Republic of the Philippines
PROVINCE OF CAGAYAN
Alimannao, Peñablanca, Cagayan

PHILIPPINE BIDDING DOCUMENTS

(As Harmonized with Development Partners)

Supply, Delivery, Installation, Testing and Configuration of Network Connectivity

Government of the Republic of the Philippines

August 13, 2021
ITB No. 0089-2021

Table of Contents

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

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

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

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

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

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

CDA - Cooperative Development Authority.

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

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

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

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

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

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

GFI – Government Financial Institution.

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

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

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

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

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

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

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

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

UN – United Nations.

Section I. Invitation to Bid

Republic of the Philippines
PROVINCE OF CAGAYAN
Municipality of Peñablanca

PROVINCIAL BIDS AND AWARDS COMMITTEE
GOODS AND SERVICES

INVITATION TO BID FOR

Supply, Delivery, Installation, Testing and Configuration of Network Connectivity.

1. The Provincial Government of Cagayan, through the Annual Budget Appropriations intends to apply the sum of **P 8,891,635.00** being the ABC to payments under the contract for **Supply, Delivery, Installation, Testing and Configuration of Network Connectivity** / [Goods 0089-2021]. Bids received in excess of the ABC shall be automatically rejected at the bid opening.

2. The Provincial Government of Cagayan- Bids and Awards Committee now invites bids for the above Procurement Project. Delivery of the Goods is required by **180 days.** Bidders should have completed, within the last five years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

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

   Bidding is open to all interested bidders, whether local or foreign, subject to the conditions for eligibility provided in the 2016 revised IRR of RA No. 9184.

4. Prospective Bidders may obtain further information from Bids and Awards Committee - Goods and Services (BAC-GS) of the Provincial Government of Cagayan and inspect the Bidding Documents at the address given below during Mondays to Fridays from 8:00 A.M. to 5:00 P.M.

5. A complete set of Bidding Documents may be acquired by interested Bidders on **August 13-September 1, 2021** from the given address and website below upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of **P 10,000.00**. The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person.

6. The Provincial Government of Cagayan- Bids and Awards Committee (Goods and Services) will hold a Pre-Bid Conference[1] on **August 20, 2021, 1:30 p.m.** at 2nd Floor, GSO Building, BAC Conference Room, Capitol Compound, Capitol Hills, Alimannao Peñablanca Cagayan and/or through video conferencing or webcasting through Google Meetings, which shall be open to prospective bidders.

7. Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below, on or before **September 2, 2021, 8:30 a.m**. Late bids shall not be accepted.

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

9. Bid opening shall be on **September 2, 2021, 1:00 p.m.** at the given address below and/or via Google Meetings. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

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

11. For further information, please refer to:

ATTY. IAN LUIS C. AGUILA, CPA
Head, BAC Secretariat/General Services Officer
Capitol Hills, Capitol Compound,
Alimannao Peñablanca Cagayan
pbac.cagayan@gmail.com
(078) 396-2143

12. You may visit the following websites:

For downloading of Bidding Documents: www.cagayan.gov.ph
For Google Meetings link: PBAC Cagayan-Goods and Services
Pre-Bid meeting link: meet.google.com/knx-chjy-fkc
Bid Conference Meeting link: meet.google.com/fqc-imjs-sba

July 13, 2021.

ATTY. ROGELIO R. TALIPING, JR.
Vice-Chairperson
PBAC Goods and Services

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

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, Provincial Government of Cagayan wishes to receive Bids for the **Supply, Delivery, Installation, Testing and Configuration of Network Connectivity**, with identification number **Goods 0089-2021.**

The Procurement Project (referred to herein as "Project") is composed of **13 items**, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

2.1. The GOP through the source of funding as indicated below for **F.Y. 2021** in the amount of **P 10,000,000.00**

2.2. The source of funding is:

a. LGUs, the Annual or Supplemental Budget, as approved by the Sanggunian.

3. Bidding Requirements

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

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

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

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

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

5. Eligible Bidders

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

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

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

a. The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.

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

6. Origin of Goods

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

7. Subcontracts

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

The Procuring Entity has prescribed that:

a. **Subcontracting is not allowed.**

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

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time and either at its physical address **2nd Floor GSO Building, BAC Conference Room**, **Capitol Hills, Alimannao Peñablanca Cagayan /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 the last five years prior to the deadline for the submission and receipt of bids.

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

11. Documents comprising the Bid: Financial Component

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

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

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

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

12. Bid Prices

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

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

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

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

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

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

b. For Goods offered from abroad:

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

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

13. Bid and Payment Currencies

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

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

a. Philippine Pesos.

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration[2] or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and bid security shall be valid for 120 days reckoning from the bid opening. 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 four copies of the first and second components of its Bid. **One (1) copy marked "ORIGINAL" and 3 photocopies, properly tabbed/labeled.**

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

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

16. Deadline for Submission of Bids

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

17. Opening and Preliminary Examination of Bids

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

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

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

[2] 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.

18. Domestic Preference

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

19. Detailed Evaluation and Comparison of Bids

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

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

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

19.4. The Project shall be awarded as follows:

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

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

20. Post-Qualification

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

<table>
<tr><th>ITB Clause</th><th></th></tr>
<tr><td>5.3</td><td>For this purpose, contracts similar to the Project shall be:

a. Installation and Configuration of Network Connectivity.

b. Completed within the last 5 years prior to the deadline for the submission and receipt of bids.</td></tr>
<tr><td>7.1</td><td>Sub-contracting is not allowed.</td></tr>
<tr><td>12</td><td>The price of the Goods shall be quoted DDP Provincial Government of Cagayan or the applicable International Commercial Terms (INCOTERMS) for this Project.</td></tr>
<tr><td>14.1</td><td>The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts:
a. The amount of not less than two percent (2%) of the ABC if bid security is in cash, cashier’s/manager’s check, bank draft/guarantee or irrevocable letter of credit; or

b. The amount of not less than five percent (5%) of the ABC if bid security is in Surety Bond.</td></tr>
<tr><td>19.3</td><td><table><tr><th>No.</th><th>Particulars</th><th>Qty</th><th>ABC</th></tr><tr><td>1</td><td>Refer to Schedule of Requirements</td><td></td><td>6,951,679.50</td></tr></table></td></tr>
<tr><td>20.2</td><td>No further instructions.</td></tr>
<tr><td>21.2</td><td>ADDITIONAL DOCUMENTS REQUIRED:
1. Statement of Manpower Requirement
2. Aftersales Service/Parts Warranty Statement in compliance with Section VII
3. Un-amended Sales Literature/Brochure</td></tr>
</table>

