REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF CUSTOMS
Port Area, Manila

BIDDING DOCUMENTS

FOR THE

Managed High-Speed Network And Internet Connectivity

Project ID No. : BOC-GOODS-2015-42
October 2015

TABLE OF CONTENTS

SECTION I. INVITATION TO BID

SECTION II. INSTRUCTIONS TO BIDDERS

SECTION III. BID DATA SHEET

SECTION IV. GENERAL CONDITIONS OF CONTRACT

SECTION V. SPECIAL CONDITIONS OF CONTRACT

SECTION VI. SCHEDULE OF REQUIREMENTS

SECTION VII. TECHNICAL SPECIFICATIONS

SECTION VIII. BIDDING FORMS

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF CUSTOMS
PORT AREA, MANILA

SECTION I. INVITATION TO BID
Managed High-Speed Network and Internet Connectivity

1. The Bureau of Customs (BOC) through the authorized appropriations under the FY 2015 General Appropriations Act intends to apply the sum of One-Hundred Two Million Pesos (PhP102,000,000.00) being the Approved Budget for the Contract (ABC) to payments under the contract for the **Managed High-Speed Network and Internet Connectivity**. Bids received in excess of the ABC shall be automatically rejected at the bid opening.

2. The BOC now invites bids for the project, Managed High-Speed Network and Internet Connectivity. Delivery of the goods/services shall be in accordance with the delivery schedule under Section VI, Schedule of Requirements. Bidders should have completed, within five (5) years prior to the date of Pre-Bid Conference, 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 (ITB).

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "pass/fail" criterion as specified in the Implementing Rules and Regulations (IRR) of Republic Act (R.A.) No. 9184, otherwise known as the "Government Procurement Reform Act."

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

5. A complete set of Bidding Documents may be acquired by interested Bidders on October 21, 2015 from the address below and upon payment of a non-refundable fee for the Bidding Documents, pursuant to the latest guidelines issued by the GPPB, in the amount of Fifty Thousand Pesos (PhP50,000.00). It may also be downloaded free of charge from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and the website of the BOC, provided that Bidders shall pay the nonrefundable fee for the Bidding Documents not later than the submission of their bids.

6. The BOC will hold a Pre-Bid Conference on October 30, 2015, 1:30 p.m. at the GSD Conference Room, Ground Floor, OCOM Building, South Harbor, Gate 3, Port Area, Manila, which shall be open to all interested parties.

7. Bids must be delivered to the address below on or before November 13, 2015, 1:30 p.m. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in the ITB Clause 18.

   Bid opening shall be on November 13, 2015, 1:30 p.m. at the GSD Conference Room, Ground Floor, OCOM Building, South Harbor, Gate 3, Port Area, Manila. Bids will be opened in the presence of the Bidders' representatives who choose to attend at the address below. Late bids shall not be accepted.

8. The bidders shall drop three (3) copies of their bids containing the technical component of the bid, including the eligibility requirements, and the financial component of the bid, in two (2) separate sealed envelopes in the bid box located at the above-mentioned address.

9. The BOC reserves the right to accept or reject any bid, to annul the bidding process, and to reject all bids at any time prior to contract award, without thereby incurring any liability to the affected bidder or bidders.

10. For further information, please refer to:

BOC-BAC Secretariat
General Services Division
OCOM Bldg., South Harbor, Gate 3, Port Area, Manila
Telefax No. 527-9757
Email address: bocbacsecretariat2015@gmail.com

DIR. DIMPNA O. LEJOS
Officer-In-Charge
Internal Administration Group
Chairperson, BOC-BAC

Section II. Instructions to Bidders

TABLE OF CONTENTS

A. General 7

1. Scope of Bid 7
2. Source of Funds 7
3. Corrupt, Fraudulent, Collusive, and Coercive Practices 7
4. Conflict of Interest 8
5. Eligible Bidders 9
6. Bidder’s Responsibilities 10
7. Origin of Goods 12
8. Subcontracts 12

B. Contents of Bidding Documents 12

9. Pre-Bid Conference 12
10. Clarification and Amendment of Bidding Documents 13

C. Preparation of Bids 13

11. Language of Bid 13
12. Documents Comprising the Bid: Eligibility and Technical Components 14
13. Documents Comprising the Bid: Financial Component 15
14. Alternative Bids 16
15. Bid Prices 16
16. Bid Currencies 17
17. Bid Validity 18
18. Bid Security 18
19. Format and Signing of Bids 20
20. Sealing and Marking of Bids 20

D. Submission and Opening of Bids 21

21. Deadline for Submission of Bids 21
22. Late Bids 21
23. Modification and Withdrawal of Bids 21
24. Opening and Preliminary Examination of Bids 22

E. Evaluation and Comparison of Bids 23

25. Process to be Confidential 23
26. Clarification of Bids 23
27. Domestic Preference 23
28. Detailed Evaluation and Comparison of Bids 24
29. Post-Qualification 25
30. Reservation Clause 26

F. Award of Contract 27

31. Contract Award 27
32. Signing of the Contract 28
33. Performance Security 28
34. Notice to Proceed 29

35. Protest Mechanism 29

A. General

1. Scope of Bid

1.1. The procuring entity named in the **BDS** (hereinafter referred to as the "Procuring Entity") wishes to receive bids for supply and delivery of the goods as described in Section VII. Technical Specifications (hereinafter referred to as the "Goods").

1.2. The name, identification, and number of lots specific to this bidding are provided in the **BDS**. The contracting strategy and basis of evaluation of lots is described in ITB Clause 28.

2. Source of Funds

The Procuring Entity has a budget or has applied for or received funds from the Funding Source named in the **BDS**, and in the amount indicated in the **BDS**. It intends to apply part of the funds received for the Project, as defined in the **BDS**, to cover eligible payments under the contract.

3. Corrupt, Fraudulent, Collusive, and Coercive Practices

3.1. Unless otherwise specified in the **BDS**, 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. In pursuance of this policy, the Procuring Entity:

(a) defines, for purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and includes the offering, giving, receiving, or soliciting of anything of value to influence the \action of any such official in the procurement process or in contract execution; entering, on behalf of the government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in RA 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) "collusive practices" means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) "coercive practices" means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) "obstructive practice" is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

3.2. Further, the Procuring Entity will seek to impose the maximum civil, administrative, and/or criminal penalties available under applicable laws on individuals and organizations deemed to be involved in any of the practices mentioned in ITB Clause 3.1(a).

3.3. Furthermore, the Funding Source and the Procuring Entity reserve the right to inspect and audit records and accounts of a bidder or supplier in the bidding for and performance of a contract themselves or through independent auditors as reflected in the GCC Clause 3.

4. Conflict of Interest

4.1. All Bidders found to have conflicting interests shall be disqualified to participate in the procurement at hand, without prejudice to the imposition of appropriate administrative, civil, and criminal sanctions. A Bidder may be considered to have conflicting interests with another Bidder in any of the events described in paragraphs (a) through (c) below and a general conflict of interest in any of the circumstances set out in paragraphs (d) through (f) below:

(a) A Bidder has controlling shareholders in common with another Bidder;

(b) A Bidder receives or has received any direct or indirect subsidy from any other Bidder;

(c) A Bidder has the same legal representative as that of another Bidder for purposes of this bid;

(d) A Bidder has a relationship, directly or through third parties, that puts them in a position to have access to information about or influence on the bid of another Bidder or influence the decisions of the Procuring Entity regarding this bidding process. This will include a firm or an organization who lends, or temporarily seconds, its personnel to firms or organizations which are engaged in consulting services for the preparation related to procurement for or implementation of the project if the personnel would be involved in any capacity on the same project;

(e) A Bidder submits more than one bid in this bidding process. However, this does not limit the participation of subcontractors in more than one bid; or

(f) A Bidder who participated as a consultant in the preparation of the design or technical specifications of the Goods and related services that are the subject of the bid.

4.2. In accordance with Section 47 of the IRR of RA 9184, all Bidding Documents shall be accompanied by a sworn affidavit of the Bidder that it is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), members of the Technical Working Group (TWG), members of the BAC Secretariat, the head of the Project Management Office (PMO) or the end-user unit, and the project consultants, by consanguinity or affinity up to the third civil degree. On the part of the Bidder, this Clause shall apply to the following persons:

(a) If the Bidder is an individual or a sole proprietorship, to the Bidder himself;

(b) If the Bidder is a partnership, to all its officers and members;

(c) If the Bidder is a corporation, to all its officers, directors, and controlling stockholders; and

(d) If the Bidder is a joint venture (JV), the provisions of items (a), (b), or (c) of this Clause shall correspondingly apply to each of the members of the said JV, as may be appropriate.

Relationship of the nature described above or failure to comply with this Clause will result in the automatic disqualification of a Bidder.

5. Eligible Bidders

5.1. Unless otherwise indicated in the **BDS**, the following persons shall be eligible to participate in this bidding:

(a) Duly licensed Filipino citizens/sole proprietorships;

(b) Partnerships duly organized under the laws of the Philippines and of which at least sixty percent (60%) of the interest belongs to citizens of the Philippines;

(c) Corporations duly organized under the laws of the Philippines, and of which at least sixty percent (60%) of the outstanding capital stock belongs to citizens of the Philippines;

(d) Cooperatives duly organized under the laws of the Philippines, and of which at least sixty percent (60%) of the interest belongs to citizens of the Philippines; and

(e) Unless otherwise provided in the BDS, persons/entities forming themselves into a JV, *i.e.*, a group of two (2) or more persons/entities that intend to be jointly and severally responsible or liable for a particular contract: Provided, however, that Filipino ownership or interest of the joint venture concerned shall be at least sixty percent (60%).

5.2. Foreign bidders may be eligible to participate when any of the following circumstances exist, as specified in the BDS:

(a) When a Treaty or International or Executive Agreement as provided in Section 4 of the RA 9184 and its IRR allow foreign bidders to participate;

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

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

(d) When there is a need to prevent situations that defeat competition or restrain trade.

5.3. Government corporate entities may be eligible to participate only if they can establish that they (a) are legally and financially autonomous, (b) operate under commercial law, and (c) are not dependent agencies of the GOP or the Procuring Entity.

5.4. Unless otherwise provided in the **BDS**, the Bidder must have completed at least one contract similar to the Project the value of which, adjusted to current prices using the National Statistics Office consumer price index, must be at least equivalent to a percentage of the ABC stated in the **BDS**.

For this purpose, contracts similar to the Project shall be those described in the **BDS**, and completed within the relevant period stated in the Invitation to Bid and **ITB** Clause 12.1(a)(iii).

5.5. The Bidder must submit a computation of its Net Financial Contracting Capacity (NFCC), which must be at least equal to the ABC to be bid, calculated as follows:

NFCC = [(Current assets minus current liabilities) (K)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started coinciding with the contract for this Project.

Where:

K = 10 for a contract duration of one year or less, 15 for a contract duration of more than one year up to two years, and 20 for a contract duration of more than two years.

The values of the bidder’s current assets and current liabilities shall be based on the data submitted to the BIR, through its Electronic Filing and Payment System (EFPS).

6. Bidder’s Responsibilities

6.1. The Bidder or its duly authorized representative shall submit a sworn statement in the form prescribed in Section VIII. Bidding Forms as required in ITB Clause 12.1(b) (iii).

6.2. The Bidder is responsible for the following:

(a) Having taken steps to carefully examine all of the Bidding Documents;

(b) Having acknowledged all conditions, local or otherwise, affecting the implementation of the contract;

(c) Having made an estimate of the facilities available and needed for the contract to be bid, if any; and

(d) Having complied with its responsibility to inquire or secure Supplemental/Bid Bulletin(s) as provided under ITB Clause 10.3.

(e) Ensuring that it is not "blacklisted" or barred from bidding by the GOP or any of its agencies, offices, corporations, or LGUs, including foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the GPPB;

(f) Ensuring that 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;

(g) Authorizing the Head of the Procuring Entity or its duly authorized representative/s to verify all the documents submitted;

(h) Ensuring that the signatory is the duly authorized representative of the Bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the Bidder in the bidding, with the duly notarized Secretary's Certificate attesting to such fact, if the Bidder is a corporation, partnership, cooperative, or joint venture;

(i) Complying with the disclosure provision under Section 47 of RA 9184 in relation to other provisions of RA 3019; and

(j) Complying with existing labor laws and standards, in the case of procurement of services.

Failure to observe any of the above responsibilities shall be at the risk of the Bidder concerned.

6.3. The Bidder is expected to examine all instructions, forms, terms, and specifications in the Bidding Documents.

6.4. It shall be the sole responsibility of the Bidder to determine and to satisfy itself by such means as it considers necessary or desirable as to all matters pertaining to the contract to be bid, including: (a) the location and the nature of this Project; (b) climatic conditions; (c) transportation facilities; and (d) other factors that may affect the cost, duration, and execution or implementation of this Project.

6.5. The Procuring Entity shall not assume any responsibility regarding erroneous interpretations or conclusions by the prospective or eligible bidder out of the data furnished by the procuring entity.

6.6. The Bidder shall bear all costs associated with the preparation and submission of his bid, and the Procuring Entity will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6.7. Before submitting their bids, the Bidder is deemed to have become familiar with all existing laws, decrees, ordinances, acts and regulations of the Philippines which may affect this Project in any way.

6.8. The Bidder should note that the Procuring Entity will accept bids only from those that have paid the nonrefundable fee for the Bidding Documents at the office indicated in the Invitation to Bid.

7. Origin of Goods

Unless otherwise indicated in the **BDS**, there is no restriction on the origin of goods other than those prohibited by a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, subject to ITB Clause 27.1.

8. Subcontracts

8.1. Unless otherwise specified in the **BDS**, the Bidder may subcontract portions of the Goods to an extent as may be approved by the Procuring Entity and stated in the **BDS**. However, subcontracting of any portion shall not relieve the Bidder from any liability or obligation that may arise from the contract for this Project.

8.2. Subcontractors must comply with the eligibility criteria and the documentary requirements specified in the **BDS**. In the event that any subcontractor is found by the Procuring Entity to be ineligible, the subcontracting of such portion of the Goods shall be disallowed.

8.3. The Bidder may identify the subcontractor to whom a portion of the Goods will be subcontracted at any stage of the bidding process or during contract implementation. If the Bidder opts to disclose the name of the subcontractor during bid submission, the Bidder shall include the required documents as part of the technical component of its bid.

B. Contents of Bidding Documents

9. Pre-Bid Conference

9.1. (a) If so specified in the **BDS**, a pre-bid conference shall be held at the venue and on the date indicated therein, to clarify and address the Bidders' questions on the technical and financial components of this Project.

(b) *The pre-bid conference shall be held at least twelve (12) calendar days before the deadline for the submission and receipt of bids. If the Procuring Entity determines that, by reason of the method, nature, or complexity of the contract to be bid, or when international participation will be more advantageous to* *the GOP, a longer period for the preparation of bids is necessary, the pre-bid conference shall be held at least thirty (30) calendar days before the deadline for the submission and receipt of bids, as specified in the* ***BDS****.*

9.2. Bidders are encouraged to attend the pre-bid conference to ensure that they fully understand the Procuring Entity's requirements. Non-attendance of the Bidder will in no way prejudice its bid; however, the Bidder is expected to know the changes and/or amendments to the Bidding Documents discussed during the pre-bid conference.

9.3. Any statement made at the pre-bid conference shall not modify the terms of the Bidding Documents unless such statement is specifically identified in writing as an amendment thereto and issued as a Supplemental/Bid Bulletin.

10. Clarification and Amendment of Bidding Documents

10.1. Bidders who have purchased the Bidding Documents may request for clarifications on any part of the Bidding Documents for an interpretation. Such a request must be in writing and submitted to the Procuring Entity at the address indicated in the **BDS** at least ten (10) calendar days before the deadline set for the submission and receipt of bids.

10.2. Supplemental/Bid Bulletins may be issued upon the Procuring Entity's initiative for purposes of clarifying or modifying any provision of the Bidding Documents not later than seven (7) calendar days before the deadline for the submission and receipt of bids. Any modification to the Bidding Documents shall be identified as an amendment.

10.3. Any Supplemental/Bid Bulletin issued by the BAC shall also be posted on the Philippine Government Electronic Procurement System (PhilGEPS) and the website of the Procuring Entity concerned, if available. It shall be the responsibility of all Bidders who secure the Bidding Documents to inquire and secure Supplemental/Bid Bulletins that may be issued by the BAC. However, Bidders who have submitted bids before the issuance of the Supplemental/Bid Bulletin must be informed and allowed to modify or withdraw their bids in accordance with ITB Clause 23.

C. Preparation of Bids

11. Language of Bid

The bid, as well as all correspondence and documents relating to the bid exchanged by the Bidder and the Procuring Entity, shall be written in English. If the eligibility requirements or statements, the bids, and all other documents submitted to the BAC are in foreign language other than English, it must be accompanied by a translation of the documents in English. The documents shall be translated by the relevant foreign government agency, the foreign government agency authorized to translate documents, or a registered translator in the foreign bidder's country; and 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. The English translation shall govern, for purposes of interpretation of the bid.

12. Documents Comprising the Bid: Eligibility and Technical Components

12.1. Unless otherwise indicated in the **BDS**, the first envelope shall contain the following eligibility and technical documents:

(a) Eligibility Documents –

Class "A" Documents:

(i) Registration certificate from the Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for cooperatives, or any proof of such registration as stated in the **BDS**;

(ii) Mayor's permit issued by the city or municipality where the principal place of business of the prospective bidder is located;

(iii) Statement of all its ongoing government and private contracts within the period stated in the **BDS**, 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

Statement identifying the bidder's single largest completed contract similar to the contract to be bid, except under conditions provided for in Sec. 23.5.1.3. of the IRR, within the relevant period as provided in the **BDS**.

The statement shall include, for each contract, the following:

(iii.1) name of the contract;

(iii.2) date of the contract;

(iii.3) kinds of Goods;

(iii.4) amount of contract and value of outstanding contracts;

(iii.5) date of delivery; and

(iii.6) end user's acceptance or official receipt(s) issued for the contract, if completed.

(iv) Audited financial statements, stamped "received" by the Bureau of Internal Revenue (BIR) or its duly accredited and authorized institutions, for the preceding calendar year, which should not be earlier than two (2) years from bid submission;

(v) NFCC computation in accordance with ITB Clause 5.5;

(vi) Tax clearance per Executive Order 398, Series of 2005, as finally reviewed and approved by the BIR.

Class "B" Document:

(vii) If applicable, the 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.

(b) Technical Documents –

(i) Bid security in accordance with ITB Clause 18. If the Procuring Entity requires the bidders to submit the bid security in the form of:

(i.1) a bank draft/guarantee or an irrevocable letter of credit issued by a foreign bank, it shall be accompanied by a confirmation from a Universal or Commercial Bank; or

(i.2) a surety bond, it shall be accompanied by a certification by the Insurance Commission that the surety or insurance company is authorized to issue such instruments;

(ii) Conformity with technical specifications, as enumerated and specified in Sections VI and VII of the Bidding Documents; and

(iii) Sworn statement in accordance with Section 25.2(a)(iv) of the IRR of RA 9184 and using the form prescribed in Section VIII. Bidding Forms.

13. Documents Comprising the Bid: Financial Component

13.1. Unless otherwise stated in the **BDS**, the financial component of the bid shall contain the following:

(a) Financial Bid Form, which includes bid prices and the bill of quantities and the applicable Price Schedules, in accordance with ITB Clauses 15.1 and 15.4;

(b) If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification from the DTI, SEC, or CDA issued in accordance with **ITB** Clause 27, unless otherwise provided in the **BDS**; and

(c) Any other document related to the financial component of the bid as stated in the **BDS**.

13.2. (a) Unless otherwise stated in the **BDS**, all bids that exceed the ABC shall not be accepted.

(b) Unless otherwise indicated in the **BDS**, for foreign-funded procurement, a ceiling may be applied to bid prices provided the following conditions are met:

(i) Bidding Documents are obtainable free of charge on a freely accessible website. If payment of Bidding Documents is required by the procuring entity, payment could be made upon the submission of bids.

