BASES CONVERSION AND DEVELOPMENT AUTHORITY

Procurement of the Annual Subscription of Integrated Security Suite - Endpoint Security (Lot A) and Data Security and Analytics (Lot B)

Sixth Edition
July 2020

TABLE OF CONTENTS

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

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

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

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

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

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

CDA - Cooperative Development Authority.

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

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

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

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

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

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

GFI – Government Financial Institution.

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

Goods – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term

"related" or "analogous services" shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

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

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

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

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

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

UN – United Nations.

Republic of the Philippines
Office of the President
BCDA
Bases Conversion and Development Authority

Invitation to Bid
Procurement of the Annual Subscription of Integrated Security Suite - Endpoint Security and Data Security and Analytics

1. The **GOVERNMENT OF THE PHILIPPINES (GOP)** through the **BASES CONVERSION AND DEVELOPMENT AUTHORITY (BCDA)** (hereinafter also referred to as the Procuring Entity), through 2023 BCDA's Corporate Operating Budget intends to apply the sum of Two Million Two Hundred Thousand Pesos and 00/100 (Php 2,200,000.00), inclusive of all applicable taxes and fees **for Lot A** and and Five Million Three Hundred Thousand pesos and 00/100 (Php 5,300,000.00), inclusive of all applicable taxes and fees **for Lot B**, being the Approved Budget for the Contract (ABC) to payments under the contract for the **Procurement of the Annual Subscription of the Integrated Security Suite - Endpoint Security System and Data Security and Analytics**. Bids received in excess of the ABC for each lot shall be automatically rejected at bid opening. Bidders can bid on one or all lots.

Item	Description	Qty	Total Cost (in PhP)
Lot A	**Annual Subscription of the Integrated Security Suite - Endpoint Security System**	1 lot	2,200,000.00
Lot B	**Data Security and Analytics**	1 lot	5,300,000.00
		Total:	PhP 7,500,000.00

2. The BCDA now invites bids for the **Procurement of Annual Subscription of the Integrated Security Suite - Endpoint Security System and Data Security and Analytics**. Delivery of the Goods is required within sixty (60) calendar days from the receipt of Notice to Proceed. Bidders should have completed, within five (5) years prior to 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 competitive bidding procedure using a non-discretionary "pass/fail" criterion as specified in the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act (RA) 9184, otherwise known as the "Government Procurement Reform Act".

   Bidding is limited to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country

the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

4. Prospective Bidders may obtain further information from BCDA and inspect the Bidding Documents at the address given below during business hours from **8:00 AM – 5:00 PM** and/or at the BCDA website (https://bcda.gov.ph/bids).

5. A complete set of Bidding Documents may be acquired by interested Bidders from the BCDA Corporate Center, 2nd Floor Bonifacio Technology Center, 31st St. cor. 2nd Avenue, Bonifacio Global City, Taguig City, starting **11 November 2023 up to 03 December 2023 from 8:00 AM to 5:00 PM** except Saturdays, Sundays and Holidays, and until **09:00 AM on 04 December 2023 (Monday)**, upon payment of an applicable fee for the bidding documents, pursuant to the latest Guidelines issued by the GPPB, as follows:

The cost of the bidding documents is are the following:

Lot	Cost of Bidding Documents (Php)
Lot A	5,000.00
Lot B	5,000.00

The Procuring Entity shall allow the bidder to present its proof of payment for the fees *in cash or manager's check.*

It may also be downloaded from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and the website of BCDA (www.bcda.gov.ph), provided that Bidders shall pay the applicable fee for the Bidding Documents not later than the submission of their bids.

6. The BCDA will hold a Pre-Bid Conference on **20 November 2023 (Monday) at 10:00 AM** at the BCDA Corporate Center, 2nd Floor Bonifacio Technology Center, 31st St. cor. 2nd Avenue, Bonifacio Global City, Taguig City, and via video conferencing thru Google Meet/Zoom, which shall be open to prospective bidders. To be able to **join the online pre-bid conference**, a written request shall be made/e-mailed to the BAC-G Secretariat by the prospective bidders.

7. Bids must be duly received by the BAC Secretariat at the BCDA Corporate Center, 2nd Floor Bonifacio Technology Center, 31st St. cor. 2nd Avenue, Bonifacio Global City, Taguig City on or before **09:00 AM, 04 December 2023 (Monday).**

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 **04 December 2023 (Monday) at 10:00 AM** at the BCDA Corporate Center, 2nd Floor Bonifacio Technology Center, 31st St. cor. 2nd Avenue, Bonifacio Global City, Taguig City. Bids will be opened in the presence of the bidders' representatives who choose to attend the Bid Opening at the address mentioned in the preceding paragraph, and at the same time, via video conferencing

through Google Meet/Zoom. An email invitation will be sent to bidders who purchased the bid documents.

10. The BCDA 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.

For further information, please refer to:
Mr. Daniel Carlo M. Fabila
Head, BACG Secretariat
bacgsecretariat@bcda.gov.ph
(02) 8575-1700

You may visit the website below for downloading of Bidding Documents:
https://www.bcda.gov.ph/bids

Issuance Date of Bidding Documents: **11 November 2023**

BIDS AND AWARDS COMMITTEE FOR GOODS
By:

[redacted]

RICHARD BRIAN M. CEPE
Chairperson

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, BCDA wishes to receive Bids for the **Procurement of Annual Subscription of the Integrated Security Suite - Endpoint Security System and Data Security and Analytic**. *as described in the Technical Specification herein the bidding documents (hereinafter referred to as the "Goods")*, as described in Section VII. Technical Specification.