Section IV. General Conditions of Contract

1. Scope of Contract

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

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

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

2. Advance Payment and Terms of Payment

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

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

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC**, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

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	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *[For Goods supplied from abroad, state:]* "The delivery terms applicable to the Contract are DDP delivered Tuguegarao City Cagayan. In accordance with INCOTERMS." *[For Goods supplied from within the Philippines, state:*] "The delivery terms applicable to this Contract are delivered Tuguegarao City Cagayan. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative at the Project Site is *[indicate name(s)].* **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: a. performance or supervision of on-site assembly and/or start-up of the supplied Goods; b. furnishing of tools required for assembly and/or maintenance of the supplied Goods; c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; d. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and

	e. training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods. f. **ADDITIONAL INCIDENTAL SERVICES** The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. **Spare Parts –** The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier: 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 **three (3) times the warranty period**. Spare parts or components shall be supplied as promptly as possible, but in any case, within 15 working days of placing the order.
	Packaging – The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit.

	The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity. The outer packaging must be clearly marked on at least four (4) sides as follows: Name of the Procuring Entity Name of the Supplier Contract Description Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications
	A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. **Transportation –** Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price. Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.
	Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment

	and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights –** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	Partial payment is not allowed.
4	The inspections and tests that will be conducted are: **Inspection and Testing of the Technical Specifications required**

Section VI. Schedule of Requirements

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

Item No.	Description	Unit	Qty	Total	Delivered Weeks/Months
1	Installation and Configuration of Network Connectivity	lot	1	P 8,891,635.00	180 days

Section VII. Technical Specifications

Item	Technical Specifications	Statement of Comp
Hardware Component Core Switch	Specification The proposed solution must have / support the following: **Hardware** • 24 x 10G SFP+, 6x 40G/100G QSFP28 fixed ports • Dimensions of 43.6mm x 442.0mm x 420.0mm in H x W x D • 1U Chassis Height • Rated voltage range of 100V AC to 240V AC, 50/60 Hz • Maximum voltage input of 90V AC to 290V AC, 45 Hz to 65 Hz • Maximum input current of 8A at 600W AC • Maximum power consumption of 254W • Operating temperature of -5*C to +45*C at 0m – 1800m altitude • Storage temperature of -40*C to +70*C • Less than 65 dB(A) sound pressure at normal temperature • Power Supply Surge protection of +/- 6kV in differential and / or common mode • 1+1 power redundancy • 4 Fan Modules • Heat dissipation with fan • Intelligent fan speed adjustment **SERVICE FEATURES:** **MAC** • Up to 384K MAC address entries • IEEE802.1d standards compliance • MAC address learning and aging • Static, dynamic and blackhole MAC address entries • Packet filtering based on source MAC address **VLAN** • 4K VLANs • Guest VLANs and voice VLANs • GVRP • MUX VLAN • VLAN assignment based on MAC addresses, protocols, IP subnets, policies and ports • VLAN mapping **ARP** • Static ARP • Dynamic ARP **IP ROUTING** • Static routing • RIP v1, RIP v2, RIPng • OSPF, OSPFv3 • IS-IS, IS-ISv6 • BGP, BGP4+	Bidders must state h "Comply" or "Not Com each of the individual p each Specification st corresponding perfo parameter of the equipr Statements of "Comp Comply" must be sup evidence in a Bidders B referenced to that e Evidence shall be in t manufacturer's un-am literature, unconditiona of specification and c issued by the manufactu independent test dat appropriate. A statemer supported by evide subsequently foun contradicted by the presented will render th evaluation liable for re statement either in th statement of compli supporting evidence tha be false either during Bi post-qualification or the the Contract may be r fraudulent and render t supplier liable for prosec to the applicable laws ar

- ECMP
- Routing Policy
- Up to 256K FIBv4 entries
- Up to 80K FIBv6 entries

INTEROPERABILITY

- VLAN-Based Spanning Tree (VBST), working with PVST, PVST+ and RPVST
- Link-type Negotiation Protocol (LNP) similar to DTP
- VLAN Central Management Protocol (VCMP) similar to VTP

WIRELESS SERVICES

- AP access control, AP domain management, and AP configuration template management
- Radio management, unified static configuration, and dynamic centralized management
- WLAN basic service, QoS, security and user management
- CAPWAP, tag/terminal location, and spectrum analysis

ETHERNET LOOP PROTECTION

- RRPP ring topology and RRPP multi-instance
- Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover
- SEP
- ERPS
- BFD for OSPF, BFD for IS-IS for VRRP, and BFD for PIM
- STP, RSTP and MSTP
- BPDU protection, root protection and loop protection

MPLS

- MPLS L3VPN
- MPLS L2VPN
- MPLS-TE
- MPLS QoS

IPV6 FEATURES

- IPv6 Neighbor Discovery
- PMTU
- IPv6 Ping, IPv6 Tracert, IPv6 Telnet
- ACLS based on source IPv6 addresses, destination IPv6 Addresses, Layer 4 ports, or protocol types
- Multicast Listener Discover snooping (MLD v1/v2)
- IPV6 addresses configured for sub-interfaces
- VRRP6
- DHCPv6
- L3VPN

MULTICAST

- IGMP v1/v2/v3 snooping and IGMP fast leave
- Multicast forwarding in a VLAN and multicast replication between VLANs
- Multicast load balancing among member ports of a trunk
- Controllable multicast
- Port-based multicast traffic statistics
- IGMP v1/v2/v3
- PIM-SM, PIM-DM and PIM-SSM

- MSDP
- Multicast VPN

QOS / ACL

- Rate limiting in the inbound and outbound directions of a port
- Packet redirection
- Port-based traffic policing and two-rate three-color CAR
- Eight queues on each port
- DRR, SP and DRR+SP queue scheduling algorithm
- WRED
- Re-marking of the 802.1p and DSCP field of packets
- Packet filtering at Layer 2 to Layer 4
- Filtering out invalid frames based on the source MAC address, destination MAC address, Source IP address, destination IP address, TCP/UDP source, TCP/UDP destination, port number, protocol type and VLAN ID
- Queue-based rate limiting and shaping on ports