(ii) The procuring entity has procedures in place to ensure that the ABC is based on recent estimates made by the responsible unit of the procuring entity and that the estimates reflect the quality, supervision and risk and inflationary factors, as well as prevailing market prices, associated with the types of works or goods to be procured.

(iii) The procuring entity has trained cost estimators on estimating prices and analyzing bid variances.

(iv) The procuring entity has established a system to monitor and report bid prices relative to ABC and engineer's/procuring entity's estimate.

(v) The procuring entity has established a system to monitor and report bid prices relative to ABC and procuring entity's estimate. The procuring entity has established a monitoring and evaluation system for contract implementation to provide a feedback on actual total costs of goods and works.

14. Alternative Bids

Alternative Bids shall be rejected. For this purpose, alternative bid is an offer made by a Bidder in addition or as a substitute to its original bid which may be included as part of its original bid or submitted separately therewith for purposes of bidding. A bid with options is considered an alternative bid regardless of whether said bid proposal is contained in a single envelope or submitted in two (2) or more separate bid envelopes.

15. Bid Prices

15.1. The Bidder shall complete the appropriate Price Schedules included herein, stating the unit prices, total price per item, the total amount and the expected countries of origin of the Goods to be supplied under this Project.

15.2. The Bidder shall fill in rates and prices for all items of the Goods described in the Bill of Quantities. Bids not addressing or providing all of the required items in the Bidding Documents including, where applicable, Bill of Quantities, shall be considered non-responsive and, thus, automatically disqualified. In this regard, where a required item is provided, but no price is indicated, the same shall be considered as non-responsive, but specifying a "0" (zero) for the said item would mean that it is being offered for free to the Government.

15.3. The terms Ex Works (EXW), Cost, Insurance and Freight (CIF), Cost and Insurance Paid to (CIP), Delivered Duty Paid (DDP), and other trade terms used to describe the obligations of the parties, shall be governed by the rules prescribed in the current edition of the International Commercial Terms (INCOTERMS) published by the International Chamber of Commerce, Paris.

15.4. 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), including all customs duties and sales and other taxes already paid or payable:

(i.1) on the components and raw material used in the manufacture or assembly of Goods quoted ex works or ex factory; or (i.2) on the previously imported Goods of foreign origin quoted ex warehouse, ex showroom, or off-the-shelf and any Procuring Entity country sales and other taxes which will be payable on the Goods if the contract is awarded.

(ii) The price for inland transportation, insurance, and other local costs incidental to delivery of the Goods to their final destination.

(iii) The price of other (incidental) services, if any, listed in the **BDS**.

(b) For Goods offered from abroad:

(i) Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted 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, listed in the **BDS**.

15.5. Prices quoted by the Bidder shall be fixed during the Bidder's performance of the contract and not subject to variation or price escalation on any account. A bid submitted with an adjustable price quotation shall be treated as non-responsive and shall be rejected, pursuant to ITB Clause 24.

All bid prices shall be considered as fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances. Extraordinary circumstances refer to events that may be determined by the National Economic and Development Authority in accordance with the Civil Code of the Philippines, and upon the recommendation of the Procuring Entity. Nevertheless, in cases where the cost of the awarded contract is affected by any applicable new laws, ordinances, regulations, or other acts of the GOP, promulgated after the date of bid opening, a contract price adjustment shall be made or appropriate relief shall be applied on a no loss-no gain basis.

16. Bid Currencies

16.1. Prices shall be quoted in the following currencies:

(a) For Goods that the Bidder will supply from within the Philippines, the prices shall be quoted in Philippine Pesos.

(b) For Goods that the Bidder will supply from outside the Philippines, the prices may be quoted in the currency(ies) stated in the **BDS**. 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.

16.2. If so allowed in accordance with **ITB** Clause 16.1, the Procuring Entity for purposes of bid evaluation and comparing the bid prices will convert the amounts in various currencies in which the bid price is expressed to Philippine Pesos at the foregoing exchange rates.

16.3. Unless otherwise specified in the **BDS**, payment of the contract price shall be made in Philippine Pesos.

17. Bid Validity

17.1. Bids shall remain valid for the period specified in the **BDS** which shall not exceed one hundred twenty (120) calendar days from the date of the opening of bids.

17.2. In exceptional circumstances, prior to the expiration of the Bid validity period, the Procuring Entity may request Bidders to extend the period of validity of their bids. The request and the responses shall be made in writing. The bid security described in ITB Clause 18 should also be extended corresponding to the extension of the bid validity period at the least. A Bidder may refuse the request without forfeiting its bid security, but his bid shall no longer be considered for further evaluation and award. A Bidder granting the request shall not be required or permitted to modify its bid.

18. Bid Security

18.1. The procuring entity shall prescribe in the **BDS** the acceptable forms of bid security that bidders may opt to use, which shall include the Bid Securing Declaration provided in Section 27.5 if this IRR and at least one (1) other form, the amount of which shall be equal to a percentage of the ABC in accordance with the following schedule:

Form of Bid Security	Amount of Bid Security (Equal to Percentage of the ABC)
(a) Cash or cashier's/manager's check issued by a Universal or Commercial Bank.	Two percent (2%)
(b) Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank.	
(c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	Five percent (5%)
(d) Any combination of the foregoing.	Proportionate to share of form with respect to total amount of security
(e) Bid Securing Declaration	No percentage required

For biddings conducted by LGUs, the Procuring Entity may also require bidders to submit bid securities in the form of cashier's/manager's check, bank draft/guarantee, or irrevocable letter of credit from other banks certified by the BSP as authorized to issue such financial statement.

The Bid Securing Declaration mentioned above is an undertaking which states, among others, that the bidder shall enter into contract with the procuring entity and furnish the performance security required under ITB Clause 33.2, from receipt of the Notice of Award, and committing to pay the corresponding fine, and be suspended for a period of time from being qualified to participate in any government procurement activity in the event it violates any of the conditions stated therein as provided in the guidelines issued by the GPPB.

18.2. The bid security should be valid for the period specified in the **BDS**. Any bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

18.3. No bid securities shall be returned to bidders after the opening of bids and before contract signing, except to those that failed or declared as post-disqualified, upon submission of a written waiver of their right to file a motion for reconsideration and/or protest. Without prejudice on its forfeiture, bid securities shall be returned only after the bidder with the Lowest Calculated and Responsive Bid has signed the contract and furnished the performance security, but in no case later than the expiration of the bid security validity period indicated in **ITB** Clause 18.2.

18.4. Upon signing and execution of the contract pursuant to **ITB** Clause 32, and the posting of the performance security pursuant to **ITB** Clause 33, the successful Bidder's bid security will be discharged, but in no case later than the bid security validity period as indicated in the **ITB** Clause 18.2.

18.5. The bid security may be forfeited:

(a) if a Bidder:

(i) withdraws its bid during the period of bid validity specified in **ITB** Clause 17;

(ii) does not accept the correction of errors pursuant to **ITB** Clause 28.3 (b);

(iii) fails to submit the requirements within the prescribed period or a finding against their veracity as stated in **ITB** Clause 29.2;

(iv) submission of eligibility requirements containing false information or falsified documents;

(v) submission of bids that contain false information or falsified documents, or the concealment of such information in the bids in order to influence the outcome of eligibility screening or any other stage of the public bidding;

(vi) allowing the use of one's name, or using the name of another for purposes of public bidding;

(vii) withdrawal of a bid, or refusal to accept an award, or enter into contract with the Government without justifiable cause, after the Bidder had been adjudged as having submitted the Lowest Calculated and Responsive Bid;

(viii) refusal or failure to post the required performance security within the prescribed time;

(ix) refusal to clarify or validate in writing its bid during post-qualification within a period of seven (7) calendar days from receipt of the request for clarification;

(x) any documented attempt by a bidder to unduly influence the outcome of the bidding in his favor;

(xi) failure of the potential joint venture partners to enter into the joint venture after the bid is declared successful; or

(xii) all other acts that tend to defeat the purpose of the competitive bidding, such as habitually withdrawing from bidding, submitting late Bids or patently insufficient bid, for at least three (3) times within a year, except for valid reasons.

(b) if the successful Bidder:

(i) fails to sign the contract in accordance with **ITB** Clause 32; or

(ii) fails to furnish performance security in accordance with **ITB** Clause 33.

19. Format and Signing of Bids

19.1. Bidders shall submit their bids through their duly authorized representative using the appropriate forms provided in Section VIII. Bidding Forms on or before the deadline specified in the **ITB** Clauses 21 in two (2) separate sealed bid envelopes, and which shall be submitted simultaneously. The first shall contain the technical component of the bid, including the eligibility requirements under **ITB** Clause 12.1, and the second shall contain the financial component of the bid.

19.2. Forms as mentioned in **ITB** Clause 19.1 must be completed without any alterations to their format, and no substitute form shall be accepted. All blank spaces shall be filled in with the information requested.

19.3. The Bidder shall prepare and submit an original of the first and second envelopes as described in **ITB** Clauses 12 and 13. In the event of any discrepancy between the original and the copies, the original shall prevail.

19.4. The bid, except for unamended printed literature, shall be signed, and each and every page thereof shall be initialed, by the duly authorized representative/s of the Bidder.

19.5. Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the duly authorized representative/s of the Bidder.

20. Sealing and Marking of Bids

20.1. Bidders shall enclose their original eligibility and technical documents described in ITB Clause 12 in one sealed envelope marked “ORIGINAL - TECHNICAL COMPONENT”, and the original of their financial component in another sealed envelope marked "ORIGINAL - FINANCIAL COMPONENT", sealing them all in an outer envelope marked "ORIGINAL BID".

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

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

20.4. All envelopes shall:

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

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

(c) be addressed to the Procuring Entity's BAC in accordance with **ITB** Clause 1.1;

(d) bear the specific identification of this bidding process indicated in the **ITB** Clause 1.2; and

(e) bear a warning "DO NOT OPEN BEFORE…" the date and time for the opening of bids, in accordance with **ITB** Clause 21.

20.5. If bids are not sealed and marked as required, the Procuring Entity will assume no responsibility for the misplacement or premature opening of the bid.

D. Submission and Opening of Bids

21. Deadline for Submission of Bids

Bids must be received by the Procuring Entity's BAC at the address and on or before the date and time indicated in the **BDS**.

22. Late Bids

Any bid submitted after the deadline for submission and receipt of bids prescribed by the Procuring Entity, pursuant to **ITB** Clause 21, shall be declared "Late" and shall not be accepted by the Procuring Entity.

23. Modification and Withdrawal of Bids

23.1. The Bidder may modify its bid after it has been submitted; provided that the modification is received by the Procuring Entity prior to the deadline prescribed for submission and receipt of bids. The Bidder shall not be allowed to retrieve its original bid, but shall be allowed to submit another bid equally sealed, properly identified, linked to its original bid marked as "TECHNICAL MODIFICATION" or "FINANCIAL MODIFICATION" and stamped "received" by the BAC. Bid modifications received after the applicable deadline shall not be considered and shall be returned to the Bidder unopened.

23.2. A Bidder may, through a Letter of Withdrawal, withdraw its bid after it has been submitted, for valid and justifiable reason; provided that the Letter of Withdrawal is received by the Procuring Entity prior to the deadline prescribed for submission and receipt of bids.

23.3. Bids requested to be withdrawn in accordance with ITB Clause 23.1 shall be returned unopened to the Bidders. A Bidder may also express its intention not to participate in the bidding through a letter which should reach and be stamped by the BAC before the deadline for submission and receipt of bids. A Bidder that withdraws its bid shall not be permitted to submit another bid, directly or indirectly, for the same contract.

23.4. No bid may be modified after the deadline for submission of bids. No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity specified by the Bidder on the Financial Bid Form. Withdrawal of a bid during this interval shall result in the forfeiture of the Bidder’s bid security, pursuant to ITB Clause 18.5, and the imposition of administrative, civil and criminal sanctions as prescribed by RA 9184 and its IRR.

24. Opening and Preliminary Examination of Bids

24.1. The BAC shall open the first bid envelopes of Bidders in public as specified in the **BDS** to determine each Bidder’s compliance with the documents prescribed in **ITB** Clause 12. For this purpose, the BAC shall check the submitted documents of each bidder against a checklist of required documents to ascertain if they are all present, using a non-discretionary “pass/fail” criterion. If a bidder submits the required document, it shall be rated “passed” for that particular requirement. In this regard, bids that fail to include any requirement or are incomplete or patently insufficient shall be considered as “failed”. Otherwise, the BAC shall rate the said first bid envelope as “passed”.

24.2. Unless otherwise specified in the BDS, immediately after determining compliance with the requirements in the first envelope, the BAC shall forthwith open the second bid envelope of each remaining eligible bidder whose first bid envelope was rated “passed”. The second envelope of each complying bidder shall be opened within the same day. In case one or more of the requirements in the second envelope of a particular bid is missing, incomplete or patently insufficient, and/or if the submitted total bid price exceeds the ABC unless otherwise provided in **ITB** Clause 13.2, the BAC shall rate the bid concerned as “failed”. Only bids that are determined to contain all the bid requirements for both components shall be rated “passed” and shall immediately be considered for evaluation and comparison.

24.3. Letters of withdrawal shall be read out and recorded during bid opening, and the envelope containing the corresponding withdrawn bid shall be returned to the Bidder unopened. If the withdrawing Bidder’s representative is in attendance, the original bid and all copies thereof shall be returned to the representative during the bid opening. If the representative is not in attendance, the bid shall be returned unopened by registered mail. The Bidder may withdraw its bid prior to the deadline for the submission and receipt of bids, provided that the corresponding

Letter of Withdrawal contains a valid authorization requesting for such withdrawal, subject to appropriate administrative sanctions.

24.4. If a Bidder has previously secured a certification from the Procuring Entity to the effect that it has previously submitted the above-enumerated Class "A" Documents, the said certification may be submitted in lieu of the requirements enumerated in **ITB** Clause 12.1(a), items (i) to (v).

24.5. In the case of an eligible foreign Bidder as described in **ITB** Clause 5, the Class "A" Documents described in **ITB** Clause 12.1(a) may be substituted with the appropriate equivalent documents, if any, issued by the country of the foreign Bidder concerned.

24.6. Each partner of a joint venture agreement shall likewise submit the requirements in **ITB** Clauses 12.1(a)(i) and 12.1(a)(ii). Submission of documents required under **ITB** Clauses 12.1(a)(iii) to 12.1(a)(v) by any of the joint venture partners constitutes compliance.

24.7. The Procuring Entity shall prepare the minutes of the proceedings of the bid opening that shall include, as a minimum: (a) names of Bidders, their bid price, bid security, findings of preliminary examination; and (b) attendance sheet. The BAC members shall sign the abstract of bids as read.

E. Evaluation and Comparison of Bids

25. Process to be Confidential

25.1. Members of the BAC, including its staff and personnel, as well as its Secretariat and TWG, are prohibited from making or accepting any kind of communication with any bidder regarding the evaluation of their bids until the issuance of the Notice of Award, unless otherwise allowed in the case of **ITB** Clause 26.

25.2. Any effort by a bidder to influence the Procuring Entity in the Procuring Entity's decision in respect of bid evaluation, bid comparison or contract award will result in the rejection of the Bidder's bid.

26. Clarification of Bids

To assist in the evaluation, comparison, and post-qualification of the bids, the Procuring Entity may ask in writing any Bidder for a clarification of its bid. All responses to requests for clarification shall be in writing. Any clarification submitted by a Bidder in respect to its bid and that is not in response to a request by the Procuring Entity shall not be considered.

27. Domestic Preference

27.1. Unless otherwise stated in the **BDS**, the Procuring Entity will grant a margin of preference for the purpose of comparison of bids in accordance with the following:

(a) The preference shall be applied when (i) the lowest Foreign Bid is lower than the lowest bid offered by a Domestic Bidder, or (ii) the lowest bid offered by a non-Philippine national is lower than the lowest bid offered by a Domestic Entity.

(b) For evaluation purposes, the lowest Foreign Bid or the bid offered by a non-Philippine national shall be increased by fifteen percent (15%).

(c) In the event that (i) the lowest bid offered by a Domestic Entity does not exceed the lowest Foreign Bid as increased, or (ii) the lowest bid offered by a non-Philippine national as increased, then the Procuring Entity shall award the contract to the Domestic Bidder/Entity at the amount of the lowest Foreign Bid or the bid offered by a non-Philippine national, as the case may be.

(d) If the Domestic Entity/Bidder refuses to accept the award of contract at the amount of the Foreign Bid or bid offered by a non-Philippine national within two (2) calendar days from receipt of written advice from the BAC, the Procuring Entity shall award to the bidder offering the Foreign Bid or the non-Philippine national, as the case may be, subject to post-qualification and submission of all the documentary requirements under these Bidding Documents.

27.2. A Bidder may be granted preference as a Domestic Entity subject to the certification from the DTI (in case of sole proprietorships), SEC (in case of partnerships and corporations), or CDA (in case of cooperatives) that the (a) sole proprietor is a citizen of the Philippines or the partnership, corporation, cooperative, or association is duly organized under the laws of the Philippines with at least Eighty five percent (75%) of its interest or outstanding capital stock belonging to citizens of the Philippines, (b) habitually established in business and habitually engaged in the manufacture or sale of the merchandise covered by his bid, and (c) the business has been in existence for at least five (5) consecutive years prior to the advertisement and/or posting of the Invitation to Bid for this Project.

27.3. A Bidder may be granted preference as a Domestic Bidder subject to the certification from the DTI that the Bidder is offering unmanufactured articles, materials or supplies of the growth or production of the Philippines, or manufactured articles, materials, or supplies manufactured or to be manufactured in the Philippines substantially from articles, materials, or supplies of the growth, production, or manufacture, as the case may be, of the Philippines.

28. Detailed Evaluation and Comparison of Bids

28.1. The Procuring Entity will undertake the detailed evaluation and comparison of bids which have passed the opening and preliminary examination of bids, pursuant to **ITB** Clause 24, in order to determine the Lowest Calculated Bid.

28.2. The Lowest Calculated Bid shall be determined in two steps:

(a) The detailed evaluation of the financial component of the bids, to establish the correct calculated prices of the bids; and

(b) The ranking of the total bid prices as so calculated from the lowest to the highest. The bid with the lowest price shall be identified as the Lowest Calculated Bid.

28.3. The Procuring Entity's BAC shall immediately conduct a detailed evaluation of all bids rated “passed,” using non-discretionary pass/fail criteria. Unless otherwise specified in the **BDS**, the BAC shall consider the following in the evaluation of bids:

(a) Completeness of the bid. Unless the ITB specifically allows partial bids, bids not addressing or providing all of the required items in the Schedule of Requirements including, where applicable, bill of quantities, shall be considered non-responsive and, thus, automatically disqualified. In this regard, where a required item is provided, but no price is indicated, the same shall be considered as non-responsive, but specifying a "0" (zero) for the said item would mean that it is being offered for free to the Procuring Entity; and

(b) Arithmetical corrections. Consider computational errors and omissions to enable proper comparison of all eligible bids. It may also consider bid modifications, if allowed in the **BDS**. Any adjustment shall be calculated in monetary terms to determine the calculated prices.

28.4. Based on the detailed evaluation of bids, those that comply with the above-mentioned requirements shall be ranked in the ascending order of their total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications, to identify the Lowest Calculated Bid. Total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications, which exceed the ABC shall not be considered, unless otherwise indicated in the **BDS**.

28.5. The Procuring Entity’s evaluation of bids shall only be based on the bid price quoted in the Financial Bid Form.

28.6. Bids shall be evaluated on an equal footing to ensure fair competition. For this purpose, all bidders shall be required to include in their bids the cost of all taxes, such as, but not limited to, value added tax (VAT), income tax, local taxes, and other fiscal levies and duties which shall be itemized in the bid form and reflected in the detailed estimates. Such bids, including said taxes, shall be the basis for bid evaluation and comparison.

29. Post-Qualification

29.1. The Procuring Entity shall determine to its satisfaction whether the Bidder that is evaluated as having submitted the Lowest Calculated Bid (LCB) complies with and is responsive to all the requirements and conditions specified in **ITB** Clauses 5, 12, and 13.