The Procurement Project (referred to herein as "Project") is composed of two (2) Lots, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

2.1. The GOP through the source of funding as indicated below for the **Procurement of Annual Subscription of the Integrated Security Suite - Endpoint Security System and Data Security and Analytic** in the amount of Seven Million Five Hundred Thousand and 00/100 pesos (Php 7,500,000.00), inclusive of government taxes and fees.

2.2. The source of funding is the BCDA's Corporate Operating Budget.

3. Bidding Requirements

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

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

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

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

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

5. Eligible Bidders

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

5.2. If applicable,

a. Foreign ownership exceeding those allowed under the rules may participate pursuant to:

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

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

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

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

b. 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:

If applicable:

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.

b. For the procurement of Expendable Supplies: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least twenty-five percent (25%) of the ABC.

c. For procurement where the Procuring Entity has determined, after the conduct of market research, that imposition of either (a) or (b) will likely result to failure of bidding or monopoly that will defeat the purpose of public bidding: the Bidder should comply with the following requirements, if and when applicable:

i. Completed at least two (2) similar contracts, the aggregate amount of which should be equivalent to at least *fifty percent (50%) in the case of non-expendable supplies and services or twenty-five percent (25%) in the case of expendable supplies* of the ABC for this Project; and

ii. The largest of these similar contracts must be equivalent to at least half of the percentage of the ABC as required above.

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

6. Origin of Goods

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

7. Subcontracts

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

The Procuring Entity has prescribed that subcontracting is allowed. The portions of Project and the maximum percentage allowed to be subcontracted are indicated in the **BDS**, which shall not exceed twenty percent (20%) of the contracted Goods.

7.2. The Supplier may identify its subcontractor during the contract implementation stage. Subcontractors identified during the bidding may be changed during the implementation of this Contract. Subcontractors must submit the documentary requirements under Section 23.1 of the 2016 revised IRR of RA No. 9184 and comply with the eligibility criteria specified in **ITB** Clause 5 to the implementing or end-user unit.

7.3. 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 **20 November 2023 (Monday) at 10:00 AM** at the ***BCDA Corporate Center, 2nd Floor, Bonifacio Technology Center 31st Street corner 2nd Avenue, Bonifacio Global City Taguig City*** and/or through videoconferencing/webcasting as indicated in paragraph 6 of the **IB.**

9. Clarification and Amendment of Bidding Documents

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

10. Documents comprising the Bid: Eligibility and Technical Components

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

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

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

11. Documents comprising the Bid: Financial Component

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

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

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

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

11.5. Financial proposals for single or multi-year Framework Agreement shall be submitted before the deadline of submission of bids as prescribed in the **IB**. For multi-year Framework Agreement, evaluation of the financial proposal

during this stage is for purposes of determining eligibility and whether or not such financial proposal is within the ABC.

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).**

12.2. For Framework Agreement, the following should also apply in addition to Clause 12.1:

a. For a single year Framework Agreement, the prices quoted by the Bidder shall be fixed during the Bidder's performance of the contract and not subject to variation or escalation on any account. Price schedules required under Clause 12.1 shall be submitted with the bidding documents.

b. For a multi-year Framework Agreement, the prices quoted by the Bidder during submission of eligibility documents shall be the ceiling and the price quoted during mini-competition must not exceed the initial price offer. The price quoted during call for mini-competition shall be fixed during the Bidder's performance of that Call-off and not subject to variation or escalation on any account. Price schedules required under Clause 12.1 shall be submitted with the bidding documents.

13. Bid and Payment Currencies

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

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

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration[1] or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and Bid Security shall be valid until one hundred twenty (120) calendar days from its issuance. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

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

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

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

16. Deadline for Submission of Bids

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

17. Opening and Preliminary Examination of Bids

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

[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.

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

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

18. Domestic Preference

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

19. Detailed Evaluation and Comparison of Bids

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

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

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

19.4. The Project shall be awarded as follows:

One Project having several items grouped into several lots, which shall be awarded as separate contracts per lot.

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

20. Post-Qualification

Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated

Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

21. Signing of the Contract

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

Section III. Bid Data Sheet

ITB Clause	
5.3	For this purpose, contracts similar to the Project shall be: a. For the **Procurement of Annual Subscription of the Integrated Security Suite - Endpoint Security System (Lot A),** the Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC, within five (5) years prior to the date of submission and receipt of bids**;** and b. For the **Procurement of Data Security and Analytic (Lot B)**, the Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC, within five (5) years prior to the date of submission and receipt of bids.
7.1	Subcontracting is not allowed
12	The price of the Goods shall be quoted as delivered duty paid *in Philippine Pesos.*
14.1	The bid security shall be in the form of a **Bid Securing Declaration**, or any of the following forms and amounts: For Lot A: a. The amount of not less than **Php44,000.00** which is *two percent (2%) of ABC]*, if bid security is in cash, cashier's/manager's check, bank draft/guarantee, or irrevocable letter of credit; or b. The amount of not less than **Php110,000.00** which is *five percent (5%) of ABC]* if bid security is in Surety Bond. For Lot B: c. The amount of not less than **Php106,000.00** which is *two percent (2%) of ABC]*, if bid security is in cash, cashier's/manager's check, bank draft/guarantee, or irrevocable letter of credit; or d. The amount of not less than **Php265,000.00** which is *five percent (5%) of ABC]* if bid security is in Surety Bond
19.3	The total Approved Budget for the Contract (ABC) is ***Php 7,500,000.00***. Any Bids received in excess of the ABC for each lot of the project shall not be accepted.
	a. Blacklisted consultants or service providers shall not be allowed to participate in the bidding. b. The bidder must have completed, within the period specified in the Invitation to Bid a Single Contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC. (For this purpose "similar contracts' shall refer to contracts involving the