SECURITY

- Hierarchical user management and password protection
- DoS attack defense, ARP attack defense and ICMP attack defense
- Binding the IP address, MAC address, port number and VLAN ID
- Port Isolation, port security and sticky MAC
- MAC Forced Forwarding
- Blackhole MAC address entries
- Limit on the number of learned MAC addresses
- IEEE802.1X authentication and limit on the number of users on a port
- AAA authentication, RADIUS authentication and HWTACACS authentication
- NAC
- SSH V2.0
- HTTPS
- CPU protection
- Blacklist and whitelist
- Attack source and punishment for IPV6 packets such as ND, DHCPv6 and MLD packets
- IPsec for management packet encryption
- ECA
- Deception
- MACSec

RELIABILITY

- LACP
- E-Trunk
- Ethernet OAM
- ITU-Y.1731
- DLDP
- LLDP
- BFD for BGP, BFP for IS-IS, BFD for OSPF, BFD for static routes

VXLAN

- VXLAN L2 and L3 gateways
- Centralized and distributed gateway
- BGP-EVPN

Access Switch	• Configured through the NETCONF protocol **SVF** • Acting as the parent node to vertically virtualize downlink switches and APs as one device for management • Two-layer client architecture • SVF • ASs can be independently configured. Services not supported by templates can be configured on the parent node • Third-party devices allowed between SVF parent and clients **IPCA** • Marking service packets to obtain the packet loss ratio and number of lost packets in real time • Measurement of the number of lost packets and packet loss ratio on networks and devices **MANAGEMENT AND MAINTENANCE** • Cloud-based management • Virtual cable test • SNMP v1/v2c/v3 • RMON • Web-based NMS • System logs and alarms of different severities • GVRP • MUX VLAN • Netstream • Telemetry The proposed solution must include the following accessories: • x8 Electrical Transceiver, SFP, GE, Electrical Interface Module (100m, RJ45) • x22 Optical Transceiver, SFP+, 10G, Multi-mode Module (850nm, 0.3km, LC) • x2 Stacking Cables x8 Wireless Access Contoller AP Resource Licenses * Will serve as Main Distribution Frame of the network The proposed solution must have / support the following: **HARDWARE** • 24 10/100/1000Base-T ports, 4 X 10GE SFP+ ports • Dimensions of 43.6mm x 442mm x 420mm in H x W x D • 1U in Chassis Height • 600W AC pluggable power supply type • 100V AC to 240V AC, 50/60 Hz rated voltage range • 90V to 290V, 45Hz to 65Hz maximum voltage range • Maximum power consumption of 114W • 47.5dB(A) of sound pressure under normal temperature • -5*C to +45*C operating temperature at 0m-1800m altitude • -40*C to +70*C storage temperature • +/- 6kV common mode and/ or differential mode surge protection • Air cooling heat dissipation, • Intelligent speed adjustment • Pluggable fans **SERVICE FEATURES**

MAC ADDRESS TABLE

- IEEE802.1d standards compliance
- 64K MAC address entries
- MAC address learning and aging
- Static, dynamic and blackhole MAC address entries
- Packet filtering based on source MAC address

VLAN

- 4094 VLANs
- Guest VLANs and voice VLANs
- GVRP
- MUX VLAN
- VLAN assignment based on MAC addresses, protocols, IP subnets, policies and ports
- VLAN mapping

ETHERNET LOOP PROTECTION

- RRPP ring topology and RRPP multi-instance
- Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover
- SEP
- ERPS
- BFD for OSPF, BFD for IS-IS for VRRP, and BFD for PIM
- STP, RSTP and MSTP
- BPDU protection, root protection and loop protection

IP ROUTING

- Static routing
- RIP v1, RIP v2, RIPng
- OSPF, OSPFv3
- IS-IS, IS-ISv6
- BGP, BGP4+
- ECMP
- Routing Policy
- Up to 16K FIBv4 entries
- Up to 8K FIBv6 entries

INTEROPERABILITY

- VLAN-Based Spanning Tree (VBST), working with PVST, PVST+ and RPVST
- Link-type Negotiation Protocol (LNP) similar to DTP
- VLAN Central Management Protocol (VCMP) similar to VTP

IPV6 FEATURES

- IPv6 Neighbor Discovery, up to 8K ND entries
- PMTU
- IPv6 Ping, IPv6 Tracert, IPv6 Telnet
- ACLS based on source IPv6 addresses, destination IPv6 Addresses, Layer 4 ports, or protocol types
- Multicast Listener Discover snooping (MLD v1/v2)
- IPV6 addresses configured for sub-interfaces
- VRRP6
- DHCPv6

- L3VPN

MULTICAST

- IGMP v1/v2/v3 snooping and IGMP fast leave
- Multicast forwarding in a VLAN and multicast replication between VLANs
- Multicast load balancing among member ports of a trunk
- Controllable multicast
- Post-based multicast traffic statistics
- IGMP v1/v2/v3
- PIM-SM, PIM-DM and PIM-SSM
- MSDP
- Multicast VPN

QOS / ACL

- Rate limiting in the inbound and outbound directions of a port
- Packet redirection
- Port-based traffic policing and two-rate three-color CAR
- Eight queues on each port
- DRR, SP and DRR+SP queue scheduling algorithm
- WRED
- Re-marking of the 802.1p and DSCP field of packets
- Packet filtering at Layer 2 to Layer 4
- Filtering out invalid frames based on the source MAC address, destination MAC address, Source IP address, destination IP address, TCP/UDP source, TCP/UDP destination, port number, protocol type and VLAN ID
- Queue-based rate limiting and shaping on ports

SECURITY

- Hierarchical user management and password protection
- DoS attack defense, ARP attack defense and ICMP attack defense
- Binding the IP address, MAC address, port number and VLAN ID
- Port Isolation, port security and sticky MAC
- MAC Forced Forwarding
- Blackhole MAC address entries
- Limit on the number of learned MAC addresses
- IEEE802.1X authentication and limit on the number of users on a port
- AAA authentication, RADIUS authentication and HWTACACS authentication
- NAC
- SSH V2.0
- HTTPS
- CPU protection
- Blacklist and whitelist
- Attack source and punishment for IPV6 packets such as ND, DHCPv6 and MLD packets
- IPsec
- ECA
- Deception