29.2. Within a non-extendible period of three (3) calendar days from receipt by the bidder of the notice from the BAC that it submitted the LCB, the Bidder shall submit the following documentary requirements:

(a) Latest income and business tax returns in the form specified in the **BDS**;

(b) Certificate of PhilGEPS Registration or PhilGEPS Registration Number if the procuring entity is a Philippine foreign office or post, provided that participating bidders should register with the PhilGEPS prior to bid opening; and

(c) Other appropriate licenses and permits required by law and stated in the **BDS**.

Failure of the Bidder declared as Lowest Calculated Bid to duly submit the requirements under this Clause or a finding against the veracity of such shall be ground for forfeiture of the bid security and disqualification of the Bidder for award.

29.3. The determination shall be based upon an examination of the documentary evidence of the Bidder's qualifications submitted pursuant to **ITB** Clauses 12 and 13, as well as other information as the Procuring Entity deems necessary and appropriate, using a non-discretionary "pass/fail" criterion.

29.4. If the BAC determines that the Bidder with the Lowest Calculated Bid passes all the criteria for post-qualification, it shall declare the said bid as the Lowest Calculated Responsive Bid, and recommend to the Head of the Procuring Entity the award of contract to the said Bidder at its submitted price or its calculated bid price, whichever is lower.

29.5. A negative determination shall result in rejection of the Bidder's Bid, in which event the Procuring Entity shall proceed to the next Lowest Calculated Bid to make a similar determination of that Bidder's capabilities to perform satisfactorily. If the second Bidder, however, fails the post qualification, the procedure for post qualification shall be repeated for the Bidder with the next Lowest Calculated Bid, and so on until the Lowest Calculated Responsive Bid is determined for contract award.

29.6. Within a period not exceeding seven (7) calendar days from the date of receipt of the recommendation of the BAC, the Head of the Procuring Entity shall approve or disapprove the said recommendation. In the case of GOCCs and GFIs, the period provided herein shall be fifteen (15) calendar days.

30. Reservation Clause

30.1. Notwithstanding the eligibility or post-qualification of a bidder, the Procuring Entity concerned reserves the right to review its qualifications at any stage of the procurement process if it has reasonable grounds to believe that a misrepresentation has been made by the said bidder, or that there has been a change in the Bidder's capability to undertake the project from the time it submitted its eligibility requirements. Should such review uncover any misrepresentation made in the eligibility and bidding requirements, statements or documents, or any changes in the situation of the Bidder which will affect its capability to undertake the project so that it fails the preset eligibility or bid evaluation criteria, the Procuring Entity shall consider the said Bidder as ineligible and shall disqualify it from submitting a bid or from obtaining an award or contract.

30.2. Based on the following grounds, the Procuring Entity reserves the right to reject any and all bids, declare a Failure of Bidding at any time prior to the contract award, or not to award the contract, without thereby incurring any liability, and make no assurance that a contract shall be entered into as a result of the bidding:

(a) If there is *prima facie* evidence of collusion between appropriate public officers or employees of the Procuring Entity, or between the BAC and any of the bidders, or if the collusion is between or among the bidders themselves, or between a bidder and a third party, including any act which restricts, suppresses or nullifies or tends to restrict, suppress or nullify competition;

(b) If the Procuring Entity's BAC is found to have failed in following the prescribed bidding procedures; or

(c) For any justifiable and reasonable ground where the award of the contract will not redound to the benefit of the GOP as follows:

(i) If the physical and economic conditions have significantly changed so as to render the project no longer economically, financially or technically feasible as determined by the head of the procuring entity;

(ii) If the project is no longer necessary as determined by the head of the procuring entity; and

(iii) If the source of funds for the project has been withheld or reduced through no fault of the Procuring Entity.

30.3. In addition, the Procuring Entity may likewise declare a failure of bidding when:

(a) No bids are received;

(b) All prospective bidders are declared ineligible;

(c) All bids fail to comply with all the bid requirements or fail post-qualification; or

(d) The bidder with the Lowest Calculated Responsive Bid (LCRB) refuses, without justifiable cause to accept the award of contract, and no award is made.

F. Award of Contract

31. Contract Award

31.1. Subject to **ITB** Clause 29, the Procuring Entity shall award the contract to the Bidder whose bid has been determined to be the LCRB.

31.2. Prior to the expiration of the period of bid validity, the Procuring Entity shall notify the successful Bidder in writing that its bid has been accepted, through a Notice of Award received personally or sent by registered mail or electronically, receipt of which must be confirmed in writing within two (2) days by the Bidder with the LCRB and submitted personally or sent by registered mail or electronically to the Procuring Entity.

31.3. Notwithstanding the issuance of the Notice of Award, award of contract shall be subject to the following conditions:

(a) Submission of the valid JVA, if applicable, within ten (10) calendar days from receipt by the Bidder of the notice from the BAC that the Bidder has the LCRB;

(b) Posting of the performance security in accordance with **ITB** Clause 33;

(c) Signing of the contract as provided in **ITB** Clause 32; and

(d) Approval by higher authority, if required.

31.4. At the time of contract award, the Procuring Entity shall not increase or decrease the quantity of goods originally specified in Section VI. Schedule of Requirements.

32. Signing of the Contract

32.1. At the same time as the Procuring Entity notifies the successful Bidder that its bid has been accepted, the Procuring Entity shall send the Contract Form to the Bidder, which contract has been provided in the Bidding Documents, incorporating therein all agreements between the parties.

32.2. Within ten (10) calendar days from receipt of the Notice of Award, the successful Bidder shall post the required performance security and sign and date the contract and return it to the Procuring Entity.

32.3. The Procuring Entity shall enter into contract with the successful Bidder within the same ten (10) calendar day period provided that all the documentary requirements are complied with.

32.4. The following documents shall form part of the contract:

(a) Contract Agreement;

(b) Bidding Documents;

(c) Winning bidder’s bid, including the Technical and Financial Proposals, and all other documents/statements submitted;

(d) Performance Security;

(e) Credit line in accordance with **ITB** Clause 5.5, if applicable;

(f) Notice of Award of Contract; and

(g) Other contract documents that may be required by existing laws and/or specified in the **BDS**.

33. Performance Security

33.1. To guarantee the faithful performance by the winning Bidder of its obligations under the contract, it shall post a performance security within a maximum period of ten (10) calendar days from the receipt of the Notice of Award from the Procuring Entity and in no case later than the signing of the contract.

33.2. The procuring entity shall prescribe at least two (2) acceptable forms of performance security taken from two (2) categories below that bidders may opt to use, denominated in Philippine Pesos and posted in favor of the Procuring Entity in an amount equal to the percentage of the total contract price in accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Equal to Percentage of the Total Contract Price)
(a) Cash or cashier's/manager's check issued by a Universal or Commercial Bank.	Five percent (5%)
(b) Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank.	
(c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security; and/or	Thirty percent (30%)
(d) Any combination of the foregoing.	Proportionate to share of form with respect to total amount of security

33.3. Failure of the successful Bidder to comply with the above-mentioned requirement shall constitute sufficient ground for the annulment of the award and forfeiture of the bid security, in which event the Procuring Entity shall initiate and complete the post qualification of the second Lowest Calculated Bid. The procedure shall be repeated until the LCRB is identified and selected for contract award. However if no Bidder passed post-qualification, the BAC shall declare the bidding a failure and conduct a re-bidding with re-advertisement.

34. Notice to Proceed

34.1. Within three (3) calendar days from the date of approval of the contract by the appropriate government approving authority, the Procuring Entity shall issue its Notice to Proceed to the Bidder.

34.2. The contract effectivity date shall be provided in the Notice to Proceed by the Procuring Entity, which date shall not be later than seven (7) calendar days from the issuance of the Notice to Proceed.

35. Protest Mechanism

Decision of the procuring entity at any stage of the procurement process may be questioned in accordance with Section 55 of the revised Implementing Rules and Regulations of Republic Act 9184.

Section III. Bid Data Sheet

ITB Clause	
1.1	The Procuring Entity is the Bureau of Customs.
1.2	This bidding shall have one (1) lot as follows: **Supply, delivery, installation, configuration, testing, commissioning, maintenance and management of BOC High-Speed Wide Area Network and Internet Service**
2	The Funding Source is: The Government of the Philippines (GOP) through the authorized appropriations under the FY 2015 General Appropriations Act in the total amount of **One Hundred and Two Million Pesos (PhP102,000,000.00).** The name of the Project is **Managed High-Speed Network and Internet Connectivity.**
3.1	No further instructions.
5.1e	Joint Venture is not allowed.
5.2	No further instructions.
5.4	The bidder must have completed, five (5) years prior to October 30, 2015, a single contract that is similar to the Project at hand and whose value must be at least fifty percent (50%) of the ABC to be bid. Such contract must be part of, or included in, the Statement under Item 12.1(a) (iii) hereof. Bidders shall include in their Bid a photocopy of Single Largest Completed Contract or Purchase Order and the corresponding proof of completion, such as (i) Certificate of Final Acceptance or Completion from the bidder's client; or (ii) Official Receipt issued by the bidder. Failure to submit a copy of Single Largest Completed Contract with proof of Completion or a failure against the veracity of such shall be a ground for disqualification of the bidder for award and forfeiture of the bid security.

	For this purpose, similar contract shall refer to the provision of telecommunication/network and internet services including the supply, delivery, installation, configuration, testing, commissioning, maintenance and management of a high-speed Wide Area Network and Internet services, with infrastructure, hardware, software, cabling, environmental equipment and other pertinent devices, of no less than 10 Mbps WAN Link; and the provision of associated services within the Philippines.
7	No further instructions.
8.1	Subcontracting is not allowed.
8.2	Not applicable.
9.1	The Procuring Entity will hold a Pre-Bid Conference for this Project on October 30, 2015, 1:30 p.m., at GSD Conference Room, Ground Floor, OCOM Building, South Harbor, Gate 3, Port Area, Manila.
10.1	The Procuring Entity's address is: Bureau of Customs OCOM Building, South Harbor, Gate 3, Port Area, Manila
12.1(a)	No further instructions.
12.1(a)(i)	For corporations/partnerships, the following shall also be submitted: latest general information sheet (GIS) and articles of incorporation partnerships by laws or amendments thereto, duly approved by the Securities and Exchange Commission.
12.1(a)(iii)	The statement of all ongoing government and private contracts shall include all such contracts undertaken within three (3) years prior to the deadline for the submission and receipt of bids. Likewise, the statement identifying the bidder's single largest completed contract similar to the contract to be bid shall be submitted.
12.1(b)(iii)	Notarization of this document shall comply with the 2004 Rules on Notarial Practice which limits competent evidence of identity to the following: (i) identification documents issued by an official agency bearing the photograph and signature of the individual i.e., passport, driver's license, SSS ID, GSIS e-card, etc.; and (ii) the oath of affirmation of one credible witness not privy to the instrument, document or transaction who is personally known to the notary public and who personally knows the individual and shows to the notary public documentary identification.
13.1	No additional requirements.
13.2	The ABC is **One-Hundred and Two Million Pesos (PhP102,000,000.00).** Any bid with a financial component exceeding this amount shall not be accepted.
15.4(a)(iii)	No additional requirements.

15.4(b)	Not applicable.
15.5	Not applicable.
16.1(b)	The Bid Prices for Goods supplied from outside of the Philippines shall be quoted in Philippine Pesos.
16.3	No further instructions.
17.1	Bids will be valid until March 12, 2016.
18.1	The bid security shall be either of the following forms and amounts: a) ***2% of the ABC or PhP2,040,000.00***, if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; b) ***5% of the ABC or PhP5,100,000.00***, if bid security is in Surety Bond accompanied with a certification from the Insurance Commission that insurance company is authorized to insure such security; c) Any combination of the foregoing proportionate to the share of form with respect to total amount of security; or d) Bid Securing Declaration. (Sample form is attached under Section VIII. Bidding Forms).
18.2	The bid security shall be valid until March 12, 2016.
20.3	Each Bidder shall submit one (1) original and two (2) duplicate copies of the first and second components of its bid.
21	The address for submission of bids is BAC Conference Room, General Services Division (GSD), Ground Floor, OCOM Building, BOC, South Harbor, Gate 3, Port Area, Manila. The deadline for submission of bids is November 13, 2015, 1:30 p.m. Late bids shall not be accepted.
24.1	The place of bid opening is at BAC Conference Room, General Services Division (GSD), Ground Floor, OCOM Building, BOC, South Harbor, Gate 3, Port Area, Manila. The date and time of bid opening is November 13, 2015, 1:30 p.m.
24.2	No further instructions.
27.1	No further instructions.
28.3	No further instructions.
28.3(b)	Bid modification is allowed in case of arithmetical corrections only.
28.4	No further instructions.

29.2(b)	Latest Income and Business Tax Returns, filed and paid through the Electronic Filing and Payments System (EFPS), consisting of the following: - 2013 and 2014 Income Tax Return with proof of payment - VAT Returns (Form 2550M and 2550Q) or Percentage Tax Returns (2551M) with proof of payment covering the months from April 2015 to September 2015.
29.2(d)	No further instructions.
32.4(g)	No further instructions.

Section IV. General Conditions of Contract

TABLE OF CONTENTS

1. **Definitions**..........35
2. **Corrupt, Fraudulent, Collusive, and Coercive Practices**..........35
3. **Inspection and Audit by the Funding Source**..........37
4. **Governing Law and Language**..........37
5. **Notices**..........37
6. **Scope of Contract**..........37
7. **Subcontracting**..........38
8. **Procuring Entity's Responsibilities**..........38
9. **Prices**..........38
10. **Payment**..........38
11. **Advance Payment and Terms of Payment**..........39
12. **Taxes and Duties**..........39
13. **Performance Security**..........40
14. **Use of Contract Documents and Information**..........40
15. **Standards**..........40
16. **Inspection and Tests**..........41
17. **Warranty**..........41
18. **Delays in the Supplier's Performance**..........42
19. **Liquidated Damages**..........42
20. **Settlement of Disputes**..........43
21. **Liability of the Supplier**..........43
22. **Force Majeure**..........43
23. **Termination for Default**..........44
24. **Termination for Insolvency**..........44
25. **Termination for Convenience**..........45
26. **Termination for Unlawful Acts**..........45
27. **Procedures for Termination of Contracts**..........46
28. **Assignment of Rights**..........47
29. **Contract Amendment**..........47
30. **Application**..........47

1. Definitions

1.1. In this Contract, the following terms shall be interpreted as indicated:

(a) "The Contract" means the agreement entered into between the Procuring Entity and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

(b) "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations.

(c) "The Goods" means all of the supplies, equipment, machinery, spare parts, other materials and/or general support services which the Supplier is required to provide to the Procuring Entity under the Contract.

(d) "The Services" means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Supplier covered under the Contract.

(e) "GCC" means the General Conditions of Contract contained in this Section.

(f) "SCC" means the Special Conditions of Contract.

(g) "The Procuring Entity" means the organization purchasing the Goods, as named in the **SCC**.

(h) "The Procuring Entity's country" is the Philippines.

(i) "The Supplier" means the individual contractor, manufacturer distributor, or firm supplying/manufacturing the Goods and Services under this Contract and named in the **SCC**.

(j) The "Funding Source" means the organization named in the **SCC**.

(k) "The Project Site," where applicable, means the place or places named in the **SCC**.

(l) "Day" means calendar day.

(m) The "Effective Date" of the contract will be the date of receipt by the Supplier of the Notice to Proceed or the date provided in the Notice to Proceed. Performance of all obligations shall be reckoned from the Effective Date of the Contract.

(n) "Verified Report" refers to the report submitted by the Implementing Unit to the Head of the Procuring Entity setting forth its findings as to the existence of grounds or causes for termination and explicitly stating its recommendation for the issuance of a Notice to Terminate.

2. Corrupt, Fraudulent, Collusive, and Coercive Practices

2.1. Unless otherwise provided in the **<u>SCC</u>**, the Procuring Entity as well as the bidders, contractors, or suppliers shall observe the highest standard of ethics during the procurement and execution of this Contract. In pursuance of this policy, the Procuring Entity:

(a) defines, for the purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the Government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in Republic Act 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) “collusive practices” means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) “coercive practices” means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) “obstructive practice” is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

2.2. Further the Funding Source, Borrower or Procuring Entity, as appropriate, will seek to impose the maximum civil, administrative and/or criminal penalties available under the applicable law on individuals and organizations deemed to be involved with any of the practices mentioned in GCC Clause 2.1 (a).

3. Inspection and Audit by the Funding Source

The Supplier shall permit the Funding Source to inspect the Supplier's accounts and records relating to the performance of the Supplier and to have them audited by auditors appointed by the Funding Source, if so required by the Funding Source.

4. Governing Law and Language

4.1. This Contract shall be interpreted in accordance with the laws of the Republic of the Philippines.

4.2. This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract. All correspondence and other documents pertaining to this Contract exchanged by the parties shall be written in English.

5. Notices

5.1. Any notice, request, or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request, or consent shall be deemed to have been given or made when received by the concerned party, either in person or through an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the **SCC**, which shall be effective when delivered and duly received or on the notice's effective date, whichever is later.

5.2. A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to the provisions listed in the **SCC** for GCC Clause 5.1.

6. Scope of Contract

6.1. The GOODS and Related Services to be provided shall be as specified in Section VI. Schedule of Requirements.

6.2. 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. Any additional requirements for the completion of this Contract shall be provided in the **SCC**.

7. Subcontracting

7.1. Subcontracting of any portion of the Goods, if allowed in the BDS, does not relieve the Supplier of any liability or obligation under this 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.

7.2. Subcontractors disclosed and identified during the bidding may be changed during the implementation of this Contract, subject to compliance with the required qualifications and the approval of the Procuring Entity.

8. Procuring Entity's Responsibilities

8.1. Whenever the performance of the obligations in this Contract requires that the Supplier obtain permits, approvals, import, and other licenses from local public authorities, the Procuring Entity shall, if so needed by the Supplier, make its best effort to assist the Supplier in complying with such requirements in a timely and expeditious manner.

8.2. The Procuring Entity shall pay all costs involved in the performance of its responsibilities in accordance with GCC Clause 6.

9. Prices

9.1. For the given scope of work in this Contract as awarded, all bid prices are considered fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances and upon prior approval of the GPPB in accordance with Section 61 of R.A. 9184 and its IRR or except as provided in this Clause.

9.2 Prices charged by the Supplier for Goods delivered and/or services performed under this Contract shall not vary from the prices quoted by the Supplier in its bid, with the exception of any change in price resulting from a Change Order issued in accordance with **GCC** Clause 29.

10. Payment

10.1. Payments shall be made only upon a certification by the Head of the Procuring Entity to the effect that the Goods have been rendered or delivered in accordance with the terms of this Contract and have been duly inspected and accepted. Except with the prior approval of the President no payment shall be made for services not yet rendered or for supplies and materials not yet delivered under this Contract. Ten percent (10%) of the amount of each payment shall be retained by the Procuring Entity to cover the Supplier's warranty obligations under this Contract as described in GCC Clause 17.

10.2. The Supplier's request(s) for payment shall be made to the Procuring Entity in writing, accompanied by an invoice describing, as appropriate, the Goods delivered and/or Services performed, and by documents submitted pursuant to the **SCC** provision for GCC Clause 6.2, and upon fulfillment of other obligations stipulated in this Contract.

10.3. Pursuant to GCC Clause 10.2, payments shall be made promptly by the Procuring Entity, but in no case later than sixty (60) days after submission of an invoice or claim by the Supplier.

10.4. Unless otherwise specified in the **SCC**, the currency in which payment is made to the Supplier under this Contract shall be in Philippine Pesos.

11. Advance Payment and Terms of Payment

11.1. Advance payment shall be made only after prior approval of the President, and shall not exceed fifteen percent (15%) of the Contract amount, unless otherwise directed by the President or in cases allowed under Annex "D" of RA 9184.

11.2. For Goods supplied from abroad, the terms of payment shall be as follows:

(a) On Contract Signature: Fifteen percent (15%) of the Contract Price shall be paid within sixty (60) days from signing of the Contract and upon submission of a claim and a bank guarantee for the equivalent amount valid until the Goods are delivered and in the form provided in Section VIII. Bidding Forms.

(b) On Delivery: Sixty-five percent (65%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the **SCC** provision on Delivery and Documents.