	provision of **Integrated Security Suite - Endpoint Security and IT Security Solution**). c. The bidder's SLCC, similar to the contract to be bid, should have been completed within five (5) years prior to the deadline for the submission and receipt of bids. d. The cost proposal shall be inclusive of all applicable taxes, fees and other charges relative to the bid e. The bid price shall be written in words and figures in the prescribed form. Pursuant to Section 32.2.3 of the 2016 RIRR of RA 9184, to wit: "In case of discrepancies between: (a) bid prices in figures and in words, the latter shall prevail; (b) total price per item and unit price for the item as extended or multiplied by the quantity of that item, the latter shall prevail; © stated total price and the actual sum of prices of component items, the latter shall prevail; (d) unit cost in the detailed estimate and unit cost in the bill of quantities, the latter shall prevail." f. The bidding shall be conducted on the date, time, and location as published in the Invitation to Bid. The bid date will be schedule for one (1) day and the sequence of bidding will be as follows: - Opening of Eligibility and Technical Documents - Opening of Financial Bid g. The Contract for the Integrated Security Suite- Endpoint Security and Data Security and Analytics shall be awarded to the bidder who is declared as the "Lowest Calculated and Responsive Bid". h. In case of a tie, after the post qualification the provisions of the GPBB Circular 05-2005 (Tie Breaking Method) shall apply. i. In accordance with the GPBB Non-Policy Memorandum dated 03 November 2014 (Section 32.2.1(a) of the Revised Implementing Rules and Regulation of RA 9184), zero (0) bid in any item is considered non-compliant. j. A bid price higher than the specified ABC, for the project shall automatically be disqualified.

Section IV. General Conditions of Contract

1. Scope of Contract

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

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

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

2. Advance Payment and Terms of Payment

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

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

2.3. For a single-year Framework Agreement, prices charged by the Supplier for Goods delivered and/or services performed under a Call-Off shall not vary from the prices quoted by the Supplier in its bid.

2.4. For multi-year Framework Agreement, prices charged by the Supplier for Goods delivered and/or services performed under a Call-Off shall not vary from the prices quoted by the Supplier during conduct of Mini-Competition.

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

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project 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

6.1. 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.

6.2. 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	a. Terms of Reference (TOR) or Technical Specification attached as Section VII <u>Delivery and Documents</u> For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: The delivery terms applicable to this Contract are to be delivered in Taguig City. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative is the Information and Communication Technology Department (ICTD). <u>Incidental Services</u> The Supplier is required to provide all services specified in Section VI. Schedule of Requirements, including additional services stated in TOR or Technical Specifications. a. training of the Procuring Entity's personnel, (online training) The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. <u>Spare Parts - Not Applicable</u> The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier: Select appropriate requirements and delete the rest.

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

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

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

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

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

The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods for a period of [indicate here the time period specified. If not used, indicate a time period of three times the warranty period].

Spare parts or components shall be supplied as promptly as possible, but in any case, within [insert appropriate time period] months of placing the order.

Packaging - Not Applicable

The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit.

The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity.

The outer packaging must be clearly marked on at least four (4) sides as follows:

Name of the Procuring Entity

Name of the Supplier

Contract Description

	Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications
	A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. <u>Transportation – Not Applicable</u> Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price. Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.
	Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. <u>Intellectual Property Rights - Applicable</u>

	The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	Partial payment is not allowed.
4	The inspections of the **Integrated Security Suite - Endpoint Security and Data Security and Analytics** shall be done upon delivery and shall be conducted by ICTD and supported by Certificate of Acceptance as basis for the payment and Inspection and Acceptance Report (IAR).

Section VI. Schedule of Requirements

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

Description	Quantity	Delivered, Weeks/Months
Annual Subscription of Integrated Security Suite - Endpoint Security	Lot A	Within thirty (30) Calendar Days upon the receipt of the Notice to Proceed.
Data Security and Analytics	Lot B	Within ninety (90) Calendar Days upon the receipt of the Notice to Proceed.

Bidder's Authorized Representative:

Name: _____
Legal capacity: _____
Signature: _____
Duly authorized to sign the Bid for and behalf of: _____
Date: _____

Section VII. Technical Specifications

TERMS OF REFERENCE / TECHNICAL SPECIFICATION

TERMS OF REFERENCE / TECHNICAL SPECIFICATION

	MINIMUM TECHNICAL SPECIFICATIONS	COMPLIANCE	
		Compliant	Non-Compliant
Lot A	**INTEGRATED SECURITY SUITE - ENDPOINT, SERVER AND CLOUD SECURITY MAINTENANCE**		
	Three Hundred Fifty (350) Licenses Annual Subscription		
	Threat Detection Capabilities:		
	High-fidelity machine learning (pre-execution and runtime);		
	Behavioral analysis (against scripts, injection, ransomware, memory and browser attacks);		
	File reputation;		
	Variant protection;		
	Census check;		
	Web reputation;		
	Exploit prevention (host firewall, exploit protection);		
	Command and control (C&C) blocking;		
	Data Loss Prevention;		
	Device control;		
	Good file check;		
	Endpoint Encryption		
	With Endpoint Protection:		
	With a high-fidelity machine learning (pre-execution and runtime) technology;		
	Behavioral analysis protection against scripts, injection, ransomware, memory, and browser attacks;		
	File reputation, Web reputation, Exploit preventions, Command and control monitoring with vulnerability protection;		
	Integrated Data Loss Prevention and Configurable Device Control.		
	With Vulnerability Protection:		
	Protection from vulnerability exploits, Denial of Service Attacks, Illegitimate Network Traffic, and Web Threats;		
	Provides patches for end-of-support operating systems, Hosted Intrusion Prevention;		
	Protection from vulnerability exploits, Denial of Service attacks, Illegitimate Network Traffic, and Web Threats;		
	Prevents network backdoors from penetrating the network.		
	With Endpoint Application Control		
	Prevents unwanted or unknown applications from executing at end points;		
	Provides support for application name, path, or certificate for basic application white and black listing.		