Access Points	**RELIABILITY** • LACP • E-Trunk • Ethernet OAM • ITU-Y.1731 • DLDP • LLDP **VXLAN** • VXLAN L2 and L3 gateways • Centralized and distributed gateway • BGP-EVPN • Configured through the NETCONF protocol **SVF** • Two-layer client architecture • SVF • IGMP snooping can be enabled on the access switches and the maximum number of access users on a port can be configured • ASs can be independently configured. Services not supported by templates can be configured on the parent node • Third-party devices allowed between SVF parent and clients • Working as an SVF client that is plug-and-play with zero configuration **IPCA** • Directly coloring service packets to collect real-time statistics on the number of lost packets and packet loss ratio • Collection of statistics on the number of lost packets and packet loss ratio at network and device levels **TWAMP** • Two-way IP link performance measurement • Measurement on two-way packet delay, one-way packet loss rate and one-way packet jitter **MANAGEMENT AND MAINTENANCE** • Supported stacking for up to 9 members • SNMP v1/v2c/v3 • RMON • Smart Application Control • Web-based NMS • Systems logs and alarms of different levels • GVRP • MUX VLAN • NetStream • Intelligent O&M The proposed solution must include the following accessories: x20 Optical Transceiver, SFP+, 10G, Multi-mode Module (850nm, 0.3km, LC) *Will serve as Intermediate Distribution Frame The proposed solution must have / support the following: • 47mm x 200mm x 200mm in H x W x D • 1.05 kg in Weight

- x1 10/100/1000M self-adaptive Ethernet interface (RJ45 x 2)
- 1 x USB interface
- BLE5.0 Bult-in Bluetooth
- LED indicated that indicated power-on, startup, running, alarm and fault states of the system
- In compliance with 802.3at
- -10*C to +50*C operating temperature
- -40*C to +70*C storage temperature
- IP41 dustproof and waterproof grade
- -60m to +5000 m operating altitude
- 53kPa to 106kPa operating atmospheric pressure
- Built-in adaptive array antennas
- 3.5dBi antenna gain at 2.4 GHz
- 5dBi antenna gain at 5GHz
- Less than or equal to 16 maximum number of SSIDs for each radio
- Less than or equal to 512 maximum number of users
- 25dBm maximum transmit power at 2.4GHz
- 25dBm maximum transmit power at 5GHz
- Power increment of 1dBm
- Can analyze the spectrum of no Wi-Fi interference sources and identify them
- WIDS/WIPS
- Monitor, identify, defend, counter and perform refined management on the rogue devices
- Compliance with IEEE 802.11a/b/g/n/ac/ac Wave 2/ax
- Maximum rate of up to 1.775Gbps
- Maximum ratio combining (MRC)
- Space time block code (STBC)
- Cyclic Delay Diversity (CDD)/Cyclic Shift Diversity (CSD)
- Beamforming
- MU-MIMO
- DL OFDMA 1024QAM
- Low-density parity-check (LDPC)
- Maximum-likelihood detection (MLD)
- Frame aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx)
- 802.11 dynamic frequency selection (DFS)
- Short guard interval (GI) in 20 MHz, 40 MHz, 80 MHz, and 160 MHz modes
- Priority mapping and packet scheduling based on a Wi-Fi Multimedia (WMM) profile to implement priority-based data processing and forwarding
- Automatic and manual rate adjustment
- WLAN channel management and channel rate adjustment
- Automatic channel scanning and interference avoidance
- Service set identifier (SSID) hiding
- Signal sustain technology (SST) Unscheduled automatic power save delivery (U-APSD)
- Hotspot2.0 802.11k and 802.11v smart roaming
- 802.11r fast roaming (≤ 50 ms)
- WAN authentication escape
- Compliance with IEEE 802.3ab

- Auto-negotiation of the rate and duplex mode and automatic switchover between the Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)
- Compliance with IEEE 802.1q
- SSID-based VLAN assignment
- VLAN trunk on uplink Ethernet ports
- Management channel of the AP uplink port in tagged and untagged mode
- DHCP client, obtaining IP addresses through DHCP
- Tunnel data forwarding and direct data forwarding
- Application identification and QoS classification when AP local forwarding (also called direct forwarding), which can significantly improve voice quality for applications such as Skype, QQ, and WeChat
- STA isolation in the same VLAN
- Access control lists (ACLs)
- Link Layer Discovery Protocol (LLDP)
- Soft Generic Routing Encapsulation (GRE)
- IPv6 Source Address Validation Improvements (SAVI)
- Multicast Domain Name Service (mDNS) gateway protocol
- Priority mapping and packet scheduling based on a Wi-Fi Multimedia (WMM) profile to implement priority-based data processing and forwarding
- WMM parameter management for each radio WMM power saving
- Priority mapping for upstream packets and flow-based mapping for downstream packets
- Queue mapping and scheduling
- User-based bandwidth limiting
- Adaptive bandwidth management (automatic bandwidth adjustment based on the user quantity and radio environment) to improve user experience
- Airtime scheduling
- Open system authentication
- WEP authentication/encryption using a 64-bit, 128-bit, or 152-bit encryption key
- WPA/WPA2-PSK authentication and encryption (WPA/WPA2 personal edition)
- WPA3-SAE authentication and encryption (WPA3* personal edition)
- WPA/WPA2-802.1x authentication and encryption (WPA/WPA2 enterprise edition)
- WPA3-802.1x authentication and encryption (WPA3* enterprise edition)
- WPA-WPA2 hybrid authentication
- WPA2-WPA3* hybrid authentication
- WAPI* authentication and encryption
- Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and countermeasure, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist
- 802.1x authentication, MAC address authentication, and Portal authentication
- DHCP snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard (IPSG)
- 802.11w Protected Management Frames (PMFs)

