# PHILIPPINE BIDDING DOCUMENTS

# Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center

## Project ID: LRA SPBAC-2024-01

Government of the Republic of the Philippines

**Sixth Edition**
**July 2020**

# Preface

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

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

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

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

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

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

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

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

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

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

# Table of Contents

# *Glossary of Acronyms, Terms, and Abbreviations*

**ABC** – Approved Budget for the Contract.

**BAC** – Bids and Awards Committee.

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

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

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

**BIR** – Bureau of Internal Revenue.

**BSP** – Bangko Sentral ng Pilipinas.

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

**CDA -** Cooperative Development Authority.

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

**CIF –** Cost Insurance and Freight.

**CIP –** Carriage and Insurance Paid.

**CPI –** Consumer Price Index.

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

**DTI** – Department of Trade and Industry.

**EXW** – Ex works.

**FCA** – "Free Carrier" shipping point.

**FOB** – "Free on Board" shipping point.

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

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

**GFI** – Government Financial Institution.

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

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

**GOP** – Government of the Philippines.

**GPPB** – Government Procurement Policy Board.

**INCOTERMS –** International Commercial Terms.

**Infrastructure Projects** – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national

buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

**LGUs –** Local Government Units.

**NFCC –** Net Financial Contracting Capacity.

**NGA –** National Government Agency.

**PhilGEPS -** Philippine Government Electronic Procurement System.

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

**PSA –** Philippine Statistics Authority.

**SEC –** Securities and Exchange Commission.

**SLCC –** Single Largest Completed Contract.

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

**UN –** United Nations.

# *Section I. Invitation to Bid*

## Notes on the Invitation to Bid

The Invitation to Bid (IB) provides information that enables potential Bidders to decide whether to participate in the procurement at hand. The IB shall be posted in accordance with Section 21.2 of the 2016 revised IRR of RA No. 9184.

Apart from the essential items listed in the Bidding Documents, the IB should also indicate the following:

a. The date of availability of the Bidding Documents, which shall be from the time the IB is first advertised/posted until the deadline for the submission and receipt of bids;

b. The place where the Bidding Documents may be acquired or the website where it may be downloaded;

c. The deadline for the submission and receipt of bids; and

d. Any important bid evaluation criteria (*e.g.*, the application of a margin of preference in bid evaluation).

The IB should be incorporated in the Bidding Documents. The information contained in the IB must conform to the Bidding Documents and in particular to the relevant information in the Bid Data Sheet.

REPUBLIKA NG PILIPINAS
KAGAWARAN NG KATARUNGAN
**PANGASIWAAN SA PATALAAN NG LUPAIN**
**(LAND REGISTRATION AUTHORITY)**
East Avenue cor. NIA Road, Quezon City

# INVITATION TO BID FOR Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center

1. The **Land Registration Authority (LRA)** through the General Appropriations Act for 2024 (Republic Act No. 11975) intends to apply the sum **TWO HUNDRED SEVENTY TWO MILLION PESOS ONLY (272,000,000.00),** inclusive of VAT being the ABC to payments under the contract for the **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center** with **Project ID No. LRA SPBAC-2024-01.** Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The **LRA** now invites bids for the above Procurement Project. Delivery of the Goods and Services shall be within **ninety (90) calendar days** upon receipt of the Notice To Proceed.

   Bidders should have completed, within the past **five (5) years** from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

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

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

4. Prospective Bidders may obtain further information from **LRA-Special Bids and Awards Committee (BAC) Secretariat** through the contact details given below and inspect the Bidding Documents as posted on the websites of the LRA and the Philippine Government Electronic Procurement System (PhilGEPS)

5. A complete set of Bidding Documents may be acquired by interested Bidders on **November 20, 2024 to December 10, 2024** from the given address upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of **Fifty Thousand Pesos Only (Php 50,000.00)** at the LRA cashier located at the One-Stop-Shop (OSS). The **LRA** shall allow the bidder to present its proof of payment for the fees by presenting it in person.

6. The **LRA** will hold a **Pre-Bid Conference[1] on November 28, 2024, 10:00 AM** *at* **4th Floor, LRA Conference Room, LRA Building, East Avenue corner NIA Road, Diliman, Quezon City** which shall be open to prospective bidders.

7. **Bids must be duly received** by the BAC Secretariat through manual submission at the office address indicated below, on or before **December 10, 2024 09:00 AM. Late bids shall not be accepted.**

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

9. Bid opening shall be on **December 10, 2024 10:00 AM at 4th Floor, LRA Conference Room, LRA Building, East Avenue corner NIA Road, Diliman, Quezon City.** Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

   **For the purpose of constituting a quorum**, either the physical and virtual presence of the BAC members shall be considered pursuant to GPPB Resolution No. 09-2020.