	With Control Management (Dashboard/Management tool)		
	Web-based management system for administrators providing dashboard to display multiple information;		
	Displays alerts on the main menu to view administrator notifications concerning system or security events.		
	With Email Protection		
	Provides anti-virus, anti-spam, and anti-relay protection, quarantine email upon virus detection;		
	Has Heuristic anti-spam protection;		
	Able to protect against phishing website;		
	Have advanced detection and alert capability for early mitigation of emerging threats and targeted attacks;		
	Detects unknown URLs embedded in email messages;		
	Protects sensitive email content by encrypting inbound and outbound email messages according to specific policies;		
	Has anti-spoofing features and mail auditing and tracking features.		
	With Gateway Protection:		
	Protects HTTP, FTP, SMTP, POP3 protocols;		
	Has URL database with multiple categories;		
	Blocks forbidden internet applications through a web browser;		
	Blocks malicious sites and restricted areas;		
	Scan HTTP and HTTPs traffics for spyware and phishing-related websites;		
	Deploys policy base on users and/or groups defined in the active directory		
	Twenty (20) instance Annual Licenses Subscription of Server Security		
	Intrusion Prevention:		
	Able to provide Host-based Intrusion Detection System (HIDS)/Host-based Intrusion Prevention System (HIPS) feature, agent and agentless		
	Feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content deviations, content that signals an attack, or policy violations		
	Able to operate in detection or prevention mode to protect operating systems and enterprise applications vulnerabilities		
	Able to provide detailed events with valuable information, including identity of the attackers, when they attacked, and what they attempted to exploit; administrators should be notified automatically via alerts when an incident has occurred		
	Able to provide protection against known and zero-day attacks		
	Protection can be pushed out to thousands of virtual desktops in minutes without a system reboot		
	Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services		
	Smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code		

	Exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits		
	Compliance (Payment Card Industry Data Security Standard [PCI DSS] 6.6) to protect web applications and the data they process		
	Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot		
	Must be able to provide Application Control on the network layer		
	Firewall Function:		
	Includes an enterprise-grade, bi-directional stateful firewall providing centralized management of firewall policy, including predefined templates		
	Virtual Machine isolation		
	Fine-grained filtering (IP and MAC addresses, ports)		
	Coverage of all IP-based protocols (Transmission Control Protocol [TCP], User Datagram Protocol [UDP], Internet Control Message Protocol [ICMP], Gateway-to-Gateway Protocol [GGP], Internet Group Management Protocol [IGMP], etc.) and all frame types (Internet Protocol [IP], Address Resolution Protocol [ARP], etc.)		
	Prevention of denial of service (DoS) attack		
	Design policies per network interfaces		
	Detection of reconnaissance scans		
	Anti Malware:		
	Able to avoid resource contention such as antivirus Strom in the virtualized VDI environment		
	Able to provide Web reputation filtering to protect against malicious sites for virtual desktops		
	Log Inspection:		
	Able to provide the capability to inspect logs and events generated by operating systems and applications		
	Able to automatically recommend and assign relevant log inspection rules to the server based on the operating system and applications installed		
	Able to automatically recommend and unassigned log inspections rules that are not required		
	Comes with pre-defined template for operating system and enterprise applications to avoid manual creation of the rules		
	Able to create customized rule to support custom application		
	Integrity Monitoring:		
	Able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time		
	Virtual Patching:		
	Provide virtual patching which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable		

	systems within hours and pushes out protection to thousands of VMs within minutes		
	Vulnerability rules to shield known vulnerabilities from an unlimited number of exploits; automatically shields newly discovered vulnerable within hours		
	Intelligence to provide recommended virtual patching rules to protect OS & applications		
	Able to create scheduled tasks to run recommendation scan to discover new rules to apply		
	Able to automatically assign new virtual patching rules through scheduled tasks		
	Able to automatically unassigned virtual patching rules after physical patch has been installed		
	Event Tagging:		
	Support event tagging so that Administrator can add "tag" to events generated by the solution		
	Tag must be fully customizable; Administrators can add, edit, and delete their own tag with own name		
	Able to search for events based on the "Tag"		
	Allow administrator to specify a specific event that is to be automatically tagged by the system		
	Management Console:		
	Dashboard to display multiple information		
	Dashboard must be configurable by administrator to display the required information only		
	Web-based management system for administrators to access using web browsers		
	"Alerts" on the main menu to view administrator notifications concerning system or security events		
	Firewall events to view activities on computers with the firewall enabled (typically includes dropped or logged packets)		
	Access to Deep Packet Inspection (DPI) events to view security-related DPI activities; this section should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode)		
	System events to view a summary of security-related events, primarily for the management server and also including agents' system events; all administrative actions should be audited with the system events		
	Qualifications		
	Bidders should have completed within five (5) years from the date of submission and receipt of bids, a contract similar to the Project. Bidder must be an authorized Partner of the product owner tha the bidder is offering to ensure that support / services will be provided to BCDA. The bidder must show proof of partnership with the product owner such as certification, etc. to be submitted during the Post Qualification Bidders must have a certified engineer of the product that they are offering and will directly handle/manage the deployment. The Engineer must show proof of certification during post qualification.		
	Scope of Services		