Next-Generation Firewall	• Application identification • Telnet • STelnet using SSH v2 • SFTP using SSH v2 • SNMP v1/v2/v3 • Network Time Protocol (NTP) The proposed solution must include the following accessories: • x30 PoE Injector *Will serve as wireless connection to users using laptops **FIREWALL** **Hardware Specification** • Must provide 1 unit of firewall with 1 External Redundant Power Supply • 4 x 1GbE Copper ports • 4 x 2.5GbE Copper ports • 4 x SFP+ Fiber ports • 2 x expansion bay **Performance Specifications** • Firewall Throughput – 75 Gbps • Firewall IMIX – 33 Gbps • IPS Throughput – 25 Gbps • Threat Protection Throughput – 4.8 Gbps • The solution must support 16.6M concurrent sessions. • The solution must support 368,000 new connections/sec. • IPsec VPN Throughput – 9.8 Gbps **Firewall Features** **General Management** • Must have a purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators • Must be able to support two-factor authentication (One-time-password) for administrator access, user portal, IPSec and SSL VPN • Must have an advanced trouble-shooting tools in GUI (e.g. Packet Capture) • Must be able to support high Availability (HA) clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup • Must have a full command-line-interface (CLI) accessible from GUI • Must be able to support role-based administration • Must have an automated firmware update notification with easy automated update process and roll-back features • Must have reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers • Must have a self-service user portal • Must be able to support configuration change tracking • Must have a flexible device access control for services by zones • Must have an email or SNMP trap notification options • Must be able to support SNMPv3 and Netflow support • Must have a central management support via Cloud-based Unified Console

- Must be able to backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
- Must be able to support API for 3rd party integration
- Must be able to support interface renaming
- Must be able to use remote access option for Product Support
- Must be able to support cloud-based license management via Licensing Portal

Central Firewall Management

- Must be able to support cloud-based management and reporting for multiple firewalls provides group policy management in a single console
- Must be able support group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
- Must have a task manager that provides a full historical audit trail and status monitoring of group policy changes
- Must have a backup firmware management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
- Must be able to support firmware updates which offer one-click firmware updates to be applied to any device
- Must be able to do zero-touch deployment that enables the initial configuration to be performed in Cloud-based management and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to the Central Manager

Firewall, Networking & Routing

- Must be able to support stateful deep packet inspection firewall
- Must have a packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing
- Must be able to support "TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade polices, unique dashboard visibility, and compatibility troubleshooting"
- Must have a "DPI Engine that provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine"
- Must be able to support network Flow FastPath delivers policy-driven and intelligent acceleration of trusted traffic automatically
- Must be able to support user, group, time, or network-based policies
- Must be able to support access time polices per user/group
- Must be able to support enforcing of policy across zones, networks, or by service type
- Must have zone-based firewall
- Must have default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi
- Must have custom zones on LAN or DMZ
- Must be able to support customization of NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks
- Must have a flood protection: DoS, DDoS and portscan blocking
- Must be able to support country blocking by geo-IP

- Must have an upstream proxy support
- Must be able to support a protocol that is independent in multicast routing with IGMP snooping
- Must be able to support bridging with STP support and ARP broadcast forwarding
- Must have VLAN DHCP support and tagging
- Must have VLAN bridge support
- Must have Jumbo Frame Support
- Must have WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules
- Must have wireless WAN support (n/a in virtual deployments)
- Must be able to support 802.3ad interface link aggregation
- Must be able to support full configuration of DNS, DHCP and NTP
- Must be able to support dynamic DNS (DDNS)
- Must be able to support IPv6 Ready Logo Program Approval Certification

SD-WAN

- Must have a "Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, failover and fail-back"
- Must be able to support "Application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP"
- Must be able to support application routing over preferred links via firewall rules or policy-based routing
- Must be affordable, flexible, and can support zero-touch or low-touch deployment
- Must have a robust VPN support including IPSec and SSL VPN
- Must have a centralized VPN orchestration
- Must have a unique RED Layer 2 tunnel with routing

Base Traffic Shaping & Quotas

- Must be able to support "Flexible network or user-based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)"
- Must be able to set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
- Must have a real-time VoIP optimization
- Must be able to support DSCP marking

Authentication

- Must be able to support authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- Must have a server authentication agent for Active Directory SSO, STAS, SATC
- Must be able to support Single sign-on: Active directory, eDirectory, RADIUS Accounting
- Must be able have client authentication agents for Windows, Mac OS X, Linux 32/64
- Must be able to support browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
- Must have a browser Captive Portal

- Must be able to support authentication certificates for iOS and Android
- Must be able to support authentication services for IPSec, SSL, L2TP, PPTP
- Must be able to support Google Chromebook authentication support for environments with Active Directory and Google G Suite
- Must be able to support API-based authentication

User Self-Serve Portal

- Must have a download for the Authentication Client Application
- Must support download of SSL remote access client (Windows) and configuration files (other OS)
- Must be able to support hotspot access information
- Must be able to support change of user name and password
- Must be able to view personal internet usage
- Must be able to access quarantined messages and manage user-based block/allow sender lists (requires Email Protection)

Base VPN Options

- Must be able to support Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
- Must have a Remote Ethernet Device (RED) site-to-site VPN tunnel (robust and light-weight)
- Must be able to support L2TP and PPTP
- Must be able to support route-based VPN
- Must be able to support remote access: SSL, IPsec, iPhone/iPad/ Cisco/Android VPN client support
- Must be able to support IKEv2
- Must have a SSL client for Windows and configuration download via user portal

Connect VPN Client

- Must be able to support authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
- Must be able to support intelligent split-tunneling for optimum traffic routing
- Must be able to support NAT-traversal
- Must have a client-monitor for graphical overview of connection status
- Must be able to support Mac and Windows

Network Protection Subscription
Intrusion Prevention (IPS)

- Must be able to support a high-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
- Must have thousands of signatures
- Must have a granular category selection
- Must be able to support for custom IPS signatures
- Must be able to support IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added

ATP and Security Heartbeat

- Must have an advanced Threat Protection (Must be able to detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)

SD-Remote Ethernet Device Management

- Must have a Central management of all SD-RED devices
- Must be able to support No configuration: Automatically connects through a cloud-based provisioning service
- Must be able to support secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption
- Must be able to have a virtual Ethernet for reliable transfer of all traffic between locations
- Must be able to support IP address management with centrally defined DHCP and DNS Server configuration
- Must be able to remotely de-authorize RED device after a select period of inactivity
- Must be able to support compression of tunnel traffic
- Must be able to support VLAN port configuration options