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

11. For further information, please refer to:

    a) **Mr. ANTHONY BRANDON G. JUAN**
    SPBAC Secretariat Assistant Head
    2nd Floor, Information Management Center (IMC) Building
    Mobile No. 0968-8587425

    b) **Ms. GRACE-ANN A. LICO**
    SPBAC Secretariat Member
    2nd Floor, Information Management Center (IMC) Building
    Mobile No. 0995-1981129

12. For viewing and downloading of Bidding Documents:

    http://notices.philgeps.gov.ph/
    https://lra.gov.ph/bids-oppurtunities/

*Date Issuance of Bidding Documents* *20 November 2024 at Quezon City*

**Atty. SALVALENTE THADDEUS B. ELIZALDE**
Chairperson, LRA Special Bids and Awards Committee
East Avenue corner NIA Road, Diliman, Quezon City

---

# *Section II. Instructions to Bidders*

## Notes on the Instructions to Bidders

This Section on the Instruction to Bidders (ITB) provides the information necessary for bidders to prepare responsive bids, in accordance with the requirements of the Procuring Entity. It also provides information on bid submission, eligibility check, opening and evaluation of bids, post-qualification, and on the award of contract.

## 1. Scope of Bid

The Procuring Entity**, Land Registration Authority (LRA)** wishes to receive Bids for the **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center** with identification number **LRA SPBAC-2024-01**

The Procurement Project (referred to herein as "Project") is composed of one (1) lot, the details of which are described in Section VII (Technical Specifications).

## 2. Funding Information

2.1. The GOP through the source of funding as indicated below for FY 2024 in the amount of **TWO HUNDRED SEVENTY TWO MILLION PESOS ONLY (272,000,000.00),** inclusive of VAT.

2.2. The source of funding is the General Appropriations Act of 2024 (Republic Act No. 11975)

## 3. Bidding Requirements

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

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

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

## 4. Corrupt, Fraudulent, Collusive, and Coercive Practices

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

## 5. Eligible Bidders

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

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

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

For the procurement of Non-expendable Supplies and Services: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.

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

## 6. Origin of Goods

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

## 7. Subcontracts

The Procuring Entity has prescribed that: **Subcontracting is not allowed.**

## 8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on **November 28, 2024, 10:00AM at 4th Floor, LRA Conference Room, LRA Building, East Avenue corner NIA Road, Diliman, Quezon City**

## 9. Clarification and Amendment of Bidding Documents

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

## 10. Documents comprising the Bid: Eligibility and Technical Components

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

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within **five (5) years** prior to the deadline for the submission and receipt of bids.

10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must

be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

## 11. Documents comprising the Bid: Financial Component

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

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

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

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

## 12. Bid Prices

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

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

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

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

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

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

b. For Goods offered from abroad:

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

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

## 13. Bid and Payment Currencies

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

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

*].*

## 14. Bid Security

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

14.2. The Bid and bid security shall be valid until **April 09, 2025 or one hundred twenty (120) calendar days from Bid Opening**. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

## 15. Sealing and Marking of Bids

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

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

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

## 16. Deadline for Submission of Bids

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

[2] In the case of Framework Agreement, the undertaking shall refer to entering into contract with the Procuring Entity and furnishing of the performance security or the performance securing declaration within ten (10) calendar days from receipt of Notice to Execute Framework Agreement.

## 17. Opening and Preliminary Examination of Bids

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

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

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

## 18. Domestic Preference

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

## 19. Detailed Evaluation and Comparison of Bids

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

19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB** Clause 14 shall be submitted for each lot or item separately.

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

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

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

committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

## 20. Post-Qualification

20.2. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

## 21. Signing of the Contract

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

# *Section III. Bid Data Sheet*

## Notes on the Bid Data Sheet

The Bid Data Sheet (BDS) consists of provisions that supplement, amend, or specify in detail, information, or requirements included in the ITB found in Section II, which are specific to each procurement.

This Section is intended to assist the Procuring Entity in providing the specific information in relation to corresponding clauses in the ITB and has to be prepared for each specific procurement.

The Procuring Entity should specify in the BDS information and requirements specific to the circumstances of the Procuring Entity, the processing of the procurement, and the bid evaluation criteria that will apply to the Bids. In preparing the BDS, the following aspects should be checked:

a. Information that specifies and complements provisions of the ITB must be incorporated.

b. Amendments and/or supplements, if any, to provisions of the ITB as necessitated by the circumstances of the specific procurement, must also be incorporated.