(c) On Acceptance: The remaining twenty percent (20%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of submission of the acceptance and inspection certificate for the respective delivery issued by the Procuring Entity's authorized representative. In the event that no inspection or acceptance certificate is issued by the Procuring Entity's authorized representative within forty five (45) days of the date shown on the delivery receipt the Supplier shall have the right to claim payment of the remaining twenty percent (20%) subject to the Procuring Entity's own verification of the reason(s) for the failure to issue documents (vii) and (viii) as described in the **SCC** provision on Delivery and Documents.

11.3. All progress payments shall first be charged against the advance payment until the latter has been fully exhausted.

12. Taxes and Duties

The Supplier, whether local or foreign, shall be entirely responsible for all the necessary taxes, stamp duties, license fees, and other such levies imposed for the completion of this Contract.

13. Performance Security

13.1. Within ten (10) calendar days from receipt of the Notice of Award from the Procuring Entity but in no case later than the signing of the contract by both parties, the successful Bidder shall furnish the performance security in any the forms prescribed in the ITB Clause 33.2.

13.2. The performance security posted in favor of the Procuring Entity shall be forfeited in the event it is established that the winning bidder is in default in any of its obligations under the contract.

13.3. The performance security shall remain valid until issuance by the Procuring Entity of the Certificate of Final Acceptance.

13.4. The performance security may be released by the Procuring Entity and returned to the Supplier after the issuance of the Certificate of Final Acceptance subject to the following conditions:

(a) There are no pending claims against the Supplier or the surety company filed by the Procuring Entity;

(b) The Supplier has no pending claims for labor and materials filed against it; and

(c) Other terms specified in the **SCC**.

13.5. In case of a reduction of the contract value, the Procuring Entity shall allow a proportional reduction in the original performance security, provided that any such reduction is more than ten percent (10%) and that the aggregate of such reductions is not more than fifty percent (50%) of the original performance security.

14. Use of Contract Documents and Information

14.1. The Supplier shall not, except for purposes of performing the obligations in this Contract, without the Procuring Entity’s prior written consent, disclose this Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring Entity. Any such disclosure shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

14.2. Any document, other than this Contract itself, enumerated in GCC Clause 14.1 shall remain the property of the Procuring Entity and shall be returned (all copies) to the Procuring Entity on completion of the Supplier’s performance under this Contract if so required by the Procuring Entity.

15. Standards

The Goods provided under this Contract shall conform to the standards mentioned in the Section VII. Technical Specifications; and, when no applicable standard is mentioned, to the authoritative standards appropriate to the Goods' country of origin. Such standards shall be the latest issued by the institution concerned.

16. Inspection and Tests

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

16.2. If applicable, the inspections and tests may be conducted on the premises of the Supplier or its subcontractor(s), at point of delivery, and/or at the goods' final destination. If conducted on the premises of the Supplier or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring Entity.

16.3. The Procuring Entity or its designated representative shall be entitled to attend the tests and/or inspections referred to in this Clause provided that the Procuring Entity shall bear all of its own costs and expenses incurred in connection with such attendance including, but not limited to, all traveling and board and lodging expenses.

16.4. The Procuring Entity may reject any Goods or any part thereof that fail to pass any test and/or inspection or do not conform to the specifications. The Supplier shall either rectify or replace such rejected Goods or parts thereof or make alterations necessary to meet the specifications at no cost to the Procuring Entity, and shall repeat the test and/or inspection, at no cost to the Procuring Entity, upon giving a notice pursuant to GCC Clause 5.

16.5. The Supplier agrees that neither the execution of a test and/or inspection of the Goods or any part thereof, nor the attendance by the Procuring Entity or its representative, shall release the Supplier from any warranties or other obligations under this Contract.

17. Warranty

17.1. The Supplier warrants that the Goods supplied under the Contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the Procuring Entity provides otherwise.

17.2. The Supplier further warrants that all Goods supplied under this Contract shall have no defect, arising from design, materials, or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Goods in the conditions prevailing in the country of final destination.

17.3. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier for a minimum period specified in the **SCC**. The obligation for the warranty shall be covered by, at the Supplier's option, either retention money in an amount equivalent to at least ten percent (10%) of every progress payment, or a special bank guarantee equivalent to at least ten percent (10%) of the Contract Price or other such amount if so specified in the **SCC**. The said amounts shall only be released after the lapse of the warranty period specified in the **SCC;** provided, however, that the Supplies delivered are free from patent and latent defects and all the conditions imposed under this Contract have been fully met.

17.4. 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, within the period specified in the **SCC** and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the Procuring Entity.

17.5. If the Supplier, having been notified, fails to remedy the defect(s) within the period specified in GCC Clause 17.4, the Procuring Entity may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Procuring Entity may have against the Supplier under the Contract and under the applicable law.

18. Delays in the Supplier's Performance

18.1. Delivery of the Goods and/or performance of Services shall be made by the Supplier in accordance with the time schedule prescribed by the Procuring Entity in Section VI. Schedule of Requirements.

18.2. If at any time during the performance of this Contract, the Supplier or its Subcontractor(s) should encounter conditions impeding timely delivery of the Goods and/or performance of Services, the Supplier shall promptly notify the Procuring Entity in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, and upon causes provided for under GCC Clause 22, the Procuring Entity shall evaluate the situation and may extend the Supplier's time for performance, in which case the extension shall be ratified by the parties by amendment of Contract.

18.3. Except as provided under GCC Clause 22, a delay by the Supplier in the performance of its obligations shall render the Supplier liable to the imposition of liquidated damages pursuant to GCC Clause 19, unless an extension of time is agreed upon pursuant to GCC Clause 29 without the application of liquidated damages.

19. Liquidated Damages

Subject to **GCC** Clauses 18 and 22, if the Supplier fails to satisfactorily deliver any or all of the Goods and/or to perform the Services within the period(s) specified in this Contract inclusive of duly granted time extensions if any, the Procuring Entity shall, without prejudice to its other remedies under this Contract and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance. The maximum deduction shall be ten percent (10%) of the amount of contract. Once the maximum is reached, the Procuring Entity shall rescind the Contract pursuant to **GCC** Clause 23, without prejudice to other courses of action and remedies open to it.

20. Settlement of Disputes

20.1. If any dispute or difference of any kind whatsoever shall arise between the Procuring Entity and the Supplier in connection with or arising out of this Contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

20.2. If after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the Procuring Entity or the Supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

20.3. Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this Clause shall be settled by arbitration. Arbitration may be commenced prior to or after delivery of the Goods under this Contract.

20.4. In the case of a dispute between the Procuring Entity and the Supplier, the dispute shall be resolved in accordance with Republic Act 9285 ("R.A. 9285"), otherwise known as the "Alternative Dispute Resolution Act of 2004."

20.5. Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree; and the Procuring Entity shall pay the Supplier any monies due the Supplier.

21. Liability of the Supplier

21.1. The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines, subject to additional provisions, if any, set forth in the **SCC**.

21.2. Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent rights, if applicable, the aggregate liability of the Supplier to the Procuring Entity shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

22. Force Majeure

22.1. The Supplier shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the Contract is the result of a *force majeure.*

22.2. For purposes of this Contract the terms "*force majeure*" and "fortuitous event" may be used interchangeably. In this regard, a fortuitous event or *force majeure* shall be interpreted to mean an event which the Contractor could not have foreseen, or which though foreseen, was inevitable. It shall not include ordinary unfavorable weather conditions; and any other cause the effects of which could have been avoided with the exercise of reasonable diligence by the Contractor. Such events may include, but not limited to, acts of the Procuring Entity in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

22.3. If a *force majeure* situation arises, the Supplier shall promptly notify the Procuring Entity in writing of such condition and the cause thereof. Unless otherwise directed by the Procuring Entity in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the *force majeure*.

23. Termination for Default

23.1. The Procuring Entity shall terminate this Contract for default when any of the following conditions attends its implementation:

(a) Outside of *force majeure*, the Supplier fails to deliver or perform any or all of the Goods within the period(s) specified in the contract, or within any extension thereof granted by the Procuring Entity pursuant to a request made by the Supplier prior to the delay, and such failure amounts to at least ten percent (10%) of the contact price;

(b) As a result of *force majeure*, the Supplier is unable to deliver or perform any or all of the Goods, amounting to at least ten percent (10%) of the contract price, for a period of not less than sixty (60) calendar days after receipt of the notice from the Procuring Entity stating that the circumstance of force majeure is deemed to have ceased; or

(c) The Supplier fails to perform any other obligation under the Contract.

23.2. In the event the Procuring Entity terminates this Contract in whole or in part, for any of the reasons provided under **GCC** Clauses 23 to 26, the Procuring Entity may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Procuring Entity for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of this Contract to the extent not terminated.

23.3. In case the delay in the delivery of the Goods and/or performance of the Services exceeds a time duration equivalent to ten percent (10%) of the specified contract time plus any time extension duly granted to the Supplier, the Procuring Entity may terminate this Contract, forfeit the Supplier's performance security and award the same to a qualified Supplier.

24. Termination for Insolvency

The Procuring Entity shall terminate this Contract if the Supplier is declared bankrupt or insolvent as determined with finality by a court of competent jurisdiction. In this event, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Entity and/or the Supplier.

25. Termination for Convenience

25.1. The Procuring Entity may terminate this Contract, in whole or in part, at any time for its convenience. The Head of the Procuring Entity may terminate a contract for the convenience of the Government if he has determined the existence of conditions that make Project Implementation economically, financially or technically impractical and/or unnecessary, such as, but not limited to, fortuitous event(s) or changes in law and national government policies.

25.2. The Goods that have been delivered and/or performed or are ready for delivery or performance within thirty (30) calendar days after the Supplier's receipt of Notice to Terminate shall be accepted by the Procuring Entity at the contract terms and prices. For Goods not yet performed and/or ready for delivery, the Procuring Entity may elect:

(a) to have any portion delivered and/or performed and paid at the contract terms and prices; and/or

(b) to cancel the remainder and pay to the Supplier an agreed amount for partially completed and/or performed goods and for materials and parts previously procured by the Supplier.

25.3. If the Supplier suffers loss in its initial performance of the terminated contract, such as purchase of raw materials for goods specially manufactured for the Procuring Entity which cannot be sold in open market, it shall be allowed to recover partially from this Contract, on a *quantum meruit* basis. Before recovery may be made, the fact of loss must be established under oath by the Supplier to the satisfaction of the Procuring Entity before recovery may be made.

26. Termination for Unlawful Acts

26.1. The Procuring Entity may terminate this Contract in case it is determined *prima facie* that the Supplier has engaged, before or during the implementation of this Contract, in unlawful deeds and behaviors relative to contract acquisition and implementation. Unlawful acts include, but are not limited to, the following:

(a) Corrupt, fraudulent, and coercive practices as defined in ITB Clause 3.1(a);

(b) Drawing up or using forged documents;

(c) Using adulterated materials, means or methods, or engaging in production contrary to rules of science or the trade; and

(d) Any other act analogous to the foregoing.

27. Procedures for Termination of Contracts

27.1. The following provisions shall govern the procedures for termination of this Contract:

(a) Upon receipt of a written report of acts or causes which may constitute ground(s) for termination as aforementioned, or upon its own initiative, the Implementing Unit shall, within a period of seven (7) calendar days, verify the existence of such ground(s) and cause the execution of a Verified Report, with all relevant evidence attached;

(b) Upon recommendation by the Implementing Unit, the Head of the Procuring Entity shall terminate this Contract only by a written notice to the Supplier conveying the termination of this Contract. The notice shall state:

(i) that this Contract is being terminated for any of the ground(s) aforementioned, and a statement of the acts that constitute the ground(s) constituting the same;

(ii) the extent of termination, whether in whole or in part;

(iii) an instruction to the Supplier to show cause as to why this Contract should not be terminated; and

(iv) special instructions of the Procuring Entity, if any.

(c) The Notice to Terminate shall be accompanied by a copy of the Verified Report;

(d) Within a period of seven (7) calendar days from receipt of the Notice of Termination, the Supplier shall submit to the Head of the Procuring Entity a verified position paper stating why this Contract should not be terminated. If the Supplier fails to show cause after the lapse of the seven (7) day period, either by inaction or by default, the Head of the Procuring Entity shall issue an order terminating this Contract;

(e) The Procuring Entity may, at any time before receipt of the Supplier's verified position paper described in item (d) above withdraw the Notice to Terminate if it is determined that certain items or works subject of the notice had been completed, delivered, or performed before the Supplier's receipt of the notice;

(f) Within a non-extendible period of ten (10) calendar days from receipt of the verified position paper, the Head of the Procuring Entity shall decide whether or not to terminate this Contract. It shall serve a written notice to the Supplier of its decision and, unless otherwise provided, this Contract is deemed terminated from receipt of the Supplier of the notice of decision. The termination shall only be based on the ground(s) stated in the Notice to Terminate;

(g) The Head of the Procuring Entity may create a Contract Termination Review Committee (CTRC) to assist him in the discharge of this function. All decisions recommended by the CTRC shall be subject to the approval of the Head of the Procuring Entity; and

(h) The Supplier must serve a written notice to the Procuring Entity of its intention to terminate the contract at least thirty (30) calendar days before its intended termination. The Contract is deemed terminated if it is not resumed in thirty (30) calendar days after the receipt of such notice by the Procuring Entity.

28. Assignment of Rights

The Supplier shall not assign his rights or obligations under this Contract, in whole or in part, except with the Procuring Entity’s prior written consent.

29. Contract Amendment

Subject to applicable laws, no variation in or modification of the terms of this Contract shall be made except by written amendment signed by the parties.

30. Application

These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of this Contract.

Section V. Special Conditions of Contract

GCC Clause	
1.1 (g)	The Procuring Entity is the **Bureau of Customs (BOC).**
1.1 (i)	The Supplier is:
1.1 (j)	The Funding Source is: The Government of the Philippines (GOP) through the authorized appropriations under the FY 2015 General Appropriations Act**.**
1.1 (k)	Project Site: Stated in the Section VI. Schedule of Requirements
5.1	The Procuring Entity's address for Notices is: Bureau of Customs Customs ICT Center, South Harbor, Gate 3, Port Area, Manila Tel Nos. (02) 705-6053/6083 Contact Person: DEP. COMM. DENNIS B. REYES The Supplier's address for Notices is:
6.2	The Goods/services shall only be delivered by the Supplier as indicated in Sec. VI. Schedule of Requirements. Moreover, the delivery schedule as indicated in Section VI. Schedule of Requirements may be modified at the option of the Procuring Entity, with prior due notice, written or verbal, to the Supplier.
8.	**Other specific responsibilities of the procuring entity:** a. Upon request, Customer must provide information to Service Provider, its subcontractors or its designated point of contact that is reasonably necessary or useful for Service Provider to perform its obligations. In addition, upon request Customer will provide Service Provider or its Designees with access to Customer facilities, installation sites, and equipment as reasonably necessary or useful for Service Provider to perform its obligations hereunder. b. Customer must obtain any necessary permits, licenses, variances, and/or other authorizations required by state and local jurisdictions for installation and operation of the CPE on Customer's premises or where the jurisdiction requires Customer to obtain the permit, license, variance and/or authorization. c. Customer must provide adequate building space, circuitry, facility wiring,

	temperature, humidity, and power to comply with the standards established by the manufacturer of the CPE for proper installation and operation of Managed WAN Service. d. Out of band access is required for Managed WAN Full, Managed WAN Physical and Third Party Transport service. Customer must provide and install at their cost either a dedicated, analog telephone connection or indirect cable access (such as terminal server) for use by each OOB modem for troubleshooting each circuit that is part Managed WAN Full, Managed WAN Physical, or Third Party Transport service. The analog telephone connection must maintain a minimum 9600 bits per second connection rate for site level SLAs to apply. e. Upon Service Provider's reasonable request, Customer will assist in troubleshooting Managed Devices, including reboot, reading LED light statuses where applicable, verification of equipment power, verification of cable connections, and insertion of a loopback plug. f. Customer shall notify Service Provider via a Change Management Request of any maintenance that may affect the operating status of the Managed Devices. **Duties and Responsibilities of the Customer** a. Grant the ISP's authorized representative access to its premises, equipment and facilities located therein to perform its obligations, provided that such representative shall be accompanied by the duly assigned BOC personnel; b. Responsible for the safe custody and use of the equipment installed by the ISP provider; c. Monitor the provided services and verify if the parameters under the Service Level Agreement are met and performed by the ISP provider; d. Issue Certificate of Inspection and Acceptance as stipulated in Section VII Subsection II, Item 4; e. At the end of each year, BOC will conduct an assessment of the quality of service provided particularly the cost charged by the ISP provider and the range of services it offers against other Service Providers in the area; and f. Conducts assessment/evaluation of the ISP 60 days before the end of the contract.
10.2	Payment shall be made within fifteen (15) calendar days after the submission of Billing Statement, Certificate of Acceptance and Completion by the end-user and Delivery Receipts.
10.4	No further instructions.
11	Payment shall be made on the following schedule: a. One-time payment of service charge, if any, shall be made after full/complete delivery, installation, configuration, and activation of Internet services within

	the prescribed period and upon issuance of the Certificate of Inspection and Acceptance by the BOC. b. Succeeding payment shall be made on a monthly basis for 24 months subject to submission of billing statement and other supporting documents by the Service Provider and subject to the issuance of certificate of satisfactory service by BOC.
13.4	No further instructions.
16.1	Not applicable.
17.3	Not applicable.
17.4	Not applicable.

Section VI. Schedule of Requirements

Item	General Description	Quantity	Delivery, Weeks/Months
1	Delivery, installation and commissioning of all hardware, software and other equipment for all sites	1 lot	Within 90 days from receipt of Notice to Proceed
2	Implementation of the network and internet services	N.A.	Monthly, to start after delivery and acceptance of Item 1 above

Note: ***All goods/services should be delivered/installed/implemented at the Bureau of Customs, Port Area, Manila, and to specified ports/subports all over the country.***

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

________________________ ____________________________ ____________

Name of Company/Bidder **Signature Over Printed Name of Representative** **Date**

Section VII. Technical Specifications

Bidders must state here either “Comply” or “Not Comply” against each of the individual parameters of each Specification stating the corresponding performance parameter of the goods/services offered. Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause (ii) and/or **GCC** Clause 0.

I. MANAGED SECURE WIDE AREA NETWORK SERVICE

	TECHNICAL AND REQUIREMENTS SPECIFICATION	**Statement of Compliance**
1	**General requirements**	
	The Service Provider shall manage and provide maintenance for the existing BOC Internet Protocol-Virtual Private Network (IPVPN) Infrastructure which shall be the single point of contact for all the network links. The service shall include upgrade of existing bandwidth of all BOC sites within the IPVPN (see coverage and bandwidth) and supply and delivery of new equipment.	
	The Service Provider shall render all the required and necessary services in accordance with accepted standards, conventions and practices; and, in compliance with applicable laws, rules and regulations governing the installation, operation and maintenance of a IPVPN infrastructure.	
	Within two (2) months from the receipt of the Notice to Proceed, the Service Provider shall complete the necessary maintenance on all BOC sites including the connectivity and CPE deployed on each sites of the agency's existing IPVPN.	
	For a period of twelve (24) months from Start of the Services, the Service Provider shall operate, maintain and manage the IPVPN connectivity among the Major Ports and Sub Port Offices.	
	Within a 12-month service period, the Service Provider shall provide a 24/7 Technical Support Services. All Service Requests shall be immediately acted upon when received. The Service Provider shall perform due diligence until the matter is resolved to the satisfaction of the Bureau. In the event that service is not resolved within 4 hours, the Service Provider shall provide additional resources to correct the issue. The Service Provider shall also elevate the issue internally within the company if not resolved within 4 hours. The Service Provider shall provide status of issue resolution every 4 hours until the matter is resolved. In the event that service is not restored within 24 hours, except for interruptions due to Force Majeure, the Service Provider shall provide an additional credit of 1 day (in addition to the normal service credit provided by the contract) for each 24 hours period that service is interrupted. For interruptions due to Force Majeure, the Service Provider shall restore service at the earliest possible time.	