Clientless VPN

- Must be able to have unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC

Web Protection Subscription
Web Protection and Control

- Must be able to support fully transparent proxy for anti-malware and web-filtering
- Must be able to have an Enhanced Advanced Threat Protection
- Must be able to have an URL Filter database with millions of sites across 92 categories backed by OEMLabs
- Must be able to support surfing quota time policies per user/group
- Must be able to have access time polices per user/group
- Must be able to support malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email
- Must be able to have an advanced web malware protection with JavaScript emulation
- Must be able to have a live Protection real-time in-the-cloud lookups for the latest threat intelligence
- Must be able to have a second independent malware detection engine for dual-scanning
- Must be able to support real-time or batch mode scanning
- Must be able to have a pharming Protection
- Must be able to support HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions
- Must be able to support SSL protocol tunneling detection and enforcement
- Must be able to support certificate validation
- Must be able to support high performance web content caching
- Must be able to support forced caching for managed endpoint updates
- Must be able to have a file type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
- Must be able to support youtube for Schools enforcement per policy (user/group)

- Must be able to support "SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)"
- Must be able to support "Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists"
- Must have the ability to block Potentially Unwanted Applications (PUAs)
- Must be able to support web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
- Must be able to support User/Group policy enforcement on Google Chromebooks

Cloud Application Visibility

- Must be able to have a Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
- Must be able to have a Discover Shadow IT at a glance
- Must have the ability to drill down in order to obtain details on users, traffic, and data
- Must have the ability of one-click access to traffic shaping policies
- Must be able to support filter cloud application usage by category or volume
- Must be able to support detailed customizable cloud application usage report for full historical reporting

Application Protection and Control

- Must be able to support signature-based application control with patterns for thousands of applications
- Must be able to support Cloud Application Visibility and Control to discover Shadow IT
- Must be able to support App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
- Must be able to support Micro app discovery and control
- Must be able to support "Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level "
- Must be able to support Per-user or network rule application control policy enforcement

Web & App Traffic Shaping

- Must be able to support custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared

Threat Intelligence Analysis

- Must be able to automatically sent all files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) for Threat Intelligence Analysis

- Must have the ability for all files to be checked against OEMLab's massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware
- Must be able to have an extensive reporting that includes a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model.

Email Protection Subscription
Email Protection and Control

- Must be able to support email scanning with SMTP, POP3 and IMAP support
- Must be able to support reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology
- Must have the ability to block spam and malware during the SMTP transaction
- Must be able to support DKIM and BATV anti-spam protection
- Must be able to support Spam greylisting and Sender Policy Framework (SPF) protection
- Must have the ability of recipient verification for mistyped email addresses
- Must have a second independent malware detection engine for dual scanning
- Must have a live protection in real-time, in-the-cloud lookups for the latest threat intelligence
- Must be able to support smart host support for outbound relays
- Must have the ability of file type detection/blocking/scanning of attachments
- Must be able to accept, reject or drop over-sized messages
- Must be able to detects phishing URLs within e-mails
- Must be able to use pre-defined content scanning rules or create your own custom rules based on a variety of criteria with granular policy options and exceptions
- Must be able to support TLS encryption support for SMTP, POP, and IMAP
- Must be able to append signature automatically to all outbound messages
- Must be able to support individual user-based block and allow sender lists maintained through the user portal

Email Quarantine Management

- Must be able to support spam quarantine digest and notifications options
- Must be able to support malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages
- Must have a self-serve user portal for viewing and releasing quarantined messages

Email Encryption and DLP

- Must be able to support patent-pending SPX encryption for one-way message encryption

- Must be able to support recipient self-registration SPX password management
- Must have the ability to add attachments to SPX secure replies
- Must be completely transparent, no additional software or client required
- Must have a DLP engine with automatic scanning of emails and attachments for sensitive data
- Must have a pre-packaged of sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by the OEMLabs

Web Server Protection Subscription
Web Application Firewall Protection

- Must be able to support reverse proxy
- Must be able to support URL hardening engine with deep-linking and directory traversal prevention
- Must be able to support Form Hardening engine
- Must be able to support SQL injection protection
- Must be able to support cross-site scripting protection
- Must have dual-antivirus engines
- Must have a HTTPS(TLS/SSL) encryption offloading
- Must be able to support cookie signing with digital signatures
- Must be able to support path-based routing
- Must be able to support outlook anywhere protocol support
- Must be able to support reverse authentication (offloading) for form-based and basic authentication for server access
- Must be able to support virtual server and physical server abstraction
- Must be have an integrated load balancer that spreads visitors across multiple servers
- Must be able to have the ability of skipping individual checks in a granular fashion as required
- Must be able to have the ability to match requests from source networks or specified target URLs
- Must be able to support for logical and/or operators
- Must be able to assists compatibility with various configurations and non-standard deployments
- Must have options to change Web Application Firewall performance parameters
- Must be able to have a scan size limit option
- Must be able to Allow/Block IP ranges
- Must be able to support wildcard for server paths and domains
- Must have the ability to automatically append a prefix/suffix for authentication

Reporting
Central Firewall Reporting

- Must have pre-defined reports with flexible customization options
- Must have a reporting for Firewalls (hardware, software, virtual, and cloud)
- Must have an intuitive user interface provides graphical representation of data
- Must have a report dashboard provides an at-a-glance view of events over the past 24 hours
- Must be easily identify network activities, trends, and potential attacks
- Must have an easy backup of logs with quick retrieval for audit needs

	• Must be able to have a simplified deployment without the need for technical expertise **On-Box Reporting** • Must have hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless, Security Heartbeat, Sandstorm), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA) • Must have a current Activity Monitoring: system health, live users, IPSec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks • Must be able to report anonymization • Must have a report scheduling to multiple recipients by report group with flexible frequency options • Must be able to export reports as HTML, PDF, Excel (XLS) • Must have report bookmarks • Must have a log retention customization by category • Must have a full-featured Live Log Viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization **Bidder's qualification and capability** • The bidder must be a Platinum Partner or equivalent of their proposed solution. • The bidder must provide Manufacturer certification that they are authorized partner of the solution proposed. • The bidder must have at least two (2) certified architect of the solution proposed; Certificate of employment and photocopy of the individual certificate from the principal/manufacturer must be submitted. • The bidder must have at least (2) Senior Project Manager with Project Management Professional (PMP) certification. Must attach valid certification and should be an employee of the bidder.
Active Directory Server	*Will serve as control panel for the client • Form Factor: Rack Server • Drive Bays: Up to 4 x 3.5" Hot-Plug drives. • CPU: Intel Xeon E-2226G 3.4GHz, 12M cache, 6C/6T, 80W • Memory: 2 x 16GB 2666MT/s UDIMM. • Storage: ○ 2 x 960GB SSD SATA Mixed Used 6Gbps 512e Hot Plug • RAID Controller: ○ 8-port 12Gbps Hardware RAID controller ○ Able to support RAID levels 0, 1, 5, 6, 10, & 50. ○ Can supports real-time RAID monitoring and hardware inventory • I/O & Ports: ○ Dual Port 1Gb LOM • Power Supply: Dual 350W Redundant Hot Plug Power Supplies. • Supports Integration with third-party consoles. • Supports Connection for third-party consoles. • Supported Operating System: ○ Windows Server with Hyper-V ○ RHEL