# Bid Data Sheet

| ITB Clause | |
|---|---|
| 5.3 | For this purpose, contracts similar to the Project shall be:<br><br>a. Refer to **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center**<br><br>b. completed within five (5) years prior to the deadline for the submission and receipt of bids. |
| 7.1 | ***Subcontracting is not allowed.*** |
| 12 | Not Applicable |
| 14.1 | The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts:<br>a. The amount of not less than **Php 5,440,000.00** *(2%) of ABC]*, if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or<br><br>b. The amount of not less than **Php 13,600,000.00** *(5%) of ABC]* if bid security is in Surety Bond. |
| 19.3 | The Project, **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center** with ABC of **TWO HUNDRED SEVENTY TWO MILLION PESOS ONLY (Php 272,000,000.00),** VAT inclusive.<br><br>The computation of a prospective bidder's NFCC must be at least equal to the ABC to be bid, pursuant to Section 23.4.1.1 of the 2016 Revised IRR of RA No. 9184. |
| 20.2 | Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit it latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law. |
| | Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Single/Lowest Calculated Bid, the Bidder shall submit ALL of the following post-qualification requirements:<br>1. Photocopy of Single Largest Completed Contract or Purchase Order<br>2. The corresponding proof of completion which could either be:<br>a) Certificate of Final Acceptance / Completion from the bidder's client; or<br>b) Official Receipt or Sales Invoice of the bidder covering the full amount of the contract<br><br>3. Latest Income & Business Tax Returns, filed and paid through the Electronic Filing and Payments System (eFPS) and other appropriate licenses and permits required by law.<br>4. Valid Mayor's / Business Permit for FY 2024. |
| 21.2 | **Other Documentary Submission (to be submitted during bid opening)**<br><br>1. **Manufacturer's Authorization Form (MAF) / Letter of Support** from the Manufacturer for the following components:<br>a. Infrastructure Development<br>1. Equipment/Modular Racks |

| | |
|---|---|
| | 2. Environmental Monitoring System<br>3. Electrical Monitoring System<br>4. Door Access System<br>b. Power and Cooling Solutions<br>1. Uninterruptible Power Supply (UPS)<br>2. Power Distribution Units (PDUs)<br>3. Precision Air-Conditioning Units (PACU)<br>c. Security (Physical & Data) and Safety Systems<br>1. Fire Detection, Alarm, and Suppression System<br>2. CCTV System<br>3. Managed Cyber Security Services<br>d. IT Infrastructure and Services<br>1. Servers, Licenses, Storage, and Hyper-Converged Infrastructure<br>2. (HCI) Services<br>3. Network Switches and Devices<br>4. Active Directory<br>5. Managed Kubernetes System and DBAAS System<br>6. Data Center Backup Solution<br>7. Data Center NAS Storage<br>**2. Project Proposal and Plan**<br>The winning bidder shall submit a comprehensive Project Proposal and Plan that includes the following key elements:<br>a. **Timeline**: A detailed schedule outlining the phases of implementation, key milestones, and completion dates.<br>b. **Implementation Plan**: A step-by-step strategy for executing the project, including resource allocation, methodologies and risk management.<br>c. **Hardware**: A complete list of all hardware to be delivered, including specifications, quantities and warranties.<br>d. **Services**: A breakdown of all services to be provided such as installation, configuration, technical support and maintenance.<br>e. **Software Subscription**: Clear details on the software deliverables, subscription terms, and activation timelines, including provisions for open-source software support, where applicable<br>3. **Manpower Requirements** for the project as listed in Item 16 “Bidder’s Qualification”. |

# *Section IV. General Conditions of Contract*

## Notes on the General Conditions of Contract

The General Conditions of Contract (GCC) in this Section, read in conjunction with the Special Conditions of Contract in Section V and other documents listed therein, should be a complete document expressing all the rights and obligations of the parties.

Matters governing performance of the Supplier, payments under the contract, or matters affecting the risks, rights, and obligations of the parties under the contract are included in the GCC and Special Conditions of Contract.

Any complementary information, which may be needed, shall be introduced only through the Special Conditions of Contract.

## 1. Scope of Contract

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

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

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

## 2. Advance Payment and Terms of Payment

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

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

## 3. Performance Security

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

## 4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC**, **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.

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

## 5. Warranty

5.1 In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.

5.2 The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

## 6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

# *Section V. Special Conditions of Contract*

## Notes on the Special Conditions of Contract

Similar to the BDS, the clauses in this Section are intended to assist the Procuring Entity in providing contract-specific information in relation to corresponding clauses in the GCC found in Section IV.

The Special Conditions of Contract (SCC) complement the GCC, specifying contractual requirements linked to the special circumstances of the Procuring Entity, the Procuring Entity's country, the sector, and the Goods purchased. In preparing this Section, the following aspects should be checked:

a. Information that complements provisions of the GCC must be incorporated.

b. Amendments and/or supplements to provisions of the GCC as necessitated by the circumstances of the specific purchase, must also be incorporated.