	The Service Provider shall be responsible for the supply, delivery, installation, configuration and maintenance of connectivity and the needed equipment / active components for the said IPVPN connection for all sites nationwide. The Service Provider shall provide any and all equipment, parts or supplies necessary to accomplish this IPVPN Infrastructure from the BOC existing/ new network including but not limited to modems, routers, switches, firewall, etc.	
	The Service Provider shall provide managed network administration services including but not limited to the following: status monitoring, additional VLAN activation, editing of routes, IP address allocation, traffic report generation, basic troubleshooting, stopping/starting/restarting of network equipment and password resetting.	
	The Service Provider shall provide a datacenter facility that has a team of at least Ten (10) certified network professionals for the proposed solution for 24x7 operation to monitor, troubleshoot and maintain the network.	
	To make sure that all sites will have the maximum uptime, it is required that all of it be terminated in a carrier neutral, resilient and robust datacenter that is available and operates 24x7 and complies to ISO 9001 - Quality Management System, ISO 27001 -Information Security Management, ISO 20000-1 for Service Management for IT, ISO 14001 – Environmental Management System, ISO 22301 - Business Continuity.	
	The Service Provider is required to bid on all services and for all sites for this is a one-lot bid.	
	All services shall be provided 24 hours a day, 7 days a week, and 365 days a year continuously.	
	The Service Provider shall complete the 1st BER of any of the existing BOC sites within 120 days from the date that the Notice to Proceed was received for all sites. If this is not meet, the BOC will not issue an Acceptance Certificate to be used for billing purposes unless corrected. This will be applied to all sites until all sites are completed.	
	All services shall be bid and paid in Philippine Pesos, at a fixed monthly rate, inclusive of all taxes and any other fees or charges. Rates are not subject to fluctuations in foreign currency valuations.	
	The Service Provider shall provide credits in the next monthly billing for all downtimes of the service, or if the service drops below specified bandwidths. This will be subject for SLA (Service Level Agreement)	
	The Service Provider shall provide a team of at least Ten (10) certified network professionals and at least Forty (60) MEF-CECP (MEF – Carrier Ethernet Certified Professional) for the proposed solution for 24x7 operation to monitor, troubleshoot and maintain the network.	
	All sites shall have the ability to communicate with any and all other sites directly for both voice and data. The Service Provider is responsible for ensuring the proper routing for all communications to the proper site.	
2	**MONITORING SERVICES**	
	2.1 Monitoring Service Provider delivers proactive monitoring of all Customer-designated Managed Devices 24 hours a day, seven days a week. Service Provider will monitor Customer’s Managed Devices via use of the simple network management protocol (SNMP) and internet control message protocol (ICMP, commonly called a “ping”) for status and error conditions.	
	2.2 Notification.	

	Service Provider delivers fault notification for Customer's Managed Devices. Service Provider Network Operation Center (NOC) will create a trouble ticket and notify Customer's designated point of contact immediately. Service Provider will notify the Customer's designated point of contact via e-mail or automated phone message at Service Provider option. Upon the creation of a trouble ticket, the NOC will begin troubleshooting the circuit until the problem has been verified as fixed and the ticket will then be closed. Once the non- Service Provider issue has been resolved by Customer, the ticket will be closed by Service Provider.	
	2.3 Monitoring Management. The NOC provides physical fault detection, isolation and monitoring services for Managed Devices. The NOC provides coverage 24 hours per day, seven days per week. Physical faults will be resolved by Service Provider whether due to Service Provider, Customer or third party issues. Managed Device Logical faults are Customer's responsibility. Customer will inform Service Provider of physical faults once it has completed its logical troubleshooting if Service Provider is maintenance provider for Customer's CPE. Service Provider is responsible to resolve both logical and physical issues with Customer's cooperation whether due to Service Provider, Customer or third party issues. Service Provider may resolve the fault condition remotely or by dispatching a technician to Customer's site, at Service Provider's option. Management of Managed Devices includes management of applicable software licenses that may be configured on Managed Devices.	
	2.4 Threshold Proactive Performance Monitoring (PPM). Threshold PPM provides analysis of Managed WAN performance against Service Provider-predefined thresholds for standard performance. Performance-related threshold alerts from the Customer Network result in automatic trouble ticket generation to the NOC. No additional graphical reports are provided.	
	2.5 Third Party Transport Service. Service Provider monitors and manages Customer's 3rd Party Transport circuit from its NOC and informs Customer of the existence of any outages or problems with the 3rd Party Transport circuit. 3rd Party Transport is available to Customers with at least two managed sites on the Service Provider network.	
3	**REPORTING**	
	3.1 WAN Analysis Standard Reporting. Service Provider delivers an online dashboard that will enable BOC IT Management team to generate and view reports on their own anytime and anywhere. Available report type should have option to identify pocket types that passes through the network.	
	All report logs should be protected from all forms of alteration and deletion as stated on Republic Act 9470.	
	3.2 Monthly Report. The Customer will receive one report per month that contains performance-affecting incidents within the Customer Network, identified by Customer's selected reporting application. Volume statistics for the Customer's Network may also be included upon request. The incidences may be for a single technology or multiple technologies such as, but not limited to, the	

	Managed Device and its physical and virtual interfaces. The monthly report is prepared and delivered as follows: • The monthly report is reviewed internally with the Service Provider account team and applicable Service Provider operation and engineering personnel prior to delivery. • Service Provider issues with the Customer Network that are identified are referred to the appropriate Service Provider organization for resolution. • The account team delivers the report to the Customer and will schedule a conference with the Customer to present and review the performance reporting.	
	3.3 Monthly Performance Report Customization. Customer may request that the report be customized as provided in this section. Other requests for report customization will be considered on a case-by-case basis and must be approved by Service.	
	3.4 Quarterly Review. Service Provider will review the previous quarter reporting with the Customer via conference call. Customer may request face to face quarterly review meetings however such meetings will be at the Service Provider's discretion and at the Customer's expense.	
4	**IMPLEMENTATION**	
	4.1 Managed Implementation. Service Provider delivers a support for the planning, system engineering and overall project management of a new network including without limitation: • collection of system, application and end-user requirements • Review of the current network topology and create and implement design changes to improve reliability and security. • creation of the overall project plan including system design and equipment configuration • installation of a separate wall mounted cabinet for each of every site which will isolate managed appliance from other network appliance on the site • implementation of the overall project plan; and • network site installation and acceptance Service Provider will provide Managed Implementation on a *per-project basis* in accordance with a separate requirement that contains appropriate terms and conditions agreed to by Customer and Service Provider.	
5	**MIGRATION**	
	5.1 Basic Managed Migration. Service Provider to assess the Customer's current network and CPE, including, but not limited to: network topology, protocols, network performance history, site related information and Customer network management gap analysis.	
	Implementation Engineering Activities. During the implementation of the new migrated service, Service Provider will perform the following services:	

	□ install Out of Band (OOB) modem and confirm OOB connectivity;
	□ schedule and complete physical and logical installations;
	□ establish and verify management connectivity for Private service;
	□ verify Simple Network Management Protocol (SNMP), and connectivity;
	□ configure Customer Private IP devices;
	□ verify the elements of Private IP service are operational.	

	5.2 Complex Managed Migration. In addition to the services provided under the basic Managed Migration, Service Provider will perform the following design and implementation service:	
	Private IP Service Implementation and Activation. Service Provider will implement and activate the network based on the requirements. Service Provider will complete the physical and logical activation of the Managed Devices. Prior to activation of Customer's network service, the Service Provider will: □ coordinate site surveys, if determined to be necessary by Service Provider; □ coordinate the activation of circuits and remote configuration of CPE; □ test access circuits/DSU/CSU; □ enable data ports; and, □ ping Customer Managed Device at time of activation.	
6	**NETWORK ANALYSIS**	
	6.1 NA Service Provisioning. Service Provider will deliver the Network Analysis service for the Customer's Network.	
	Service Provider will provide performance analysis for the previous month of usage/network performance for presentation to the Customer each month.	
	Service Provider will provide written and verbal report of an analysis of the Customer's Network via conference call each month for the previous month that is based, in part on the performance reports and includes performance, utilization, and analysis of errors occurring in the Managed WAN.	
	Service Provider will provide quarterly Customer Network performance reviews and conduct a conference call to discuss the review.	
	6.2 NA Setup Schedule. The typical implementation schedule for NA is: Stage 1 □ Service Provider will allocate staff to provide NA for Customer. □ Requirements briefings are held with Customer and the Service Provider account team for Customer. □ Service Provider and the Customer will meet to identify monthly deliverable data and expectations □ Service Provider will conduct internal Service Provider briefings with operations engineering organizations to determine what performance	

	issues may be known about the Customer Network in order to make recommendations to the Customer. Stage 2 □ If Customer requires, alias naming of the database elements is completed for reporting. □ If Customer requires, implementation of grouping the database elements is completed for reporting. □ Periodic monitoring of the data is provided. Stage 3 □ Service Provider produces initial monthly network analysis report. Stage 4 □ Service Provider will continue to produce monthly reports.	
7	**NETWORK ENGINEERING SERVICE**	
	7.1 <u>NE Service Provisioning</u>. Service Provider will render a consumable consultancy equivalent to 250 man-hours per year. Upon Customer's order, Service Provider will provide ongoing Network Engineering activities described below for the Customer's Network. NE is provided by shared NE resources that provide ongoing planning and engineering activities to the Customer Network. Service Provider will execute follow-up recommendations, at Customer's request related to key areas of Customer Network operation. NE is only available during Business Days. Physical Customer Network changes requested by Customer and performed by Service Provider will result in related charges to Customer. NE charges only cover the required engineering services defined below. Service Provider reserves the right to charge, at Service Provider's then current labor rate.	
	7.2 <u>Design Optimization and Capacity Planning</u> □ Service Provider reviews the Customer Network reports based on Customer's selected reporting application. Based on this review, Service Provider will review with the Customer certain information, for example i) the performance of the Network, ii) recommended scalability options, iii) logical addressing, iv) redundancy, and v) logical and physical capacity of the Customer Network. □ Service Provider will review performance reports provided as part of Customer's Managed WAN and make design or configuration recommendations that may be performed by Service Provider. □ Service Provider will provide engineering support for proof of concept prototyping and testing of Customer Network designs and capacity plans.	
	7.3 <u>Strategic Planning and Design</u> □ Service Provider will be a technical advisor to Customer for the Customer's Network and Customer will request any changes to the Customer Network via the optional change management process. □ Upon Customer's request, Service Provider will assess the current	

	Managed Devices and evaluate the benefit and compatibility of new software or hardware releases consistent with Customer's current architecture. □ Service Provider will plan and recommend end-of-life remediation for Managed Devices. □ As part of Change Management activities, Service Provider will review Customer Network design architecture against the Customer's on-going network requirements. □ Service Provider will evaluate new technology changes and recommend technology upgrades for Managed Devices. Recommendations and evaluations are limited to features and services the Customer requires. Any additional or changed hardware or software recommended are at an additional cost. □ Service Provider will conduct an annual formal technology assessment on the Managed Devices that are part of the NE supported architecture and will provide an overview of the findings to the Customer via a conference call. Customer may request a face to face annual formal technology assessment.	
	7.4 Design Services. Service Provider will provide a consultant who will create a Customer design document based on a written statement of requirements agreed to by Customer.	
	7.5 Enhanced Cyber Security integration • Service Provider will collaborate with Cyber Security Service Providers and integrate any network security device and implementation in the managed network. • Service Providers SLA and deliverables will not be affected by such activity.	
8	**SUPPORT SERVICE**	
	8.1 Support Services.	
	Service Provider will work on issues for Managed Devices related to operating system vulnerability checks, including operating system upgrades to eliminate known vulnerabilities.	
	Service Provider will provide engineering and technical support for the Managed Devices for problem resolution of design related issues identified by Service Provider engineers or Managed Device vendor's technical support.	
9	**CHANGE MANAGEMENT**	
	9.1 Network Change Management Support □ Service Provider will attend Customer Change Management technical meetings as scheduled. □ Service Provider will design and implement changes on Managed Devices based on Customer request and requirements and recommends design changes to correct a Customer Network fault or problem. □ Service Provider will work with Customer to define requirements, design, document, and work with Service Provider operations to implement changes on Managed Devices only. Service Provider operations perform the Change Management activities and NE	

	performs billable OCM and design-impacting Managed Device changes.	
10	**DOCUMENTATION**	
	10.1 Network Documentation Maintenance. Service Provider will update the data network as-built documentation and CDD consistent with major in-scope adds/moves/changes to the Customer Network	

II. DIRECT INTERNET SERVICE

	TECHNICAL AND REQUIREMENTS SPECIFICATION	Statement of Compliance
1	**I. Scope of Work** The project also covers acquisition and implementation to enhance the internet connection of the BOC. It involves the following: a. Engagement of primary ISP from BOC Data Center to the provider's central office; b. Subscription of the Internet Connection will be 2 years upon issuance of Acceptance Notice; c. Integration of the proposed Internet connections to the existing BOC network infrastructure. The winning ISP bidder/s shall provide the necessary hardware, terminations and other services required to setup the internet connection. Details of the technical requirements are indicated in Section VII; d. Provision of diagnostic reports and updates in case of connection failure; e. Provision of monthly utilization graphs and/or MRTG tool for monitoring of link quality and bandwidth utilization; f. Delivery of an IPv6 ready and/or compliant connection; g. Provision of 24x7 support services; and h. Entering into a Service Level Agreement which defines parameters of rebates for nonperformance, etc.	
2	**Technical Requirements** a. Bidders must submit detailed work plan specifying installation design, detailed activities, connectivity diagram from end user premise up to the last mile and timelines in order to determine compatibility with the existing Local Area Network configuration and the BOC building's electrical power rating. Bidders are required to conduct site inspection. b. The technical requirements and evaluation parameters are as follows:	
	1. Setup a Dedicated Direct Internet Connection at BOC. Provide connection from entrance facility to BOC's MDF.	
	2. Provide and Configure router for the direct Internet connection.	

	3. Provide and install a Channel Service Unit/Data Service Unit (CSU/ DSU) modem at both ends of the Internet connections.	
	4. Assign **17** Public Internet Protocol (IP) Addresses to BOC.	
	5. Provide reliable Forwarding and Secondary DNS.	
	6. 99.95% Availability and Quality of Connection.	
	7. Latency (Delay) • Not more than 10 milliseconds average trip from BOC to ISP port • Not more than 100 milliseconds average trip from ISP port to International Port	
	8. Provide single point of contact for customer support in both areas of network connectivity and Internet access.	
	9. Submit Access/usage/downtime reports and online MRTG monitoring.	
	10. Provide proactive notice of scheduled downtimes or service interruption not less than 7 days.	
	11. Render customer service support, escalation procedures and compensation for service interruption or downtime 24 hours x 7 days.	
	12. Provide “Performance Credit” or rebate in the Service Level Agreement (SLA).	
3	**Network Backbone Requirements**	
	13. The bidder should have easy access and connectivity to Local Internet Exchange for local routing and connectivity to Asia Pacific for regional traffic, offers faster connection to local/regional contents, flexibility and bandwidth Efficiency that also translates to cost efficiency.	
	14. Must have connectivity to Asia Pacific countries namely: Japan, Taiwan, Singapore, Hongkong, India, Malaysia, Indonesia, Thailand and Korea which enables to regionalize internet traffic within Asia pacific region	
	15. Must have a direct peering and presence at PH OpenIX for manage connectivity and total control of internet traffic going to US Speeds ranging from 64Kbps to 100Mbps or higher	
	16. Must provide single-end-ordering (one-stop shop) to eliminate the need to talk to several providers i.e., leased line provider, Internet Service Provider in the US, IPL provider both local and International, Internet-related requirements like IP addresses, domain names, etc. Usage statistics and utilization reports	
	17. Must have classes of service to provide options (ranging from E1 up to GigE) that fits to the immediate need and budget and the flexibility to grow bandwidth in the future as required.	

	18. Must have at least five international gateways and a high-end platform of multiprotocol routers which combines proven software technology with exceptional reliability, availability, serviceability, and performance features to meet the requirements of today's most mission-critical internetworks, 24 x 7 customer support, escalation procedures and compensation for service interruption or downtime. The Service Provider must provide a **certification that they are connected or subscribed to Tier 1 or Tier 2 networks or ISPs**. Requires at least 2 POPs in US and 3 POPs in Asia Pacific Region.	
4	**Duties and Responsibilities of the Internet Service Provider (ISP)**	
	1. Pre-Installation Provide detailed work plan specifying installation design, detailed activities, network diagram showing connectivity from end user's datacenter up to the last mile and timelines.	
	2. Actual Installation a. Set up Internet Connection with the Committed Information Rate (CIR) connection bandwidth for both upstream and downstream network traffic flows at the BOC; b. Provide and install a Channel Service Unit/Data Service Unit (CSU/DSU) modem at both ends of the Internet connections. c. Configure a Router at both ends of the Internet connections. d. Provide internet connectivity directly to end user's server room, including materials needed for the purpose. This includes provision for the installation of cables/insulation using industry standard and materials.	
	3. Configuration a. Configure CSU/DSU modem for dedicated direct internet speed connection; b. Configure router to the equivalent direct Internet connection speed; c. Configure backup router, if any. d. Assign **17** Public Internet Protocol Addresses to BOC; e. Provide DNS reverse lookup for entries with the assigned classless network; and, f. Provide reliable Forwarding and Secondary DNS.	
	4. Testing Period a. The selected ISP shall notify the BOC in writing seven (7) days prior to the required inspection/testing of the internet service connection. b. The acceptance test procedure shall be in accordance with the following: i. The acceptance testing will be undertaken for a period of seven (7) days. ii. Direct Internet will have no service interruption during the agreed test period. iii. The guaranteed Internet bandwidth of 8 Mbps direct internet with 8 Mbps Committed Information Rate (CIR) is attained during working hours (i.e., 7:00 a.m. to 7:00 p.m.). iv. Average latency should not exceed more than 10 milliseconds	

average round trip from BOC to ISP port and not more than 100milliseconds average round trip from ISP port to US/International port.

v. MRTG should be in place.

vi. Assignment of **17** Public IP Addresses.

vii. The provider must conduct a Bit Error Rate (BER) test during the testing period to eliminate cyclic redundancy check (CRC) errors.

If any of the foregoing conditions are not met, the count of the testing period shall be restarted until all of these conditions have been duly satisfied continuously for 7 working days.

Start of the Contractor’s billing shall be based on the date of issuance of “Certificate of Acceptance”.

During the testing period, the Contractor shall not be held liable for performance degradation/interruptions that are beyond its control such as power outages, fluctuations or failure or malfunction of BOC own equipment, and international/ regional internet backbone problems.

c. BOC (through a BOC Acceptance Committee) shall issue immediately the Certificate of Inspection and Acceptance to the Provider upon successful completion of the testing certifying that the Service Provider conforms to pertinent requirement in Section VII.

5. Implementation

a. Providers shall maintain all equipment in proper working order.

b. Providers shall provide an escalation list and procedure in reporting fault and outages.

c. Providers must immediately advice BOC any downtime occurrence or if any case the internet is rerouted to a backup link.

d. Providers must have standby equipment to replace immediately the existing equipment once found defective.

6. Rebates

a. Provide industry standard Service Level Agreement (SLA) which shall carry a corresponding “Performance Credit” or rebate in favor of BOC should any of the committed parameters mentioned below is not met.

b. The selected ISP provider/s should be able to render the following services:

g. Availability

If Last Mile is:	Metrics
Copper or Fiber	99.8%
Radio	99.6% (applicable only to circuits in CBD areas)

ii. Latency

Provide not more than 10 milliseconds average round trip latency from BOC to local ISP port; and Provide not more than 100 milliseconds average round trip latency from local ISP port to US/International port.

c. Render 24 hours x 7 days customer service support.

Support response time 30 minutes for emergency tickets for the following categories:

- Link connection is down
- Packet loss, variation in latency
- Routing issue

Two (2) hours response time for technical problem that requires on-site services. For problem reported after 7:00 PM, services shall be rendered 8:00 in the morning of the following business day.