	Activation and maintenance of the annual license subscription of the Integrated Security Suite - Endpoint, Server and Cloud Security.		
	Implementation Period		
	The implementation shall commence upon the receipt of the Notice to Proceed. The annual subscription will start after the expiration of the existing subscription.		
	Training/ Knowledge Transfer		
	Should provide knowledge transfer training min for 10 pax Refresher training to cater to IT personnel for the latest updates of the solution for the Integrated Security Suite- Endpoint Security for two (2) sessions of four (4) hours within the year.		
	Support Services		
	Should provide 24/7 support with onsite assistance depending on severity as determined by the BCDA team to be provided by a local provider Security Assessment and recommendation should be provided on the 1st week of the 3rd month and last week of the 9th Month of the subscription period		
	Payment Terms		
	BCDA agrees to pay the total amount inclusive of all applicable taxes and fees upon issuance of Certificate of Completion and Acceptance.		
	Notes		
	All specifications are minimum requirements. Proponents may propose equivalent or higher specifications.		
Lot B	**Data Security and Analytics**		
	Three Hundred Fifty (350) Licenses Annual Subscription		
	General		
	The solution should have capabilities of Zero Trust for connectivity and Security Service Edge for security into a single unified service that protects all transactions to enterprise-owned resources and the public Internet.		
	The solution should be a Zero Trust Security Service Edge that allows users to securely connect to any applications from any location.		
	The solution must have these security features in a single platform to provide comprehensive protection to all users regardless of their location:		
	1. Centralized Management Console		
	2. Network Data Loss Prevention		
	3. Outbound Firewall Protection with Threat Prevention/Intrusion Prevention System		
	4. Malware Defense		
	5. URL Filtering/controls		
	6. Malware Sandboxing		
	7. SSL Traffic Management		
	8. Cloud Access Security Broker (CASB)		
	9. DNS Security		
	10. Secure Access to Private Resource		

	11. Zero Trust Features based on NIST 800-207		
	12. Reporting and Analytics		
	The solution should provide full native support for Windows, iOS, MacOS, Android, Chrome OS and Linux OS.		
	The solution should have a unified and native single service edge for both Private and Public Access and does not require any third-party solution.		
	The solution should support deployment architectures such as Full Cloud, Hybrid or Full On-prem Architecture.		
	The solution should provide containerized architecture, having dedicated cloud gateways and reporter with dedicated/exclusive/static Public IP Addresses from the principal.		
	The solution should provide a containerized architecture/dedicated data plane that allows full session inspection.		
	The solution should provide a containerized architecture/dedicated data plane that provides SSL traffic visibility for both proxy and dynamic analysis engine.		
	The solution should provide dedicated Public IPs from the product owner to allow tenant restriction controls or conditional access for external services or public SaaS applications (e.g. O365, Azure, Google etc)		
	The solution should provide complete data isolation for each customer allowing for complete isolation of HTTPS decryption keys, log data and geo-zoning for GDPR.		
	The solution should provide full control and customer separation for data processing and log retention for data sovereignty and compliance		
	The solution should be capable of supporting a hybrid architecture, having a cloud SaaS service and appliance on-premise which provide 100% features parity and any policies or controls configured within the cloud service should be automatically extended into the on-prem appliance.		
	The solution must have a principal's local presence in the Philippines which include locally based sales, implementation, and support team		
	Minimum Features		
	Complete Web/URL Filtering		
	The solution must support forward proxy of HTTP/HTTPS traffic flows including other TCP ports.		
	The solution should support protocols beyond HTTP/HTTPS and inspect at the application layer (L7 FWaaS).		
	The solution should have the capability to support transparent proxy type application flows.		
	The solution should have the capability to direct traffic via explicit proxy.		
	The solution should be able to support these data traffic redirection or connectivity methods below for on-site and mobile users:		
	1. Agent - Typically used on managed devices to redirect data traffic to the solution whether onsite or remote.		
	2. Proxy – Settings configured and locked in the web browser		
	3. DNS – DNS settings configured on the endpoint to point to the		

	service		
	4. GRE Tunnels – The tunnel is established between a router or firewall to the solution		
	5. IPSec Tunnels – The tunnel is established between a router or firewall to the solution		
	6. Network Connector - It can be deployed in two formats(Virtua Machine in OVF format and Docker Image format) tha provide a path to private resources for remote users and can also be used to automatically route outbound data to the solution from a location.		
	7. Web Cache Communication Protocol (WCCP)/ITD – Typically used on routers to redirect traffic to on-premise appliance		
	The solution must have the ability to steer traffic directly from a managed endpoint to the associated secure web gateway.		
	The solution must provide complete list of web categories which can be used to protect users against threats, unsuitable content, and unproductive sites.		
	The solution must provide auto-categorization of new web sites.		
	The solution must have the capability to identify uncategorized sites and take action based on the policy.		
	The solution should have the capability to restrict which browsers and operating systems that can be utilized by users that are connected to the platform.		
	The solution must allow for customer creation of URL allow and block lists.		
	The solution should support registry entries and IP address in URL lists.		
	The solution should allow for customer to create list of inappropriate keywords aside from the pre-defined keyword lists.		
	The solution should allow for customer to restrict activity over specific networking ports.		
	The solution should allow for customer to prevent users from downloading files that have specific extensions.		
	The solution should allow for customer to prevent access to specific top-level domains (TLDs)		
	The solution must support policy layering which allows advanced configurations to be applied based on multiple and potentially regularly changing user criteria like IP/Username/Geo-Location or Group/s.		
	The solution must support user, group, and business unit level for granular policy enforcement.		
	The solution must have the ability to use URLs/Domains and CIDR notation in policy creation, URL lists, etc.		
	The solution must have the ability to bypass URLs/Domains and IPs (as source or destination) in policy creation, URL lists, etc.		
	The solution should allow for customer to create custom URL categories.		
	The solution must provide access controls based on user, group, IP, or geographic location.		
	The solution must have the capability to apply SSL decryption to all or selected destinations		
	The solution must have the capability to support PAC file hosting.		