	○ SLES ○ Ubuntu Server ○ Citrix XenServer ○ VMware ESXi • Able to support the following security features: ○ TPM 1.2/2.0 optional ○ Secure Boot ○ Silicon Root of Trust ○ Cryptographically signed firmware ○ System Lockdown ○ System Erase • Must include server warranty of 3-years 24x7 Onsite support. • WinSvrSTDCore 2019 OLP 16Lic NL Gov CoreLic *Will serve as domain controller for client computers
Application Server	• Form Factor: Rack Server • Drive Bays: Up to 8 x 2.5" Hot-Plug drives. • CPU: Intel Xeon Gold 6238 2.1GHz, 30.25M cache, 22C/44T, 140W • Memory: 2 x 16GB 3200MT/s RDIMM Dual Rank. • Storage: ○ 2 x 480GB SSD SATA Mixed Used 6Gbps 512e Hot Plug ○ 4 x 1.92TB SSD SATA Mixed Used 6Gbps 512e Hot Plug • RAID Controller: ○ 8-port 12Gbps Hardware RAID controller ○ Able to support RAID levels 0, 1, 5, 6, 10, & 50. ○ Can supports real-time RAID monitoring and hardware inventory • I/O & Ports: ○ Dual Port 1Gb LOM ○ Quad Port 10GbE SFP+ • Power Supply: Dual 550W Redundant Hot Plug Power Supplies. • Supports Integration with third-party consoles. • Supports Connection for third-party consoles. • Supported Operating System: ○ Windows Server with Hyper-V ○ RHEL ○ SLES ○ Ubuntu Server ○ Citrix XenServer ○ VMware ESXi • Able to support the following security features: ○ TPM 1.2/2.0 optional ○ Secure Boot ○ Silicon Root of Trust ○ Cryptographically signed firmware ○ System Lockdown ○ System Erase • Must include server warranty of 3-years 24x7 Onsite support. • WinSvrSTDCore 2019 OLP 16Lic NL Gov CoreLic *Will serve as a server to run specific applications needed by the Provincial Government of Cagayan
6 Core Fiber Optic Cable (1lot)	• Opti-Core Fiber Optic Distribution Cable shall be used. • The Contractor shall supply and install multi-core fiber optic cables as the vertical/horizontal backbone cables as noted in this specification and in the drawings/SLD.

	• The Contractor shall observe the bending radius and pulling strength requirements of all backbone cables during handling and installation. • Each optical fiber shall be buffered with color-coded PVC for identification of multi-core fiber optics cable. The connector type shall be SC connector. • The fiber optic cable shall meet the NEC requirements for OFNR or OFNP and comply with Bell core, FDDI, TIA/EIA-568-C.3, IEC and ICEA standards. • All Multimode optical fiber cables shall be graded index with core/cladding construction of 50/125 m; the fiber shall be compliant to the performance specifications for OM3 Multimode fiber detailed in ISO11801. • The fiber optic cable shall be protected by means of either a cable tray or a dedicated fiber routing system at all times. Each end of the fiber optic cable shall contain a slack storage box with approximately three (3) meters of cable slack. • OM3 Maximum Cable Attenuation Performance o Transmission Wavelength: 850nm – 1300nm o Maximum Attenuation: 3.5 – 1.5
Pigtail SC Type OM3 (SC Connector)	*Will serve as a fast connection from MDF to IDF • TIA/EIA-604-3[SC] • Ferrule type: Zirconia ceramic ferrule with a pre-polished fiber stub. • Insertion Loss: 0.3dB average (multimode). • Return Loss: >50dB (multimode) • No special fiber termination tools required. • Translucent inner housing assembly facilitates inspection of the fiber termination quality, results in rapid installations, improved termination yields, and lower installed costs. • Mechanical cable retention consistently provides higher than industry standard cable retention; requires no adhesive, speeding installation. • Allow up to ten (10) re-terminations.
Fiber Optic Patch Cord Duplex OM3	*Will serve as link from fibre panel to Switches • Pass all TIA/EIA-568-C.3 performance requirements • Insertion loss per connection: 0.10dB • Return loss: 20dB min. (multimode); 26dB min. (10Gig multimode) • 100% factory terminated and tested for insertion loss • Meets UL1666 (OFNR) flame ratings • Lifetime traceability of test data to a Q.C. number on each patch cord • Duplex Patch Cords include Duplex Clips to maintain polarity • "The Contractor shall supply and install multi-core fiber optic cables with patch panel 1U as the vertical/horizontal backbone cables as noted in this specification and in the drawings/SLD." • The type of fiber optic patch cords to be used shall be selected to suit the type of fiber optic connector that is installed in the corresponding fiber termination tray.
Horizontal Cabling	*Will serve as link from Switch to Switch **1. Category 6 UTP Cable** • The Contractor shall supply and install horizontal cables to connect each TO to the FD termination hardware for the respective floor. • The type of horizontal cables used for each work location shall be 4 pair Category 6 unshielded twisted pair UTP construction. • The Cat6 UTP cable shall be constructed of 24 AWG copper conductors with HDPE insulation. • The copper conductors shall be twisted into pairs, separated by a cross-divider; crosstalk cancellation spiral in the form of a cross that maintains constant distance between all the 4 pairs. This will ensure that even under torsion during installation, the crosstalk should be constant over the whole cable. • The copper conductors shall be covered in a flame retard PVC jacket.