Rebate Schedule for Downtime Connection Interruption/Outage:

If the interruption is attributable to the ISP, as acknowledged by the ISP's Fault Management Center, the ISP shall voluntarily make the appropriate "Performance Credit" or rebate to the BOC without the need to report or claim on the outage. The credit allowance/rebate shall be applied to the next billing month.

Credit for Interruptions to service will be allowed as follows:

Interruptions of 24 Hours or less

Length of Interruption	Rebate Factor
Less than 30 minutes	None
30 - 179 minutes	1 / 10 day
180 - 359 minutes	1 / 5 day
360 - 539 minutes	2 / 5 day
540 - 719 minutes	3 / 5 day
720 - 899 minutes	4 / 5 day
900 - 1440 minutes	One day

For interruption over 24 hours, credit will be allowed in 3/5 day multiples for each 3-hour period of interruption or fraction thereof over 24 hours.

All incidences of interruptions should be included in the monthly reporting.

7. Maintenance

a. Provide a single point of contact for customer support in both areas of network connectivity and Internet access;

b. Shall respond to request for maintenance at no cost to BOC;

c. Provide not less than 7 days proactive notice of scheduled downtimes, service interruption, upgrades or preventive maintenance, if any; subject to the approval of BOC authorized representative; and

d. Submit monthly access/usage reports to attest compliance to the SLA.

III. WAN LINK FOR HEAD OFFICE AND COLLECTION DISTRICTS

	TECHNICAL AND REQUIREMENTS SPECIFICATION	Statement of Compliance
1	The Solution Provider shall follow the required line speeds for each BOC site as stated in the Technical Specifications.	

2	The Solution Provider shall manage the BOC Wide Area Network (WAN) links and shall be the single point of contact for all the network links.	
3	Within Two (2) months from the issuance of Notice to Proceed, the Solution Provider shall install the connectivity infrastructure between and among the Office of the Commissioner and Collection Districts at the required line speeds.	
4	The Solution Provider shall operate, maintain and manage the connectivity between and among the Office of the Commissioner and Collection Districts during the period of the contract.	
5	In any event that single or multiple offices have technical issue on the connectivity, this shall not affect the rest of the offices and the remaining sites shall remain connected.	
6	The Solution Provider shall be responsible for the connectivity and the needed equipment or active components for the connectivity solution, aside from the BOC existing network equipment. The Solution Provider shall provide all equipment, parts or supplies to accomplish the connectivity infrastructure including but not limited to modems, routers, switches, etc.	
7	The Solution Provider shall provide a connectivity solution that is IP-based.	
8	The Solution Provider shall provide managed network administration services including but not limited to: status monitoring, additional VLAN activation if necessary, editing of routes, IP address allocation, traffic report generation, basic troubleshooting, stopping/starting/restarting of network equipment and password resetting if needed.	
9	The Solution Provider shall have a monitoring facility with a team of certified network professionals providing 24x7 services on network monitoring, troubleshooting and maintenance.	
10	The Solution Provider shall guarantee the throughput of all sites as specified in the bandwidth requirements. This includes not only the modem connection but also throughout of the Wide Area Network. If the Service Provider does not meet the required throughput for all or particular site/s, BOC will impose penalty rebate for that specific site/s computed as 50% per day for any day that the throughput is not met.	
11	All the equipment the Solution Provider will provide shall be compatible with BOC's electrical system, which is 220-240V. The Solution Provider is responsible for providing any converters necessary for connecting the electrical system at no cost to BOC.	

12	The Solution Provider shall provide 2 separate Bit Error Rate (BER) tests for all services, for a continuous period of not less than 24 hours each that is acceptable to the BOC. In the event that either BER test is not acceptable, then the test will be repeated until it is acceptable to the BOC. The Solution Provider is responsible for providing the proper equipment for the BER test. The Solution Provider shall conduct the 1st BER test as part of their installation procedures. After successful completion of the 1st BER test and complete installation, the Solution Provider shall notify the BOC of the completion of the BER test and request for acceptance of the service to the BOC. Upon receipt of the notification, BOC will schedule the acceptance of the service at its convenience. The acceptance procedures will require that a 2nd BER test to be conducted, which is to be witnessed and signed by the BOC's authorized representative. All BER test results shall be provided in their original form from the BER test devices, signed by the witnesses of the test.	
13	The Solution Provider shall complete the installation and 1st BER test within 180 days (six months) from the date the Notice to Proceed is issued. If this is not met, BOC will not issue an Acceptance Certificate to be used for billing purposes unless corrected. This will be applied to all sites until all sites are completed.	
14	The Service Provider shall allow the BOC a free five-day (business days) trial after successful completion of the 2nd BER test to ensure the service is compatible with all specifications and BOCs equipment, software, and network. In the event that the BOC deems the service is not acceptable, then the 2nd BER test and free five-day trial shall be repeated until the BOC deems the service acceptable.	
15	The connectivity solution must be capable of handling both voice and data transmission, with adjustable quality of service capabilities for type of traffic prioritization.	
16	All sites shall have the ability to communicate with any and all other sites directly for both voice and data. The Solution Provider shall be responsible for ensuring the proper routing for all communications to the proper sites.	
17	The Solution Provider (SP) shall ensure a smooth migration from the BOC existing Solution Provider to the new SP. There shall be no downtime on the BOC's communication link during the transition.	
18	The Solution Provider shall provide as part of their proposal a diagram which will show how the BOC office will be connected. The diagram shall clearly reflect specific type of connectivity technology for each site.	
19	During the contract period, the provider shall allow the provision to increase in the bandwidth at a specific rate and shall be able to allow such change in any given office site.	

IV. NETWORK EQUIPMENT

	TECHNICAL AND REQUIREMENTS SPECIFICATION	**Statement of Compliance**
1	**Core Switches** **Physical Specification** • Must be modular and chassis-based with at least six (6) slots	

- Must have at least four (4) nonblocking 10 Gigabit Ethernet uplinks [SFP+] per chassis
- Must have Hot Swappable Redundant AC Power Supply
- Switch chassis must be redundant
- Each chassis must include four (1) x 24 SFP-based ports line card that can support copper or fiber transceiver modules
- Each chassis must include one (1) x 48 Gigabit Ethernet copper ports Line card.

Performance and Scalability

Must at least have the following:

- 928 Gbps switching capacity
- 48 Gbps per slot of Switching Capacity
- Can support up to 250 Mpps of throughput for IPv4 and 125Mpps for IPv6
- Must be capable of Virtual Switching System (VSS) or equivalent wherein the two chassis will act as a single virtual switch.
- 4 GB of SDRAM
- 2GB NVRAM

Features

- Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other)
- Port Security, DHCP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the-middle attacks
- Per-port broadcast, multicast, and unicast storm control
- Must restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a non-broadcast multi-access like segment
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1Q VLAN Trunking
- Platform must have the ability to apply QoS configuration
- Management and Troubleshooting Requirements
    - Platform allow user connectivity via Secure Shell (SSH)
    - Simple Network Management Protocol (SNMP) version 1,2c, and 3
    - Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network
    - Integrated Security Features include Port Security
    - Switch-port auto recovery (Err disable)
    - IEEE 802.1ab Link Layer Discovery Protocol (LLDP).
    - IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)
- Platform support user authentication (local or radius) to control access
- IPv6 Compliance
- Dual stack support for IPv4/IPv6 and Dynamic hardware forwarding-

	table allocations for ease of IPv4-to-IPv6 migration • In-Service Software Upgrade (ISSU) support	
2	**Distribution Switches** Physical Specification • Twenty-four(24) 10/100/1000 Ethernet ports with four (4) Gigabit Ethernet SFP ports Two (2) 1GE SFP Single mode or Multimode Fiber transceiver modules • Can support stacking up to 9 switches in a single Stack with 480 Gbps of stacking bandwidth • Can support aggregation of available power in a stack of switches and manage it as one common power pool for the entire stack • Redundant AC Power Supply • Must be redundant switch Performance and Scalability Must at least have the following: • Forwarding Rate – 68.4 Mpps • Switching Bandwidth - 92 Gbps • Flash Memory – 2GB □ DRAM – 4GB • VLAN IDs – 4000 Features • Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other) • Port Security, DHCP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the- middle attacks • Must support secure access to the network, enforce security policies, and deliver standard based security solutions such as 802.1X enabling secure collaboration and policy compliance. • Must restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a non-broadcast multi-access like segment. • Must provide security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic. • Per-VLAN Rapid Spanning Tree (PVRST+) • SNMPv3 • IEEE 802.1Q VLAN Trunking • Platform must have the ability to apply QoS configuration • Management and Troubleshooting Requirements - Platform allow user connectivity via Secure Shell (SSH) - Simple Network Management Protocol (SNMP) version 1,2c, and 3 - Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network - Integrated Security Features include Port Security - Switch-port auto recovery (Err disable) - Layer 2 Trace route - IEEE 802.1ab Link Layer Discovery Protocol	

	(LLDP). - IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) • Platform support user authentication (local or radius) to control access Support for IPv4 and IPv6 routing	
3	**Access Switches** Physical Specification • All access switches must be PoE • Forty-eight(48) 10/100/1000 Ethernet ports with four 4 SFP-based ports • Must support stacking up to eight (8) switches in a single stack. • Each switch must support copper or fiber transceiver modules Performance and Scalability Must at least have the following: • Forwarding Rate – 107.1 Mpps • Switching Capacity - 216 Gbps • Flash Memory – 128 MB • DRAM – 512 MB Maximum VLANs – 1023 • VLAN IDs – 4096 Features • Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other) • Port Security, IGMP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the-middle attacks • Per-port broadcast, multicast, and unicast storm control • Must support flexible authentication including 802.1X authentication • Port-Based ACLs Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1Q VLAN Trunking • Platform must have the ability to apply QoS configuration • Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD • Bridge Protocol Data Unit (BPDU) Guard • Platform allow user connectivity via Secure Shell (SSH) • Simple Network Management Protocol (SNMP) version 1,2c, and 3 • Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network • Layer 2 Trace route • IEEE 802.1ab Link Layer Discovery Protocol (LLDP) • IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) • Supports Automatic media-dependent interface crossover • Supports Multicast VLAN Registration	

	• Supports dynamic VLANs and dynamic trunk configuration across all switches.	
4	**Server Farm Switches** Physical Specification • Twenty-four(24) 10/100/1000 Ethernet ports with four (4) Gigabit Ethernet SFP ports • Two (2) 1GE SFP Single mode or Multimode Fiber transceiver modules • Can support stacking up to 9 switches in a single Stack with 480 Gbps of stacking bandwidth • Can support aggregation of available power in a stack of switches and manage it as one common power pool for the entire stack • Redundant AC Power Supply □ Must be redundant switch Performance and Scalability Must at least have the following: • Forwarding Rate – 68.4 Mpps • Switching Bandwidth - 92 Gbps • Flash Memory – 2GB □ DRAM – 4GB □ VLAN IDs – 4000 Features • Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other) • Port Security, DHCP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the- middle attacks • Must support secure access to the network, enforce security policies, and deliver standard based security solutions such as 802.1X enabling secure collaboration and policy compliance. • Must restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a non-broadcast multi-access like segment. • Must provide security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic. • Per-VLAN Rapid Spanning Tree (PVRST+) • SNMPv3 □ IEEE 802.1Q VLAN Trunking • Platform must have the ability to apply QoS configuration • Management and Troubleshooting Requirements - Platform allow user connectivity via Secure Shell (SSH) - Simple Network Management Protocol (SNMP) version 1,2c, and 3 - Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network - Integrated Security Features include Port Security - Switch-port autorecovery (Err disable) - Layer 2 Trace route - IEEE 802.1ab Link Layer Discovery Protocol (LLDP).	

	- IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) • Platform support user authentication (local or radius) to control access • Support for IPv4 and IPv6 routing	
5	**WAN Switches** Physical Specification • Forty-eight(48) 10/100/1000 Ethernet ports with four 4 SFP-based ports • Must support stacking up to eight (8) switches in a single stack. • Each switch must support copper or fiber transceiver modules Performance and Scalability Must at least have the following: • Forwarding Rate – 107.1 Mpps • Switching Capacity - 216 Gbps • Flash Memory – 128 MB • DRAM – 512 MB • Maximum VLANs – 1023 • VLAN IDs – 4096 Features • Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other) • Port Security, IGMP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the-middle attacks • Per-port broadcast, multicast, and unicast storm control • Must support flexible authentication including 802.1X authentication • Port-Based ACLs • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1Q VLAN Trunking • Platform must have the ability to apply QoS configuration • Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD • Bridge Protocol Data Unit (BPDU) Guard • Platform allow user connectivity via Secure Shell (SSH) • Simple Network Management Protocol (SNMP) version 1,2c, and 3 • Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network • Layer 2 Trace route • IEEE 802.1ab Link Layer Discovery Protocol (LLDP). • IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) • Supports Automatic media-dependent interface crossover	

	• Supports Multicast VLAN Registration • Supports dynamic VLANs and dynamic trunk configuration across all switches.	
6	**DMZ Switches** Physical Specification • Forty-eight (48) 10/100/1000 Ethernet ports with four 4 SFP-based ports • Must be stackable up to eight (8) switches in a single stack. • Each switch must support copper or fiber transceiver modules Performance and Scalability Must at least have the following: • Forwarding Rate – 107.1 Mpps • Switching Capacity - 216 Gbps • Flash Memory – 128 MB • DRAM – 512 MB • Maximum VLANs – 1023 • VLAN IDs – 4096 Features • Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other) • Port Security, IGMP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the-middle attacks • Per-port broadcast, multicast, and unicast storm control • Must support flexible authentication including 802.1X authentication • Port-Based ACLs • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1Q VLAN Trunking • Platform must have the ability to apply QoS configuration • Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD • Bridge Protocol Data Unit (BPDU) Guard • Platform allow user connectivity via Secure Shell (SSH) • Simple Network Management Protocol (SNMP) version 1,2c, and 3 • Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network • Layer 2 Trace route • IEEE 802.1ab Link Layer Discovery Protocol (LLDP). • IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) • Supports Automatic media-dependent interface crossover • Supports Multicast VLAN Registration • Supports dynamic VLANs and dynamic trunk configuration across all	

	switches.	
7	**WAN Routers** Physical Specification Must have the following: • Four (4)-on board 10/100/1000 routed ports. - With two (2) of the Gigabit Ethernet (10/100/1000) WAN ports on the proposed router must support Small Form-Factor Pluggable (SFP)-based connectivity in lieu of RJ-45 ports, enabling fiber connectivity • Has 1GB DRAM by default and can expand up to 2GB • Has 256MB External Flash by default and can expand up to 8GB • Router should have 2nd external compact flash card slot • Has one (1) USB Console Port • Has one(1) Serial Console Port • Has one(1) Serial Auxiliary Port • Redundant AC Power Supply Performance and Scalability Must at least have the following: • Enabled for deployment in high-speed WAN environments with concurrent services up to 350 Mbps • Multi-Gigabit Fabric enables high bandwidth module to module communication without compromising routing performance • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency Features • Must have a universal image installed on the router that contains software technology sets and can be activated by software license. • Support intelligent power management and allowing to control power to the modules based on the time of day. • Should support IPv4, IPv6 static routing and Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) compliant • Should support Firewall and VPN features and optional intrusion prevention and content security features • Capable of IPv4 and IPv6, AAA, ACL, PBR, GRE, RADIUS, TACACS, SNMP, Multicast, QoS, VLAN and WCCP (or its equivalent) • Support various major WAN protocols/ Interface: High Speed WAN interface, ISDN, ATM, T1/E1, xDSL	
8	**Routers(for Metro E links)** Physical Specification Must have the following: • Three (3)-on board 10/100/1000 routed ports. • Has 512MB DRAM by default and can expand up to 2GB • Has 256MB External Flash by default and can expand up to 8GB • Router should have 2nd external compact flash card slot • Has one (1) USB Console Port Has one(1) Serial Console Port	

	• Has one(1) Serial Auxiliary Port Performance and Scalability Must at least have the following: • Enabled for deployment in high-speed WAN environments with concurrent services up to 35 Mbps • Multi-Gigabit Fabric enables high bandwidth module to module communication without compromising routing performance • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency Features • Must have a universal image installed on the router that contains software technology sets and can be activated by software license. • Support intelligent power management and allowing to control power to the modules based on the time of day. • Should support IPv4, IPv6 static routing and Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) compliant • Capable of IPv4 and IPv6, AAA, ACL, PBR, GRE, RADIUS, TACACS, SNMP, Multicast, QoS, VLAN and WCCP (or its equivalent) • Support various major WAN protocols/ Interface: High Speed WAN interface, ISDN, ATM, T1/E1, xDSL	
9	**Branch Routers** Physical Specification Must have the following: • Two (2)-on board 10/100/1000 routed ports. • Has 512MB DRAM by default and can expand up to 2.5GB • Has 256MB External Flash by default and can expand up to 8GB • Router should have 2nd external compact flash card slot • Has one (1) USB Console Port • Has one(1) Serial Console Port • Has one(1) Serial Auxiliary Port Performance and Scalability Must at least have the following: • Enabled for deployment in high-speed WAN environments with concurrent services up to 25 Mbps • Multi-Gigabit Fabric enables high bandwidth module to module communication without compromising routing performance • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency Features • Must have a universal image installed on the router that contains software technology sets and can be activated by software license. • Support intelligent power management and allowing to control power to the modules based on the time of day. • Should support IPv4, IPv6 static routing and Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP)	

	compliant • Capable of IPv4 and IPv6, AAA, ACL, PBR, GRE, RADIUS, TACACS, SNMP, Multicast, QoS, VLAN and WCCP (or its equivalent) • Support various major WAN protocols/ Interface: High Speed WAN interface, ISDN, ATM, T1/E1, xDSL • Supports Multicast VLAN Registration • Supports dynamic VLANs and dynamic trunk configuration across all switches.	
10	**Switches for the Branch Sites** Physical Specification • All access switches must be PoE • Twenty-four(24) 10/100/1000 Ethernet ports with four 4 SFP-based ports • Must support stacking up to eight (8) switches in a single stack. • Each switch must support copper or fiber transceiver modules Performance and Scalability Must at least have the following: • Forwarding Rate – 71.4 Mpps • Switching Capacity - 216 Gbps • Flash Memory – 128 MB • DRAM – 512 MB • Maximum VLANs – 1023 • VLAN IDs – 4096 Features • Port aggregation technology, where ports should not be contiguous or on the same module when configuring LACP (IEEE 802.3ad LACP or any other) • Port Security, IGMP Snooping, Dynamic ARP Inspection and IP Source Guard – security features to prevent man-in-the-middle attacks • Per-port broadcast, multicast, and unicast storm control • Must support flexible authentication including 802.1X authentication • Port-Based ACLs □ Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1Q VLAN Trunking • Platform must have the ability to apply QoS configuration • Unidirectional Link Detection (UDLD) Protocol and Aggressive UDLD • Bridge Protocol Data Unit (BPDU) Guard • Platform allow user connectivity via Secure Shell (SSH) • Simple Network Management Protocol (SNMP) version 1,2c, and 3 • Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) that support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network • Layer 2 Trace route	

	• IEEE 802.1ab Link Layer Discovery Protocol (LLDP). • IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) Supports Automatic media-dependent interface crossover • Supports Multicast VLAN Registration • Supports dynamic VLANs and dynamic trunk configuration across all switches.	

Technical Specifications		
	DESCRIPTION	**Compliance**
Data Center / Server Farm Firewall		
1	Appliance should support Active/Standby or Failover hardware feature.	
2	Appliance should have Eight (8) Gigabit Ethernet ports.	
3	Capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
4	Capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).	
5	Capable to detect variants of known threats, as well as new threats (i.e., so-called “unknown threats”).	
6	Capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface).	
7	Capable of detecting multi-part or extended threats by aggregating and correlating the multiple, disparate events associated with them.	
8	Capable of detecting and blocking IPv6 attacks.	
9	Provides network-based detection of malware by checking the disposition of known files in the Security Intelligence engine using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts.	
10	Advance custom signature creation where the user can write their own IPS signature using different signature format.	
11	Capable of customizing Rate-based attacks. This will able to identify or lessen the false positive alerts and able to provide prioritization.	
12	Able to inspect and block in-line deployment in Trunk mode and Access mode links/interface.	
13	Able to perform inspection and blocking threats in a logical in-line deployment.	
14	Identifies the Geolocation of the Source and Destination of IP Address.	
15	Able to allow/block traffic based on per Zone, Network, VLAN, Geolocation, Application and URL sites.	
16	Able to enforce policy rules based on Per User account (can be integrated with the Active Directory).	
17	Can associate with File and IPS rules to provide an effective policy.	