	The solution must provide URL look up functionality against category or policy.		
	The solution must be able to detect and provide appropriate action for TLS certificate issues, including, but not limited to: Expired certs, Cert Domain Mismatches, Self-Signed Certs, Untrusted Certs, Invalid CAs, Insecure ciphers, Too Long Cert Chains and etc.		
	The solution should allow for XFF header modifications.		
	The solution should allow for the creation of whitelist/blacklist that can be updated via API		
	The solution must be capable of creating/modifying custom user block messages.		
	The solution should support transparent authentication without so much reliance on directory service integration.		
	Secure Sockets Layer(SSL) traffic management		
	The solution should provide granular SSL traffic controls and options for different TLS versions and Ciphers		
	The solution should provide a broad array of selective decryption options that allow certain traffic to be decrypted while leaving other traffic untouched based on category, group, domain, app or network subnet.		
	Cloud Access Security Broker (CASB)		
	The solution should natively support O365 and Google Tenant Restriction		
	The solution must support CASB feature to apply fine grained controls on SaaS and Social Media applications		
	The solution should have the capability to enforce safe search across popular search engines such as Google, Yahoo, Bing and Youtube.		
	The solution should allow for customer to manage access to any SaaS Applications via conditional access or via custom CASB rules for bespoke company's compliance requirements.		
	The solution should have the capability to control file uploads to sanctioned and unsanctioned cloud services including generic websites.		
	The solution must support API CASB integrations for the major SaaS applications such as Box, Google and O365.		
	The solution must support out-of-band data discovery via API CASB to highlight sensitive data across SaaS applications and situations where sensitive content is shared publicly via share links		
	Malware Defense		
	The solution should provide capabilities that include malware scanning of full content and files, including data transferred within encrypted HTTPS connections.		
	The solution should support multiple engines to detect and prevent threats in all traffic processed by the platform, options include; C2 and Threat Feed Defense, Content-Based Malware Defense, Email File Types scanning,and etc.		
	The solution should provide defense-in-depth and comprehensive protection by leveraging leading Cybersecurity companies and cutting edge malware defense technology.		
	The solution should allow malware scanning rules to be fully configurable which include the content types, target destination/s, traffic direction, priority, action and etc.		

	The solution should have malware sandboxing built into the platform for further analysis of suspicious content.		
	The solution must support heuristic analysis that looks at patterns within the transactions to determine whether the transaction might be malicious or risky.		
	The solution must support Google Web Risk Protection that allows feeds from the Google Risk database to be ingested and applied to transactions.		
	The solution should have IDS/IPS signature based capabilities.		
	The solution should have IDS/IPS tuning capabilities.		
	The solution must have the capability to import custom created IDS/IPS signatures.		
	Zero Trust Capabilities		
	The solution should implement all of the core tenets and network requirements of the NIST 800-207 Zero Trust Architecture publication.		
	The solution should be a single unified Zero Trust Security Service Edge that can be used to apply consistent security policies across all resources and users, regardless of resource or user location.		
	The solution should have the ability to catalog all resources an enterprise needs to protect, including applications, data, and services.		
	The solution should have the ability to label resources to identify the type of resources present within an organization.		
	The solution should have the ability to categorize resources by type, functional category, and location.		
	The solution should have the ability to assign a risk and impact level to resources.		
	The solution should have the ability to catalog all assets and devices accessing sensitive resources within an organization.		
	The solution should have the ability to catalog all users accessing sensitive resources within an organization.		
	The solution should have the ability to force modern authentication, such as SAML or OIDC, for ALL resources, including resources that do not support modern authentication.		
	The solution should support Automatic Application & Service discovery to find shadow IT and resources that need protection.		
	The solution should have an Advanced Trust Algorithms that adaptively and automatically score users, assets, resources, and transactions to resources in real-time.		
	The solution should have an Asset and Posture management to ensure assets meet minimum requirements before accessing critical resources.		
	The solution should have continuous adaptive access trust scoring algorithms that include scoring and adaptive access decisions based on MFA, impossible user travel, geographic location at the time of resource access, firewall and anti-malware being enabled, disk encryption, and much more.		
	The solution should have the capability to create resource policies according to the NIST 800-207 Zero Trust Architecture that automatically denies unauthorized users access to enterprise-owned resources while only allowing access to approved users.		
	The solution should have NIST 800-207 Criteria-Based access policies		

