30.	The solution must have the ability to remain fully effective when configured to share no data, events, nor any information with the Provider or the Provider's network.	
2.3.31.	The solution must have the capability to block Inbound Infections reliably, as the blocking solution is natively supported.	
2.3.32.	The solution must utilize a Global Intelligence Network to benefit from information gathered by the research efforts of the Provider, in which subscribers receive and optionally share malware intelligence such as zero-day attacks and call-back destinations.	
2.3.33.	The solution must have the ability to display the geo-location of the remote command and control server(s) when possible.	
2.3.34.	The solution must have the ability to report the SRC IP, Destination IP, C&C, URL, BOT name, Malware class, executable run, used protocols, and infection severity of the attack.	
2.3.35.	The solution must have the fail-open capability to allow all packets to pass through the sub-system in case of software, hardware, or power failure when it is deployed inline.	
2.3.36.	The solution must support advanced detection of lateral threats within an enterprise network.	
2.3.37.	The solution must support an advanced correlation and analytics engine with a machine learning module and 120+ unique rules to detect stealthy lateral (east-west) traffic.	
2.3.38.	The solution must detonate malware and ransomware such as WannaCry, as well as other suspicious files and objects moving internally via the SMB protocol.	
2.3.39.	The solution must provide 10 minutes (+/- 5 minutes) of L4 and L7 alert context to quickly investigate attacker activity and conduct forensics analysis.	
2.3.40.	The solution must generate metadata for comprehensive analysis, including the following protocols: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS.	
2.3.41.	The solution must support custom dashboards allowing you to create personal named dashboards that display the dashboard widgets you choose and cover the period you configure.	
2.3.42.	The solution must support an analysis statistics widget that displays the percentage and the number of malicious and non-malicious URLs that have been scanned.	
2.3.43.	The solution must support whitelisting of the domain. You can add FQDN and wildcard domains to a whitelist using the Web UI or CLI.	
2.3.44.	The solution must able to map the alerts to the MITRE ATT&CK Framework to give more context for attack investigation and to allow easier triaging.	
2.3.45.	The solution must support the analysis of content from outbound traffic from the network to the internet.	

2.3.46. `The solution must detect malicious communication by TLS fingerprinting with JA3 between the client and server. 2.3.47. The solution must be able to support full integration with the existing central management appliance to correlate alerts from all the network advanced threat protection appliances for a broader view of an attack and to set blocking rules that prevent the attack from spreading further.	
3. General Qualification of the Service Provider 3.1. The reseller must be a duly certified Partner of FireEye for the past 5 years and must submit the certification to the Product Principal. 3.2. The reseller must have at least 2 FireEye Certified Engineers and must submit a list of Certified Engineers. 3.3. The vendor must have installed base on FireEye solutions for the past 5 years and must provide the list of installed clients. 3.4. The reseller must include six (6) months 24x7 onsite support service and have back-to-back 24x7 web, email, and phone support with the principal. The support service must also cover any reconfiguration assistance. The reseller must provide a detailed escalation procedure as Level 1 and support including contact numbers and email addresses. 3.5. The back-to-back support assistance from the principal must have the following multiple support channels: Live Chat, Web, Phone, and Email Support 24x7. 3.6. The back to back 24x7 support from the principal must include the following: 3.6.1. Target Initial Response Times of thirty (30) minutes for Severity 1 issues (ie. Product rendered unavailable or unresponsive, requires constant restarting, etc.) 3.6.2. Immediate escalation to Advanced Level Three Engineering Support for Severity One cases, provided that the case is also phoned-in to align customer and vendor resources 3.6.3. Maintenance releases for security efficacy and other recommended software bug fixes, as well as new releases for general software updates and non-chargeable enhancements to assure systems, must contain the latest updates and stay compatible with evolving technology 3.6.4. Emergency fixes tested and verified for Severity One issues 3.6.5. RMA of defective products subject to the limited warranty 3.6.6. Access to the secure Support Portal, Community, and Knowledge Base, which includes: 3.6.6.1. A Support Portal for opening and updating support cases for your designated contacts 3.6.6.2. A Community to find and share solutions with FireEye users around the world 3.6.6.3. A Knowledge Base of known issues and articles 3.6.6.4. Online Documentation 3.6.6.5. Patch/update information 3.6.6.6. Field Notices	

Payment Milestone:

Milestones	Period	Amount	Documentary Requirements
Milestone 1	30 days upon issuance of Notice to Proceed (NTP)	90%	Certificate of Acceptance from BOC, Billing Statement
Milestone 2	60 days upon completion of Milestone 1	2.5%	Certificate of Acceptance from BOC, Billing Statement
Milestone 3	30 days upon completion of Milestone 2	2.5%	Certificate of Acceptance from BOC, Billing Statement
Milestone 4	30 days upon completion of Milestone 3	2.5%	Certificate of Acceptance from BOC, Billing Statement
Milestone 5	30 days upon completion of Milestone 4	2.5%	Certificate of Acceptance from BOC, Billing Statement

I hereby commit to comply and deliver the above requirements.