18	Passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
19	Assist to determine the scope of outbreaks by providing a visual, interactive representation of the path of an infected file takes across the network. This will help to understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer.	
20	Once detected, it contains or block malware and provides a detailed historical report and able to perform immediate action.	
21	Show the life cycle and disposition of each file in the environment from the first time it was seen to the last time as well as computers in the network that contains a malware. The parent that carried the malware/threat into the network will be identified including any file created or executed by the threat.	
22	It tracks file and network events in chronological order. This would give visibility into the events leading to and after the compromise. This includes parent processes, connections to remote host and unknown files that may have downloaded by the malware. File events should include file name, path, parent process, file size, execution context and hashes of the file. Network events should include processes attempting connection, destination IP, source and destination ports, execution context, file size, age and hash.	
23	Blocks communication based on the up-to-date IP address with Bad reputation (e.g.: Source of CnC, Malwares, SPAM, Suspicious sites).	
24	Supports IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.	
25	Appliance should have additional detection value using Honeypots.	
26	On the same IPS appliance, it detects and blocks threats through to the up to date One-to-One Signature based on the feeds provided by the IPS Security Intelligence Engine.	
27	Provides Sandboxing inspection for thorough file disposition analysis.	
28	Provides Machine learning feature wherein the file’s disposition (clean or malware) is identified based on its characteristic behavior and being compare to a Malware file behavior on your network.	
29	Support Advance malware protection for mobile where it can analyze iOS/Android applications for possible threats in real time.	
30	Provide prioritized list of potentially compromised devices for quick links to inspect and remediate the problem.	
31	Should blocks communication directly with attackers or via command and control (CnC) servers and distribution of malware at the endpoint	
32	Appliance should allow the user to upload an executable file into a sandbox environment where it can be executed and analyzed. This provides a safe and secure sandbox environment to analyze the behavior of malware and suspect files.	
33	Appliance should Provide advanced malware analysis and protection by using big data and analytics to detect, analyze and control advanced malware outbreaks.	

34	Appliance should be able to perform Retrospective Scanning that continuously track files that is known to be “unknown” that passed the “Before” and “During” attack phase.	
35	Identifies/Consolidates unknown and known malwares based on learned behavior and information of threats from various advance malware enabled devices (eg; Email Security Appliance, Web Security Appliance, Firewall with IPS appliance and IPS dedicated appliance).	
36	Provides latest Update of Network Security threat that has been identified and validated by the Centralized Security Intelligence Development, Intelligence and Detection RND Team.	
37	Appliance should be the leader in Security effectiveness in the NSS Labs Breach Detection System of year 2015.	
38	Proposed appliance should be in the "Leader" quadrant of the Gartner Magic Quadrant for IPS.	
39	Appliance should have a Stateful inspection throughput of 1.5 Gbps.	
40	Appliance should have an IPS throughput of 900mbps.	
Perimeter		
1	Appliance should support Active/Standby or Failover hardware feature.	
2	Appliance should have Eight (8) Gigabit Ethernet ports.	
3	Capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
4	Capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).	
5	Capable to detect variants of known threats, as well as new threats (i.e., so-called “unknown threats”).	
6	Capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface).	
7	Capable of detecting multi-part or extended threats by aggregating and correlating the multiple, disparate events associated with them.	
8	Capable of detecting and blocking IPv6 attacks.	
9	Provides network-based detection of malware by checking the disposition of known files in the Security Intelligence engine using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts.	
10	Advance custom signature creation where the user can write their own IPS signature using different signature format.	
11	Capable of customizing Rate-based attacks. This will able to identify or lessen the false positive alerts and able to provide prioritization.	
12	Able to inspect and block in-line deployment in Trunk mode and Access mode links/interface.	
13	Able to perform inspection and blocking threats in a logical in-line deployment.	
14	Identifies the Geolocation of the Source and Destination of IP Address.	
15	Able to allow/block traffic based on per Zone, Network, VLAN, Geolocation, Application and URL sites.	

16	Able to enforce policy rules based on Per User account (can be integrated with the Active Directory).	
17	Can associate with File and IPS rules to provide an effective policy.	
18	Passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
19	Assist to determine the scope of outbreaks by providing a visual, interactive representation of the path of an infected file takes across the network. This will help to understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer.	
20	Once detected, it contains or block malware and provides a detailed historical report and able to perform immediate action.	
21	Show the life cycle and disposition of each file in the environment from the first time it was seen to the last time as well as computers in the network that contains a malware. The parent that carried the malware/threat into the network will be identified including any file created or executed by the threat.	
22	It tracks file and network events in chronological order. This would give visibility into the events leading to and after the compromise. This includes parent processes, connections to remote host and unknown files that may have downloaded by the malware. File events should include file name, path, parent process, file size, execution context and hashes of the file. Network events should include processes attempting connection, destination IP, source and destination ports, execution context, file size, age and hash.	
23	Blocks communication based on the up-to-date IP address with Bad reputation (e.g.: Source of CnC, Malwares, SPAM, Suspicious sites).	
24	Supports IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.	
25	Appliance should have additional detection value using Honeypots.	
26	On the same IPS appliance, it detects and blocks threats through to the up to date One-to-One Signature based on the feeds provided by the IPS Security Intelligence Engine.	
27	Provides Sandboxing inspection for thorough file disposition analysis.	
28	Provides Machine learning feature wherein the file’s disposition (clean or malware) is identified based on its characteristic behavior and being compare to a Malware file behavior on your network.	
29	Support Advance malware protection for mobile where it can analyze iOS/Android applications for possible threats in real time.	
30	Provide prioritized list of potentially compromised devices for quick links to inspect and remediate the problem.	
31	Should blocks communication directly with attackers or via command and control (CnC) servers and distribution of malware at the endpoint.	
32	Appliance should allow the user to upload an executable file into a sandbox environment where it can be executed and analyzed. This provides a safe and secure sandbox environment to analyze the behavior of malware and suspect files.	

33	Appliance should Provide advanced malware analysis and protection by using big data and analytics to detect, analyze and control advanced malware outbreaks.	
34	Appliance should be able to perform Retrospective Scanning that continuously track files that is known to be “unknown” that passed the “Before” and “During” attack phase.	
35	Identifies/Consolidates unknown and known malwares based on learned behavior and information of threats from various advance malware enabled devices (eg; Email Security Appliance, Web Security Appliance, Firewall with IPS appliance and IPS dedicated appliance).	
36	Provides latest Update of Network Security threat that has been identified and validated by the Centralized Security Intelligence Development, Intelligence and Detection RND Team.	
37	Appliance should be the leader in Security effectiveness in the NSS Labs Breach Detection System of year 2015.	
38	Proposed appliance should be in the "Leader" quadrant of the Gartner Magic Quadrant for IPS.	
39	Appliance should have a Stateful inspection throughput of 1 Gbps.	
40	Appliance should have an IPS throughput of 600mbps.	
Spare Firewall		
1	Appliance should support Active/Standby or Failover hardware feature.	
2	Appliance should have Eight (8) Gigabit Ethernet ports.	
3	Capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
4	Capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).	
5	Capable to detect variants of known threats, as well as new threats (i.e., so-called “unknown threats”).	
6	Capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface).	
7	Capable of detecting multi-part or extended threats by aggregating and correlating the multiple, disparate events associated with them.	
8	Capable of detecting and blocking IPv6 attacks.	
9	Provides network-based detection of malware by checking the disposition of known files in the Security Intelligence engine using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts.	
10	Advance custom signature creation where the user can write their own IPS signature using different signature format.	
11	Capable of customizing Rate-based attacks. This will able to identify or lessen the false positive alerts and able to provide prioritization.	
12	Able to inspect and block in-line deployment in Trunk mode and Access mode links/interface.	
13	Able to perform inspection and blocking threats in a logical in-line deployment.	

14	Identifies the Geolocation of the Source and Destination of IP Address.	
15	Able to allow/block traffic based on per Zone, Network, VLAN, Geolocation, Application and URL sites.	
16	Able to enforce policy rules based on Per User account (can be integrated with the Active Directory).	
17	Can associate with File and IPS rules to provide an effective policy.	
18	Passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
19	Assist to determine the scope of outbreaks by providing a visual, interactive representation of the path of an infected file takes across the network. This will help to understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer.	
20	Once detected, it contains or block malware and provides a detailed historical report and able to perform immediate action.	
21	Show the life cycle and disposition of each file in the environment from the first time it was seen to the last time as well as computers in the network that contains a malware. The parent that carried the malware/threat into the network will be identified including any file created or executed by the threat.	
22	It tracks file and network events in chronological order. This would give visibility into the events leading to and after the compromise. This includes parent processes, connections to remote host and unknown files that may have downloaded by the malware. File events should include file name, path, parent process, file size, execution context and hashes of the file. Network events should include processes attempting connection, destination IP, source and destination ports, execution context, file size, age and hash.	
23	Blocks communication based on the up-to-date IP address with Bad reputation (e.g.: Source of CnC, Malwares, SPAM, Suspicious sites).	
24	Supports IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.	
25	Appliance should have additional detection value using Honeypots.	
26	On the same IPS appliance, it detects and blocks threats through to the up to date One-to-One Signature based on the feeds provided by the IPS Security Intelligence Engine.	
27	Provides Sandboxing inspection for thorough file disposition analysis.	
28	Provides Machine learning feature wherein the file's disposition (clean or malware) is identified based on its characteristic behavior and being compare to a Malware file behavior on your network.	
29	Support Advance malware protection for mobile where it can analyze iOS/Android applications for possible threats in real time.	
30	Provide prioritized list of potentially compromised devices for quick links to inspect and remediate the problem.	
31	Should blocks communication directly with attackers or via command and control (CnC) servers and distribution of malware at the endpoint.	

32	Appliance should allow the user to upload an executable file into a sandbox environment where it can be executed and analyzed. This provides a safe and secure sandbox environment to analyze the behavior of malware and suspect files.	
33	Appliance should Provide advanced malware analysis and protection by using big data and analytics to detect, analyze and control advanced malware outbreaks.	
34	Appliance should be able to perform Retrospective Scanning that continuously track files that is known to be “unknown” that passed the “Before” and “During” attack phase.	
35	Identifies/Consolidates unknown and known malwares based on learned behavior and information of threats from various advance malware enabled devices (e.g.; Email Security Appliance, Web Security Appliance, Firewall with IPS appliance and IPS dedicated appliance).	
36	Provides latest Update of Network Security threat that has been identified and validated by the Centralized Security Intelligence Development, Intelligence and Detection RND Team.	
37	Appliance should be the leader in Security effectiveness in the NSS Labs Breach Detection System of year 2015.	
38	Proposed appliance should be in the "Leader" quadrant of the Gartner Magic Quadrant for IPS.	
39	Appliance should have a Stateful inspection throughput of 600 Mbps.	
40	Appliance should have an IPS throughput of 400 Mbps.	
Endpoint Protection		
1	The solution must provide advanced malware analysis and protection by using big data and analytics to detect, analyze and control advanced malware outbreaks.	
2	The solution should be able to cater up to 500 VM endpoints.	
3	The solution should have a management console.	
4	The solution must be able to track file and network events in chronological order. This would give visibility into the events leading to and after the compromise. This includes parent processes, connections to remote host and unknown files that may have downloaded by the malware. File events should include file name, path, parent process, file size, execution context and hashes of the file. Network events should include processes attempting connection, destination IP, source and destination ports, execution context, file size, age and hash.	
5	The solution must allow the user to upload an executable into a sandbox environment where it can be executed and analyzed. This provides a safe and secure sandbox environment to analyze the behavior of malware and suspect files.	
6	The solution must provide control capabilities to stop the spread of malware and malware activities without waiting for security updates. Control capabilities should include: - Custom detections where you can detect and quarantine files by uploading the file or its SHA - Advance custom signature where the user can write their own signature using different signature format such as MD5, File body-based signatures, extended signature format (offsets, wildcards, regular expressions)	

	- Application Blocking to stop applications with vulnerabilities from executing until a patch has been released.	
7	The solution must have the ability to show the life cycle of each file in the environment from the first time it was seen to the last time as well as computers in the network that had it. The parent that brought the threat into the network must be displayed including any file created or executed by the threat.	
8	The solution must continuously cross-references files analyzed in the past against the latest threat intelligence and quarantines any files previously deemed clean or unknown that are now known to be a threat.	
9	Retrospective security should assist to determine the scope of outbreaks contains them and ultimately turns back the clock enabling automatic malware remediation.	
10	The solution must support Advance malware protection for mobile where it can analyze Android applications for possible threats in real time.	
11	The solution must use metadata for analysis, actual files should not be sent to the cloud for analysis.	
12	The solution must provide prioritized list of potentially compromised devices for quick links to inspect and remediate the problem.	
13	The solution must correlate activities on an endpoint with traffic on the network, providing integrated intelligence and automation across the advanced malware protection security infrastructure. It should block communication directly with attackers or via command and control (CnC) servers and distribution of malware at the endpoint.	
14	Device Flow Correlation must support custom IP black and white lists on top of the IP reputation services provided by the vendor.	
Network Access Control System		
1	Should use full proof mechanism for identifying and isolating end devices depending on network Access policy. (e.g., shall not use DHCP based mechanisms that could be compromised by manual IP settings).	
2	Isolation must be done at the network device level (e.g., Switch level) and should be able to black list hosts irrespective of the location/ port connected in the intranet. This should be performed automatically/ manually by administrators.	
3	Should be able to manage, configure and monitor centrally and should support different delegation levels for administration purposes.	
4	Should be able to support Virtual Environment.	
Device Authentication and Network Access		
1	Should allow only authenticated/managed devices to connect to organization networks.	
2	Should allow only authorized (i.e. authenticated and policy compliant) devices to connect to Company networks.	
3	Product should allow access VLAN assignment based on user role (after the host is determined to be “compliant” to policy).	
4	Should support both agent-based and agent-less NAC deployment.	
5	Should allow device authentication plus policy compliance with automated remediation using multiple logical network segmentation.	
6	Should be able to prevent users from connecting to the corporate network without login to the corporate domain. (Local logon users must be denied with intranet services).	

7	The NAC Solution should be able to detect computers joined to the Intranet domain and apply separate policies.	
8	The NAC system should support exclusion lists.	
9	Solution should provide a way for devices other than end user computers (e.g. – printers, VoIP phones, etc.) to be authenticated onto the network.	
10	Should be able to track behavioral changes after a device had authenticated to the corporate network to mitigate the threat of a different device accessing the network using the same switch port spoofing the previous device identity.	
11	Should be able to work on both 802.1x enabled and non 802.1x enabled environment.	
Policies and Compliance		
1	Should allow administrators to manipulate and maintain multiple device policies.	
2	Should retrieve policy compliance information from the end device using a secure communication method.	
3	Should be able to check for specific windows registry values & should be able to use them for policy enforcement.	
4	Should support the creation of customized policy checks.	
5	Product should support a common policy platform for all users (wired, wireless, VPN & Dialup).	
6	Should support reusable policy creation.	
7	Achiever of Common Criteria EAL4+.	
Integration into the existing environment		
1	Should not add bottle necks / more overheads to existing network performance.	
2	Deployment should not be inline and should be able to utilize SPAN ports or taps.	
3	Should dynamically set VLANs on the switch ports according to the policies set for the devices connected to it.	
4	Should provide Layer 2 switch port level access control without requiring 802.1x for authentication.	
5	Should support wired and wireless network users.	
6	Should be able to integrate with Microsoft SUS, Microsoft SCCM and Sophos End Point Security.	
Interoperability		
1	Should operate within a heterogeneous network with switches from multiple vendors (e.g. - Cisco, 3com, Alcatel, Alaxaia, Apresia, Dax, Dell, dlink, Entersys, Extreme, Force10, Brocade/Foundry, H3C, Hirschman, HP, Juniper, NEC, Nortel ,Router-Linux).	
2	Should be capable of integrating with third party wireless controllers (Cisco, Aruba, Meru, and Xirrus).	
3	Should support Active Directory Integration.	
4	Should be able to leverage existing user authentication databases such as RADIUS and LDAP without customization.	
5	Should be able to integrate with existing patch management tools such as Microsoft SMS/WSUS and SCCM.	

6	Should be able to integrate with SIEMs such as ArcSight, McAfee ESM, Splunk, Log Rhythm, IBM Qradar.	
7	Should be able to integrate with Vulnerability Assessment such as Tenable, Qualys, Rapid7, McAfee MVM.	
8	Should be able to integrate with MDMs such as Airwatch, MobileIron, Good Technology, Maas360, Citrix.	
Monitoring and Auditing		
1	Should continuously monitor machines both before and after Access to the LAN, for behavioral changes (track changes), malicious activities, etc.	
2	Should be able to audit, monitor and tie incidents to a specific user.	
3	Should be able to audit traffic and endpoints on a per-user, per-application basis for compliance with regulations.	
4	Should support policy, audit and report generation but not enforce action.	
Mobile Device Security (must be upgradable to support following options)		
1	Identify corporate vs. personal devices.	
2	Identify unauthorized and non-compliant devices.	
3	Identify mobile devices without password protection.	
4	Identify rooted devices and jailbroken devices.	
5	Identify mobile devices that are missing required apps, for example, corporate, MDM or security apps.	
6	Send messages to mobile user.	
7	Block or limit network access based on who, what, when, where, and how the device is configured.	
8	Unified management and reporting of all endpoint devices on the network regardless of user, device ownership, device type, connection method, or location.	
9	Identify and block malicious activities.	
Security Requirements		
1	The agent running on the host should not be allowed to make Access control decisions, in case the host was compromised or the agent was disabled.	
2	Should protect authentication credentials provided to it using a standard secure method.	
3	End should not be able to shutdown / disable the agent or change NAC Policies.	
Management		
1	Should support central management if multiple appliances are involved.	
2	Should support CLI and GUI-based management.	
3	Should support multiple administrative roles with varying levels of administrative access (i.e., Network Admin, Security Admin, Help Desk, etc.)	
Logging and Event Management		
1	Should provide detailed device logs and other forms of event collection for potential use in forensic analysis.	
2	Should support logged events from the NAC to be integrated / exported to a third-party security event management solution.	

General Requirements		
1	Should be configurable to scan only certain machines, based on IP address, group membership and OS types.	
2	Should support scanning of systems for MS vulnerabilities with agent installed for PCs controlled under the corporate domain.	
3	Should be able to run vulnerability scans on endpoints for Microsoft published vulnerabilities.	
4	Should be able to control the end points connected via VPN.	
5	Should provide an application programming interface (API) that facilitates the gathering of policy compliance information (such as Operating System version, patch levels, virus signature versions, connected devices, etc.) for use with customizable scripts.	
6	Should update automatically to become aware of new versions or data files of common applications (e.g., anti-virus programs, P2P Programs, OS patches, etc.).	
Network Discovery		
1	Should provide complete network visibility by automatically detecting all devices connected to the defined network scope.	
2	Should automatically classify the detected devices in to different categories according to their functions such as Windows, Printers, Linux/Unix, Macintosh, Network Devices, etc.	
3	Should provide abundant information regarding the endpoint connected to the network, such as IP Address, MAC Address, NetBIOS Name, NetBIOS Domain, Domain User, Domain Member, OS-Class, IP of the connected switch, Switch Port, Switch Port VLAN, Switch Port Status, Switch Vendor, Access status.	
Guest PC Management		
1	Should detect guest PC's as they connect to the network. Multiple parameters should be used in the process of making this decision.	
2	If detected as a guest to the network, solution should place the device in the guest group & thereafter should be governed by the guest policy.	
3	Should be able to support switchport VLAN assignments according to multiple guest roles (e.g. – contractors, consultants, visitors, etc).	
4	Should provide Forms, HTTP notifications & HTTP login prompts to the guest. This should be possible without any additional configurations at the guest PC.	
5	There should be a multiple level authorized workflow for granting network access to guest PCs.	
6	Should support self-service web portal to request authentication to the network for guests.	
Corporate PC Management & Remediation		
1	Should allow end users to receive information on their PC NAC status (i.e., successfully authenticated, failed authentication, currently being remediated, etc.).	
2	All corporate PC's should be checked against the policies set & should classify hosts as compliant & non-compliant.	
3	Should allow for different remediation processes based on user role.	