- The Cat6 UTP cable shall be Underwriter's Laboratories (UL) listed type CM.
- The Cat6 UTP cable must exceed TIA/EIA-568 C.2 Category 6 requirements. It must be tested to Class E to ensure performance for any application up to and including 1000Mbps.
- The Cat6 UTP cable must meet requirement specified for current applications such as IEEE 802.3, 10/100/1000 BASE T; IEEE 802.5, 4/16/100Mbps; ATM Forum 52/155/622/1200 Mbps, 1 Gigabit Networking.
- The horizontal cables shall be run using a star topology format from the TR on each floor to every individual TO. All cable routes must follow the routes and directions described on the drawings/SLD.
- The length of each individual run of horizontal cable from the TR to the TO shall not exceed 90m.
- The Contractor shall observe the bending radius and pulling strength requirements of the horizontal cable during handling and installation.
- Each run of cable between the TR and the TO shall be continuous without any joints or splices, except where consolidation points are required. Installation practice shall comply to manufacturer best practices.
- The cable manufacturer shall be ISO 9001 and 14001 registered.

1. Equipment Patch Cords

- All Category 6 patch cords shall be factory terminated and supported by the system manufacturer with modular plugs featuring EASY CONTROL BY TURNING BOOT to support easy moves, adds and changes.
- The type of cable used for station cords shall be 4 pair Category 6 unshielded twisted pair UTP of a stranded construction. Each patch cord shall be QC, 100% performance tested at the factory in a channel test to the proposed TIA/EIA-568-C.2 Category 6 standard.
- All patch cord shall contain a molded strain relief for the cable termination.
- All patch cord shall consist of round, 32 AWG tinned copper, stranded conductors insulated with solid polyolefin, tightly twisted into individual pairs and jacketed with flame retardant PVC. The patch cord shall come in standard lengths of one meter for Switch to Patch Panel and 3 meters for TO to Desktop, IP Phone and AP.
- All patch cord shall be UL rated 1863 and meets IEC 60603-7.
- All patch cord shall be dual rated to meet CM and LSZH flame ratings.
- All patch cord shall meet ANSI/TIA-968-A and FCC Part 68 Subpart F; contacts plated with 50 micro-inches of gold.
- The length of each station patch cord in Work Area shall be 3 meters.
- All patch cord shall have Labels on it to provide identification of performance level, length, and quality control number.
- All patch cord shall compatible with optional RJ45 plug lock-in device to prevent unauthorized removal of cable, IP phone, other networking equipment, or critical connection.

3. Copper Patch Panel

- The patch panel shall be modular with snap-in modular jack, and allow front access.
- • Modular patch panels shall consist of a metal panel with molded snap-in faceplates which can be front releasable.
- The modular patch panel shall support the appropriate Category 6 cabling and shall facilitate cross-connection and inter-connection using RJ45 8 position 8 conductors modular plug patch cords.
- Patch panels shall accept all Mini-Com modules for UTP, STP, fiber, or A/V applications and shall mount to standard 19" racks
- The modular patch panel shall be able to accommodate 24 AWG cable conductors.
- The modular patch panel shall be Underwriter's Laboratories (UL□) listed.
- The modular patch panel shall be of 1RU 24-port for 19" rack mounting.

Scope of Work – Cabling	• High density 1RU 48-port or 2RU 72-port configuration might be used if rack space is limited. • Separate modular patch panel shall be used for the termination of voice and data. **4. Horizontal Cable Manager** • Horizontal cable manager must be used with patch panel. • The horizontal cable manager shall be capable of managing cables on the front, of any 19" Data rack. • The horizontal cable manager shall consist of a 1-piece construction that is molded out of plastic. • The horizontal cable manager shall have pass through holes that incorporate integral bend radius control as well as finger with rounded edges. • The horizontal cable manager shall have rigid end fingers that incorporate integral bend radius control. The horizontal cable manager shall be available in 1RU, front only. • Supply and Delivery of Materials and Components • Underground/burial works for the fiber backbone which includes excavation, trenching, backfilling, and other necessary works. • Fiber cable pulling and layout on the designated areas. • Installation of data cabinets in designated areas. • Installation of fiber patch panel and termination. • Installation of roughing-ins with proper hangers and supports. • UTP cable pulling and layout on the designated areas. • Installation of patch panels, cable managers, faceplates and patch cords. • End to end testing, tagging and harnessing of all installed cables. • Restoration of affected areas. • Testing, commissioning and documentation. Turn-over and Acceptance."
Implementation Services of Switches and Access Points	• Configuration of Basic and Advanced Settings • Configuration of VLAN & Other Protocols • Testing & Verification of Configuration & Connectivity Knowledge Transfer
After-Sales Support	Unlimited 8x5 Helpdesk Support (no onsite) • Phone Support • Email Support Remote Support
	All works shall be directly supervised by the Information Systems unit. **A. Manpower Requirement** The bidder shall include in his quotation a statement of manpower requirement for the project for evaluation. **B. Deliverables**

No.	Particulars		Unit	Qty
1	Access Points		unit	30
2	Access Switch		unit	10

3	Core Switch		unit	2
4	FIREWALL		unit	1
5	Active Directory Server		unit	1
6	Application Server		unit	1
7	WinSvrSTDCore 2019 OLP 16Lic NL Gov CoreLic		lics	2
8	Fiber Cables		lot	1
9	UTP - Horizontal Cabling		lot	1

C. Training/Aftersales Service/Parts Warranty

Users Training for at least 4 personnel is required. Warranty period shall be
for a period of One (1) year on parts and service. Technical Support shall
be provided within 24 hours upon receipt of communication thereof via email
or phone call. In case of latent manufacturing defects, the supplier shall
replace the defective components within 7 days upon receipt of
communication letter/request.

Section VIII. Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

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

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

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

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

Technical Documents

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

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

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

☐ (i) Conformity with the Technical Specifications,
(j) Production/delivery schedule
(k) Manpower requirements
(l) After-sales/parts warranty
(m) Un amended Sales Literature
(n) Professional License
(o) Curriculum Vitae

☐ (p) 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

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

☐ (r) 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

☐ (s) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;

or

duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

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

☐ (t) *[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.

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

25 FINANCIAL COMPONENT ENVELOPE

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

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


Republic of the Philippines
gppb
Government Procurement Policy Board