_____

Name of Company (in print)

_____

Signature of Company Authorized Representative

_____

Name & Designation (in print)

_____

Date

Section VIII. Checklist of Technical and Financial Documents

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

☐ (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);
and

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

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

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

Technical Documents

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

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

☐ (h) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;
or
Original copy of Notarized Bid Securing Declaration; and

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

☐ (j) Original duly signed Omnibus Sworn Statement (OSS);
and if applicable, Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

(k) Certificate of Performance Evaluation (Certificate or any document showing project completion with at least satisfactory rating); **and**

(l) Required Licenses or Certification (Business registrations, certificate from FireEye on partnership, PhilGEPS, certificate of completion or equivalent document on previous project (Digital Signatures and/or E Signatures must

be verifiable through timestamp, encryption, envelope ID, PKI or any other means of authentication).

Financial Documents

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

☐ (n) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);

or

A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

25 FINANCIAL COMPONENT ENVELOPE

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

Bid Form

Date: _____
Invitation to Bid[2] Nº: _____

To: [name and address of Procuring Entity]

Gentlemen and/or Ladies:

Having examined the Bidding Documents including Bid Bulletin Numbers *[insert numbers],* the receipt of which is hereby duly acknowledged, we, the undersigned, offer to the BOC, our services for the project, **"Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance"** of in conformity with the said Bidding Documents for the sum of ***[total Bid amount in words and figures]*** or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

Item	Description	TOTAL COST
1 lot	Supply and Delivery of Maintenance FireEye Manage Defense, Email Threat Protection and NX Appliance	

We undertake, if our Bid is accepted, to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements.

If our Bid is accepted, we undertake to provide a performance security in the form, amounts, and within the times specified in the Bidding Documents.

We agree to abide by this Bid for the Bid Validity Period specified in **BDS** provision for **ITB Clause Error! Reference source not found.** and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

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:[3]

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

[3] Applicable only if the Funding Source is the ADB, JICA or WB.

(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 as **per ITB Clause 10 and 11** of the Bidding Documents.

We likewise certify/confirm that the undersigned, *[for sole proprietorships, insert:* as the owner and sole proprietor or authorized representative of *Name of Bidder*, has the full power and authority to participate, submit the bid, and to sign and execute the ensuing contract, on the latter's behalf for the *Name of Project* of the *Name of the Procuring Entity] [for partnerships, corporations, cooperatives, or joint ventures, insert:* is granted full power and authority by the *Name of Bidder*, to participate, submit the bid, and to sign and execute the ensuing contract on the latter's behalf for *Name of Project* of the *Name of the Procuring Entity]*.

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.

Dated this _____ day of _____ 20_____.

[signature]	*[in the capacity of]*

Duly authorized to sign Bid for and on behalf of _____

Statement of Single Largest Completed Contract which is similar in nature

Business Name: _____
Business Address:_____

Name of Contract	Date of the Contract	Kinds of Goods	Amount of Contract	Date of Delivery	End User's Acceptance or Official Receipt(s) Issued for the Contract

Submitted by : _____
(Printed Name & Signature)

Designation : _____

Date : _____

List of all Ongoing Government & Private Contracts including

Contracts awarded but not yet started

Business Name: _____
Business Address:_____

Name of Contract	Date of the Contract	Kinds of Goods	Value of Outstanding Contracts	Date of Delivery
Government				
Private				

Submitted by : _____
(Printed Name & Signature)
Designation : _____

Date : _____

Instructions:

i. State all ongoing contracts including those awarded but not yet started within three (3) years (government and private contracts, which may be similar or not similar to the project being bidded) prior to opening of bids.

ii. If there is no ongoing contract including awarded but not yet started as of the aforementioned period, state none or equivalent term.

iii. The total amount of the ongoing and awarded but not yet started contracts should be consistent with those used in the Net Financial Contracting Capacity (NFCC) in case an NFCC is submitted as an eligibility document.

Contract Agreement Form

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

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

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

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

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

(a) the Supplier's Bid, including the Technical and Financial Proposals, and all other documents/statements submitted (*e.g.* bidder's response to clarifications on the bid), including corrections to the bid resulting from the Procuring Entity's bid evaluation;
(b) the Schedule of Requirements;
(c) the Technical Specifications;
(d) the General Conditions of Contract;
(e) the Special Conditions of Contract;
(f) the Performance Security; and
(g) the Entity's Notice of Award.

3. In consideration of the payments to be made by the Entity to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Entity to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract

4. The Entity hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the time and in the manner prescribed by the contract.

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

Signed, sealed, delivered by _____ the _____ (for the Entity)

Signed, sealed, delivered by _____ the _____ (for the Supplier)

Omnibus Sworn Statement

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

SUBSCRIBED AND SWORN to before me this ___ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no. _____ and his/her Community Tax Certificate No. _____ issued on ____ at _____.

Witness my hand and seal this ___ day of *[month] [year]*.

NAME OF NOTARY PUBLIC
Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorneys No. _____
PTR No. _____ *[date issued], [place issued]*
IBP No. _____ *[date issued], [place issued]*

Doc. No. _____
Page No. _____
Book No. _____
Series of _____

* This form will not apply for WB funded projects.

Bid Securing Declaration Form

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

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

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

I/We, the undersigned, declare that:

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

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

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

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

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

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

SUBSCRIBED AND SWORN to before me this ___ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no. _____ and his/her Community Tax Certificate No. _____ issued on ____ at _____.

Witness my hand and seal this ___ day of *[month] [year]*.

NAME OF NOTARY PUBLIC
Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorneys No. _____
PTR No. _____ *[date issued], [place issued]*
IBP No. _____ *[date issued], [place issued]*

Doc. No. _____
Page No. _____
Book No. _____
Series of _____