	The solution should have NIST 800-207 Score-Based access policies		
	The solution should have Zero Trust reporting capabilities including reports by type and category, security impact, location, and score		
	The solution should have the ability to connect resources located on private networks, such as resources in an office, within Azure, AWS, or other cloud providers.		
	The solution should provide the capability to access private resources based on domain or IP/Subnet.		
	The solution should not allow users to connect directly to the private network so that other network resources are protected from unnecessary risks.		
	Data Loss Prevention		
	The solution should be able to detect, alert, and stop the transfer of sensitive data to and from the cloud		
	The solution should be capable of scanning for Credit card numbers, email addresses, and other Personally Identifiable Information (PII)		
	The solution should be able to process and parse targeted files, ensuring that even compressed content within compressed file is accessible to the detection engines		
	The solution should have a built-in content detection and content analysis engines that gives the ability to search for sensitive content with minimal configuration.		
	The solution must be able to effectively detect and prevent unique identifiers using regular expression, keywords and boolean constructs.		
	The solution should have the ability to set thresholds that trigger a DLP event.		
	The solution should have the ability to mask captured DLP data when an event is triggered.		
	The solution should have the ability to create and apply differen DLP Content Analysis Rules depending on the destination.		
	The solution should have the ability to prevent content transfers, including to personal destinations, based on document data labelling.		
	The solution should have the ability to read labels within documents from popular data labelling platforms, including Microsoft Information Protection (MIP), Boldon James, and Stealthbits.		
	The solution should have the capability to scan for content within connected applications via API CASB to find potentially risky situations, such as when sensitive documents are published via share links with public permissions.		
	Password Management		
	The solution should create, store, and protect user credentials locally on devices, and centrally manage passwords. Credentials should be able to sync between devices in an end-to-end encrypted way.		
	The solution should use these secrets to auto-fill a user's username, password, and 2FA token to log into an application, significantly streamlining the authentication process, and it can detect when a user inputs a new password and offer to save it for next time either from the browser or desktop app.		
	The solution should be capable of password sharing for granular		

	control over the access levels of users to shared folders while providing admins with full visibility and the capacity to assign user groups to shared folders		
	The solution should allow users to generate secure, complex passwords up to 200 characters, removing the burden of both creating and remembering them		
	The solution should allow IT to easily view and track user access to non-SSO accounts, monitor for password best practices and password health (including checking for weak passwords), view and log activity, manage shared user folders, and see a list of users' devices from the console		
	The solution should have a password health score that scans all passwords stored in the vault and checks how vulnerable they are		
	The solution should support multiple browsers and systems. It should include a desktop application, which is supported by Mac, Linux, Windows, iOS, and Android, and a multi-browser extension.		
	Integrations		
	The solution should support native integration with Splunk, FireEye Helix and Microsoft Sentinel for log forwarding.		
	The solution should support integration with any SIEM with fully customizable log format for forwarding. This includes forwarding protocols syslog, SCP, and SFTP.		
	The solution should support ICAP Service for content analysis offloading		
	The solution should support Cloud IDP integration such as but not limited to Azure/Okta/Google or Any IDP via SAML/OIDC.		
	The solution should support RESTFUL OPEN API which can integrate with any third party vendor.		
	Reporting		
	The solution should provide a dedicated reporter or cloud storage with dedicated Public IP Address as consolidation point of all generated events coming from users from any location.		
	The solution should be equipped with an advanced report manager, capable of tracking and generating statistics for a variety of aspects of network traffic.		
	The solution should provide information on all activity from any user/device anywhere in real time and also have the ability to backtrack historical events.		
	The solution should allow the organization to generate report on-demand or on a schedule basis.		
	The solution should have the capability to provide threat dashboard that gives the administrator an instant visibility into any infections on the network.		
	Email alerts should be provided throughout the platform including alerts for Advisories, Maintenance, and Updates.		
	Management Console		
	The solution must provide single-pane-glass management that allows administrator to do all administrative tasks such as policy configurations, viewing of reports, troubleshooting including packet capture capability from the containerized gateways and etc.		
	The solution must have a management console that is accessible from anywhere and every delegated administrator has the option to enable MFA as an added security layer for access.		

	Compliance and Certification		
	The solution should support and committed to security standards and compliance:		
	SOC 1 Type II		
	SOC 2 Type II		
	ISO-9001		
	ISO-27001		
	FedRAMP		
	Cloud Security Alliance STAR Level 1		
	Cloud Security Alliance STAR Level 2		
	StateRAMP		
	Qualifications		
	Bidders should have completed within five (5) years from the date of submission and receipt of bids, a contract similar to the Project. Bidder must be an authorized Partner of the product owner tha the bidder is offering to ensure that support / services will be provided to BCDA. The bidder must show proof of partnership with the product owner such as certification, etc. to be submitted during the Post Qualification Bidders must have a certified engineer of the product that they are offering and will directly handle/manage the deployment. The Engineer must show proof of certification during post qualification.		
	Scope of Services		
	Installation, configuration, testing, and maintenance of the Data Security and Analytics Solution. Pilot integration with 5 cloud applications		
	Implementation Period		
	The installation, configuration and testing to 350 devices should be completed within ninety (90) days upon receipt of NTP. The subscription period is twelve (12) months starting from the initial installation to devices.		
	Training/ Knowledge Transfer		
	Should provide knowledge transfer training min for 10 pax		
	Support Services		
	Should provide 24/7 support with onsite assistance depending on severity as determined by the BCDA team to be provided by a local provider		
	Payment Terms		
	BCDA agrees to pay the total amount inclusive of all applicable taxes and fees upon issuance of Certificate of Completion and Acceptance.		
	Notes		
	All specifications are minimum requirements. Proponents may propose equivalent or higher specifications.		