4	Should provide update & remediation functionality for non-compliant hosts while quarantined.	
5	Administrators should be able to filter and view the endpoints, by policy & status.	
6	Should be able to scan endpoints with or without a client installed for anti-virus status of the corporate endpoint and further state whether the anti-virus is installed, Anti-Virus is running or whether the Anti-Virus is not updated.	
7	Should identify and provide remediation support for common applications (anti-virus, personal firewall, OS patches)	
8	Should support custom checks for Windows Registry, files, services and applications.	
9	Remediation should include starting processes, killing processes, setting registry keys, starting antivirus, update anti-virus, starting windows updates & running custom scripts.	
10	Should guide users through a self-remediation process using a graphical user interface (GUI), if host is not compliant.	
11	Remediation of non-compliant hosts should be supported without any user intervention (silent-remediation).	
12	The endpoint client should have the capability to be installed on endpoints via Active Directory group policy.	
13	Should support custom remediation scripts.	
14	Should allow customized messages and display of an Acceptable Use Policy to the end user.	
Network Threat Identification and Prevention		
1	Should detect network threats such as worms & hackers.	
2	Should continuously monitor hosts for malicious acts even after hosts are successfully authenticated to the network.	
3	Detected network threats should be prevented from spreading & notifications should be sent to the end user and the administrator concerning the network threat activity via E-mail and http notification.	
4	Should be able to block specific hosts / switch ports where an attack is commencing from & should be able to track the malicious host if they change switch ports.	
5	Should protect networks against zero day attacks, without dependence on signatures.	
6	Should detect the presence of instant messengers & peer to peer applications & allow administrators to implement policies governing those applications.	
Controlling USB Devices		
1	Should be able to detect USB mass storage devices connected to any corporate PC.	
2	USB mass storage device connectivity should be restricted, allowing only an authorized set of devices to connect to the endpoint.	
3	Any type of USB devices other than Mass storages should be identified and classified, and thereafter controlled according to the company security policy regarding the type of device (e.g. – Bluetooth radios, imaging devices, etc.).	

4	Should be able to detect and disable network bridging (Connecting to corporate network while connected to internet using some other connection mechanism).	
Management Reports		
1	No of PCs complied with the NAC Policy.	
2	No of PCs quarantined.	
3	No of Guest PCs connected.	
4	Search Devices by MAC Address / IP Address / Device Name.	
High Availability and Disaster Recovery Requirements		
1	The proposed solution must include high availability and DR solution. Supplier must explain how this is achieved.	
Future Expansions		
1	The proposed solution must be scalable to expand to the branch offices and subsidiaries. Further there has to be a clear update and upgrade path without having to discard the purchased items.	
Deployment and Support		
1	Contractor must have similar deployment using the offered solution.	
2	Provide maintenance agreement for one (1) year, With Corrective/ Remedial Maintenance and Quarterly Health Check Visit.	
3	Technical support must be available 24 X 7 must provide on call support if needed, must provide procedures on support and problem escalation. Technical phone support response time must be 4 hours after notification by COMPANY personnel.	
4	Provide unlimited technical phone consultation. Must have Technical support helpdesk 7/24.	
Others		
1	The solution must be positioned in the Leader Quadrant of the Gartner Report for Network Access Control appliance.	
2	Must provide a photocopy of Common Criteria Certificate for IT Security Evaluation version 3.1 with assurance level EAL4+.	
3	Vendor must provide Certificate of Authorization that the Distributor and Reseller/Contractor are the authorized partners for the project.	
LINK CONTROLLER		
1	**Hardware**	
1.1	The goods must support quad core cpu.	
1.2	The goods must support up to 16GB of memory.	
1.3	The goods must support up to 500 GB of hard drive.	
1.4	The goods must be able to support 8 Gigabit Ethernet ports with optional 2 x fiber SFP.	
1.5	The goods must support two hot swappable power supply.	
1.6	The goods must be CSA, UL, CB, EN, IEC, and FCC certified.	
2	**Performance**	
2.1	The goods must be able to support traffic throughput of up to 10 Gbps at Layer 4 and Layer 7.	
2.2	The goods must support a maximum of 10MConcurrent Connections at Layer 4.	

2.3	The goods must support 150K connections per second at Layer 4.	
2.4	The goods must support 425K Request per Second at Layer 7.	
2.5	The goods must support 1.25M Layer 4 HTTP Requests per Second.	
2.6	The goods must be able to support hardware ssl of 4500 TPS (2K keys) and 8Gbps bulk encryption.	
3	**Features**	
3.1	Comprehensive view in the health and throughput of links.	
3.2	Support scripting language to intelligently route traffic over multiple WAN link, based on TCP/IP parameters such as: source ip address and port, destination ip address and port.	
3.3	Rerouting of traffic to the next available link by using multiple monitors to quickly and accurately determine the health and availability of every link.	
3.4	Provides advanced link traffic distribution capabilities using: - Round robin - Round trip time - Global availability - Hops - Static persistence - Dynamic ratio - Packet completion rate - Topology based routing - Virtual server capacity - Packet rates - Ratio - Kilobytes per second - Least connection	
3.5	Ability to define cost of each connection and billing scheme to automatically direct traffic based on criteria.	
3.6	Ability to define rate shaping to define application and traffic limits, control the rate at which resources are allowed to spike or burst.	
3.7	Ability to provide global application availability and health monitoring through: - Global Load Balancing - Dynamic Ratio Load Balancing - Wide area persistence - Geographic load balancing	

V. COVERAGE AND BANDWIDTH:

Item	Service	Address	Bandwidth
Direct Internet			
1	Direct Internet	BOC Head Office	200Mbps
Item	**Port**	**Address**	**Bandwidth**
	BACKHAUL		

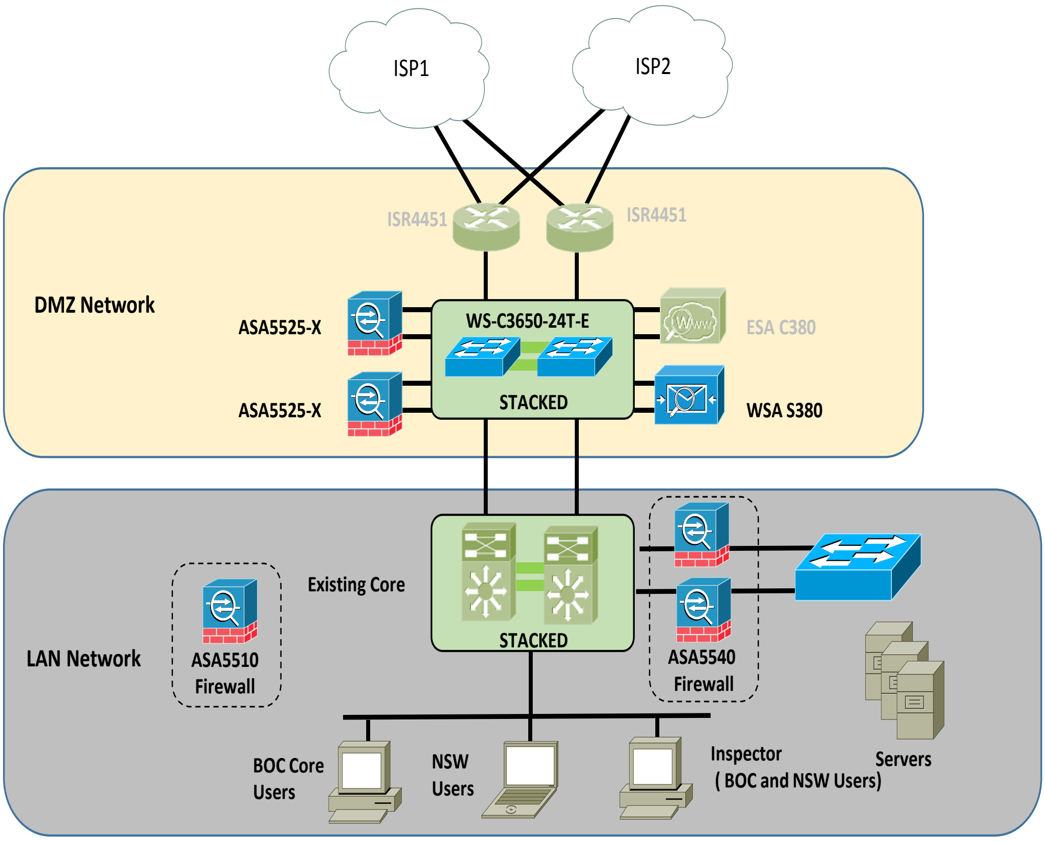
1	BOC Head Office	16th St. Port Area, Manila	200Mbps
	LARGE PORTS		
2	MANILA INTERNATIONAL CONTAINER PORT	Isla Putting Bato, North Harbor, Tondo Manila.	40Mbps
3	NAIA	Bureau of Customs - NAIA	40Mbps
		Old Mia Road, Pasay City	
	MEDIUM PORTS		
4	Port of Cebu	BOC Building, CIP Complex, Osmeña Blvd.	20Mbps
		North Reclamation Area, Cebu City	
		Contact : Bong Romero (MISTG Unit) Tel: 032-2322449	
5	Port of Batangas	Bureau of Customs	20Mbps
		Port of Batangas	
		Brgy. Sta. Clara, Batangas City	
6	Port of Davao	Km. 10 Sasa Wharf, Sasa, Davao City	20Mbps
7	PORT OF SUBIC	Bureau of Customs	20Mbps
		BLDG. 307 CANAL RD. SBMA	
		OLONGAPO CITY	
8	PORT OF CLARK	Bureau of Customs	20Mbps
		M.A. Roxas Hi way, Clark Freeport Zone (back of American Cemetery), Angeles City	
		Telefax No.: (045) 599-7189 to 90	
		Tel. No.: (045) 599-7189 and 599-7191	
	SMALL PORTS		
9	Subport of North Harbor	along Negros Navigation, PIER 2	6Mbps
10	Port of San Fernando	1300 Pennsylvania Ave., Poro Point	6Mbps
		San Fernando City, La Union	
11	Sub-Port of PEZA-Baguio	Bureau of Customs	6Mbps
		PEZA Bldg. Loakan Road, Baguio City	
12	Sub-Port of Sual	Bureau of Customs	6Mbps
		Pob. Sual, Pangasinan	
13	Sub-Port of Salumague	Bureau of Customs	6Mbps
		Cabugao, Ilocos Sur	
14	Port of Aparri	Bureau of Customs	6Mbps
		Punta, Aparri, Cagayan	
15	Sub-Port of Laoag International Airport	Bureau of Customs	6Mbps
		Brgy. Araniw, Airport Ave., Laoag City	
16	Sub-Port of Currimao	Bureau of Customs	6Mbps
		Brgy. Pias Sur, Currimao, Ilocos Norte	

17	Sub- Port of Puerto Princesa	Bureau of Customs	6Mbps
		Jango Building, Puerto Princesa City	
		Palawan 5300	
		Telno : (048) 4332118	
18	Brooke's Point Extension Office	Port Area, Buligay, Brooke's Point, Palawan	6Mbps
		Note: Travel time from Puerto Princesa to Brooke's Point is almost Four (4) hours	
		Contact Person: Alpha Grace T. Castro, OIC- 09175195640	
19	CIQS- OSS Office	RTN Pier	6Mbps
		Rio Tuba, Bataraza, Palawan	
		Travel time from Brooke's Point to Rio Tuba is 1 and a half to two (2) hours	
20	Sub- Port of Siain	Bureau of Customs	6Mbps
		Sub- Port of Siain , Plaridel, Quezon	
		Tel/fax No. 042-3029704	
21	Sub-Port of Bauan	Bureau of Customs	6Mbps
		Bauan Int’l. Port Inc.- One-Stop-Shop (BIPI-OSS), Bauan Int’l Port Inc.	
		Brgy. San Roque, Bauan Batangas	
22	Mactan	Bureau of Customs Building	6Mbps
		Mactan-Cebu International Airport Cargo Area	
		Lapu Lapu City 6015	
23	Customs Peza Clearing Office (CPCO)	MEZ1 Compound, Lapu-Lapu City.	6Mbps
		Bureau of Customs	
24	Sub-Port of Dumagute	Address: Port of Dumaguete, Port Area	6Mbps
		Tel No. 035-4223361	
25	Sub-Port of ILOILO	BOC Building, Port of ILOILO,	6Mbps
		COR MUELLE LONEY, GEN MACARIO,	
		PERALTA ST. ILOILO CITY	
26	Sub-Port of Pulupandan	Bureau of Customs	6Mbps
		Sub-Port of Pulupandan	
		Wescosita Street, Zone 5	
		Pulupandan, Negros Occidental	
27	Port of Tacloban	Trece Martirez St. Tacloban City	6Mbps
28	Sub-port of Isabel	Mabini St., Isabel, Leyte	6Mbps
		With Bayantel and Globe DSL connections	

29	Sub-port of Catbalogan	McKinley St., Catbalogan, Samar (No DSL connection yet)	6Mbps
30	Sub-Port of Dadiangas	Makar Wharf, Gen. Santos City	6Mbps
31	Port of Surigao	Bureau of Customs	6Mbps
		PPA Compound, Port Area, Surigao City	
		Telefax No.: (086) 826-8678	
		Tel. No.: (086) 232-7535	
32	Sub-Port of Nasipit (Masao)	Bureau of Customs	6Mbps
		Rudy Tiu Building, Montilla Street	
		Butuan City	
		Telefax Nos: (085) 342-5576	
		Tel. No.: (085) 341-5140	
33	Sub-Port of Bislig	Bureau of Customs	6Mbps
		Gomez Building, Mangagoy, Bislig City	
		Telefax No.: (086) 853-2209	
34	Port of Cagayan de Oro	Bureau of Customs	6Mbps
		Corrales Extension, Macabalan	
		Cagayan de Oro City	
35	Port of Iligan	Bureau of Customs	6Mbps
		Sub-port of Iligan, Port Area, Iligan City	
36	Port of Ozamis	Bureau of Customs	6Mbps
		Casa Esperanza Bldg.	
		Bernad Ave., Ozamis City	
37	Port of MCT-PHIVIDEC	Bureau of Customs	6Mbps
		Mindanao Container Terminal	
		Phividec Industrial Estate	
		Tagoloan, Misamis Oriental	
38	Port of Zamboanga	Bureau of Customs - XIth Collection DISTRICTS	6Mbps
		Port of Zamboanga, Zamboanga City	
39	Sub-Port of Zamboanga International Airport (ZIA)	Bureau of Customs	6Mbps
		Sub-Port of Zamboanga International Airport	
		Baliwasan, Zamboanga City	
40	Sub-Port of Basilan	Bureau of Customs	6Mbps
		Sub-Port of Basilan, Isabela City, Basilan	
41	Sub-Port of Jolo	Bureau of Customs	6Mbps
		Sub-Port of Jolo, Port Area, Jolo, Sulu	
42	Sub-Port of Bongao	Bureau of Customs	6Mbps

		Datu Halun St., Bongao, Tawi-Tawi	
43	Sub Port Of Kalibo		6mbps

VI. REQUIRED NETWORK LAYOUT:



I hereby certify to comply with all the above Technical Specifications.

Name of Company/Bidder	**Signature Over Printed Name of Representative**	**Date**

Section VIII. Bidding Forms

TABLE OF CONTENTS

BID FORM…………………………………………………………………….. 52

STATEMENT OF SINGLE LARGEST COMPLETED CONTRACT WHICH IS similar in nature..53

LIST OF ALL ONGOING GOVERNMENT & PRIVATE CONTRACTS INCLUDING CONTRACTS AWARDED BUT NOT YET STARTED 54

CONTRACT AGREEMENT FORM 55

OMNIBUS SWORN STATEMENT..56

BID SECURING DECLARATION...59

Bid Form

Date: ____________________

To: [name and address of Procuring Entity]
Gentlemen and/or Ladies:

Having examined the Bidding Documents including Bid Bulletin Numbers *[insert numbers]*, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to the BOC, our Goods for the project, **Managed High-Speed Network and Internet Connectivity**, in conformity with the said Bidding Documents for the sum of PhP____________________________ (in words and in figure).

Item	Description	Unit Cost (inclusive of VAT)	TOTAL COST (inclusive of VAT)
1	Delivery, installation and commissioning of all hardware, software and other equipment for all sites		
2	Implementation of the network and internet services		
		TOTAL	

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

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

We agree to abide by this Bid for the Bid Validity Period specified in **BDS** provision for **ITB** Clause 18.2 and it shall remain binding upon us and may be accepted 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 or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements as per **ITB** Clause 5 of the Bidding Documents.

Dated this ________________ day of ________________ 2015.

______________________________ ______________________________
[signature] *[in the capacity of]*

Duly authorized to sign Bid for and on behalf of ______________________________

Statement of Single Largest Completed Contract which is similar in nature

(indicate only one)

Business Name: ____

Business Address: ____

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

Submitted by : _____________________________________

(Printed Name & Signature)

Designation : _____________________________________

Date : _____________________________________

Note: Cut-off date is October 30, 2015**.**

List of all Ongoing Government & Private Contracts including Contracts awarded but not yet started

Business Name: ____
Business Address: ____

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

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

Date : ____

Instructions:

i. State all ongoing contracts including those awarded but not yet started within five (5) years (government and private contracts, which may be similar or not similar to the project being bidded) prior to November 13, 2015**.**

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

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

Contract Agreement Form

THIS AGREEMENT made the _____ day of __________ 2015 between *[name of PROCURING ENTITY]* of the Philippines (hereinafter called "the Entity") of the one part and *[name of Supplier]* of *[city and country of Supplier]* (hereinafter called "the Supplier") of the other part:

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

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

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

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

   (a) the Bid Form and the Price Schedule submitted by the Bidder;
   (b) the Schedule of Requirements;
   (c) the Technical Specifications;
   (d) the General Conditions of Contract;
   (e) the Special Conditions of Contract; and
   (f) the Entity's Notification of Award.

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

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

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

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

Signed, sealed, delivered by ________________ the ________________ (for the Supplier).

Omnibus Sworn Statement

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF ______) S.S.

AFFIDAVIT

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

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

   If a sole proprietorship: I am the sole proprietor 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 of *[Name of Bidder]*, I have full power and authority to do, execute and perform any and all acts necessary to represent it in the bidding for *[Name of the Project]* of the *[Name of the Procuring Entity]*;

   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 and/or to represent the *[Name of Bidder]* in the bidding as shown in the attached *[state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate issued by the corporation or the members of the joint venture)]*;

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;

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: I am not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

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

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

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

8. *[Name of Bidder]* is aware of and has undertaken the following responsibilities as a Bidder:

   a) Carefully examine all of the Bidding Documents;

   b) Acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;

   c) Made an estimate of the facilities available and needed for the contract to be bid, if any; and

   d) Inquire or secure 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.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 2015 at ____________, Philippines.

____
Bidder's Representative/Authorized Signatory

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

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

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

Doc. No. ___
Page No. ___
Book No. ___
Series of ___

REPUBLIC OF THE PHILIPPINES)
CITY OF ________________________) S.S.
x---x

BID-SECURING DECLARATION

Invitation to Bid/Request for Expression of Interest No.[1]: *[Insert reference number]*

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

I/We[2], 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 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[3], 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 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;

   (b) I am/we are declared as the bidder with the Lowest Calculated and Responsive Bid/Highest Rated and Responsive Bid[4], and I/we have furnished the performance security and signed the Contract.

[1] Select one and delete the other.
[2] Select one and delete the other. Adopt same instruction for similar terms throughout the document.
[3] Issued by the GPPB through GPPB Resolution 03-2012 on 27 January 2012.
[4] Select one and delete the other.

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'S
AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

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

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

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

Doc. No. ___
Page No. ___
Book No. ___
Series of ___