Bidder's Authorized Representative:

Name: _____
Legal capacity: _____
Signature: _____
Duly authorized to sign the Bid for and behalf of: _____
Date: _____

Section VIII.
Checklist of Technical and Financial Documents

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

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

Technical Documents

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

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

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

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

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

Financial Documents

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

Class "B" Documents

☐ (h) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence **or** duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

II. FINANCIAL COMPONENT ENVELOPE

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

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

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

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

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

Section IX.
Bidding Forms

Bid Form

Date: _____

Invitation to Bid No.(reference no.): _____

To: BASES CONVERSION AND DEVELOPMENT AUTHORITY
2nd Floor Bonifacio Technology Center
31st St., Cor. 2nd Ave., Bonifacio Global City
Taguig City

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

If our Bid is accepted, we undertake:

a. to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);
b. to provide performance security in the form, amounts, and within the times prescribed in the PBDs;
c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

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

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

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

The undersigned is authorized to submit the bid on behalf of ***[name of the bidder]*** as

evidenced by the attached ***[state the written authority].***

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

Name: _____
Legal capacity: _____
Signature: _____
Duly authorized to sign the Bid for and behalf of: _____
Date: _____

Price Schedule for Goods Offered from Within the Philippines

[shall be submitted with the Bid if bidder is offering goods from within the Philippines]

For Goods Offered from Within the Philippines

Name of Bidder _____ Project ID No._____ Page ___of___

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

Name: _____

Legal Capacity: _____

Signature: _____

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

Omnibus Sworn Statement (Revised)

[shall be submitted with the Bid]

REPUBLIC OF THE PHILIPPINES)

CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

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

1. *[Select one, delete the other:]*

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

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

2. *[Select one, delete the other:]*

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

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

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

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

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

6. *[Select one, delete the rest:]*

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

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

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

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

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

    a. *Carefully examining all of the Bidding Documents;*

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

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

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

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

10. ***In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.***

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

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]

[Insert signatory's legal capacity]

Affiant

[Jurat]

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

Bid Securing Declaration Form

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

REPUBLIC OF THE PHILIPPINES)

CITY OF _____) S.S.

BID SECURING DECLARATION

Project Identification No.(reference no.): *[Insert number]*

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

I/We, the undersigned, declare that:

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

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

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

   a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;

   b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and

   c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

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

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

Affiant

[Jurat]

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

Sample Forms: Goods and Services for Ongoing and Completed Contracts

SF-G&S-19A

Statement of All Ongoing Government and Private Contracts
Including Contracts Awarded but not yet Started

Business Name : _____
Business Address : _____

Name of the Contract	Date of the Contract	Contract Duration	Owner's Name and Address	Kinds of Goods	Amount of Contract	Value of Outstanding Contracts	Date of Delivery
Government Contracts:							
1.							
2.							
Private Contracts:							
1.							
2.							
Total Amount:							

*Continue in a separate sheet if necessary..

Submitted by : _____
Signature over Printed Name of Authorized Representative

Date : _____

Note:

- ❑ If there is no ongoing contract including those awarded but not yet started, state none or equivalent term.
- ❑ 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).

SF-G&S-19B

Statement of Single Largest Completed Contract (SLCC)
Similar in Nature to the Contract to be Bid

Business Name : _____
Business Address : _____

Name of the Contract	Date of the Contract	Contract Duration	Owner's Name and Address	Kinds of Goods	Amount of Contract	Date of Delivery

Submitted by : _____
Signature over Printed Name of Authorized Representative

Date : _____

Note:
This statement shall be supported by ANY of the following:

- ❑ End User's Acceptance; or
- ❑ Official Receipt of the last payment received; or
- ❑ Sales Invoice

Standard Form Number: SF-GOOD-14
Revised on: May 24, 2004

FINANCIAL DOCUMENTS FOR ELIGIBILITY CHECK

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

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

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

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

NFCC = P _____

K = 15

Submitted by:

_____
Name of Supplier / Distributor / Manufacturer

_____
Signature of Authorized Representative
Date : _____

NOTE:

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

PROCUREMENT OF THE ANNUAL SUBSCRIPTION OF THE INTEGRATED SECURITY SUITE - ENDPOINT SECURITY AND DATA SECURITY AND ANALYTICS
SCHEDULE OF BIDDING ACTIVITIES*

No.	ACTIVITIES	DATE/SCHEDULE (2023)
1	Pre-Procurement Conference	23 October 2023 (Monday)
2	Posting (Website, PhilGEPS, BCDA Premises)	11 November 2023 (Saturday)
3	Issuance of Bid Documents	11 November - 04 December 2023
4	**Pre-Bid Conference**	20 November 2023 (Monday)
5	Deadline for Request for Clarification, if any	24 November 2023 (Friday)
6	Issuance of Bid Bulletin, if any	28 November 2023 (Tuesday)
7	**Deadline for Submission of the ff: Eligibility Requirements and Financial Proposal**	09:00 AM, 04 December 2023
8	**Opening of the ff: Eligibility Requirements and the Financial Proposal**	10:00 AM, 04 December 2023
9	Bid Evaluation (TWG 's detailed evaluation of the submitted bids)	04-06 December 2023
10	Sending of letter to the Bidder with LCB advising them on the conduct of Post-Qualification	06 December 2023 (Wednesday)
11	Sending of letter to the Bidder with LCB advising them on the conduct of Post-Qualification	07 December 2023 (Thursday)
12	Post Qualification on the Bidder with LCB or succeeding LCB (if any)	08-18 December 2023
13	Deliberation by BAC of the Results of Post qualification	18 December 2023 (Monday)
14	Issuance of BAC's Recommendation (based on the Results of Post-Qual)	On or before 22 December 2023
15	Approval of BAC Resolution and Issuance of Notice of Award*	On or before 29 December 2023
16	Issuance of Notice to Proceed and Contract Signing	On or before 30 December 2023

Subject to change