However, no special condition which defeats or negates the general intent and purpose of the provisions of the GCC should be incorporated herein.

# Special Conditions of Contract

| GCC Clause | |
|---|---|
| 1 | *[List here any additional requirements for the completion of this Contract. The following requirements and the corresponding provisions may be deleted, amended, or retained depending on its applicability to this Contract:]*<br><br>**Delivery and Documents –**<br><br>For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows:<br><br>"The delivery terms applicable to the Contract are DDP delivered at **LRA Building, East Avenue corner NIA Road, Diliman, Quezon City** in accordance with INCOTERMS."<br><br>*[For Goods supplied from within the Philippines, state:*] "The delivery terms applicable to this Contract are delivered *at* **LRA Building, East Avenue corner NIA Road, Diliman, Quezon City.** Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination."<br><br>Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements).<br><br>For purposes of this Clause the Procuring Entity's Representative at the Project Site is the **Property and Supply Section of the LRA.**<br><br>**Incidental Services –**<br><br>The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements:<br><br>a. performance or supervision of on-site assembly and/or start-up of the supplied Goods;<br>b. furnishing of tools required for assembly and/or maintenance of the supplied Goods;<br>c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods;<br>d. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and |

| | |
|---|---|
| | e. training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.<br><br>The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.<br><br>**Spare Parts –**<br><br>The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:<br><br>1. such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and<br><br>2. in the event of termination of production of the spare parts:<br><br>i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and<br><br>ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.<br><br>The spare parts and other components required are listed in **Section VI (Schedule of Requirements)** and the costs thereof are included in the contract price.<br><br>The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods for a period of three (3) years<br><br>Spare parts or components shall be supplied as promptly as possible, but in any case, within one (1) month of placing the order. |
| | **Packaging –**<br><br>The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the |

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

<table>
<tr><td></td><td>The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination.<br><br>Intellectual Property Rights –<br><br>The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.</td></tr>
<tr><td></td><td>Regular and Recurring Services –<br>“The contract for regular and recurring services shall be subject to a renewal whereby the performance evaluation of the service provider shall be conducted in accordance with Section VII. Technical specifications.”</td></tr>
<tr><td>2.2</td><td>“The terms of payment shall be as follows: Progress Billing Schedule<br><br>
<table>
<tr><th>Milestone</th><th>Particulars</th><th>Payment %</th><th>Document Required for Payments</th></tr>
<tr><td>1</td><td>Mobilization/ Project Planning</td><td>15%</td><td>Submission of Project Plan</td></tr>
<tr><td>2</td><td>Civil Works</td><td>25%</td><td>Submission of As Built Plans (Civil & Electrical)</td></tr>
<tr><td>3</td><td>Equipment Delivery</td><td>35%</td><td>Delivery Receipts duly received by LRA</td></tr>
<tr><td>4</td><td>System Configuration</td><td>15%</td><td>System Testing and Commissioning report</td></tr>
<tr><td>5</td><td>Knowledge Transfer & Final Acceptance</td><td>10%</td><td>Knowledge Transfer Certificates, Warranty Certificates, Final Acceptance Report</td></tr>
</table>
</td></tr>
<tr><td>4</td><td>The inspections and tests that will be conducted are:<br><br>• The acceptability of the Goods vis-à-vis its compliance with the technical specifications will be done by LRA upon delivery of the goods.</td></tr>
</table>

# *Section VI. Schedule of Requirements*

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

| Item Number | Description | Quantity | Delivered, Weeks/Months |
|---|---|---|---|
| 1 | **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center** | One (1) lot | **Ninety (90) calendar days** upon receipt of the Notice To Proceed |

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

| _____ | _____ | _____ |
|---|---|---|
| **Name of Company / Bidder** | **Signature Over Printed Name** | **Date** |

# *Section VII. Technical Specifications*

## Technical Specifications

| Item | Specification | Statement of Compliance |
|---|---|---|
| A. | **Project Components** | |
| | The Data Center Project will consist of the following key components and deliverables:<br><br>**1. Infrastructure Development**<br>a. Site Preparation (Civil, Mechanical and Electrical Works)<br>b. Structured Cabling<br>c. Equipment / Modular Rack(s)<br>d. Environmental Monitoring System<br>e. Energy Monitoring System<br>f. Door Access System<br><br>**2. Power and Cooling Solutions**<br>a. Uninterruptible Power Supply (UPS)<br>b. Power Distribution Units (PDUs)<br>c. Precision Air-Conditioning Units<br>d. Comfort Cooling<br>e. Backup Power Generator (Diesel)<br><br>**3. Security (Physical & Data) and Safety Systems**<br>a. Fire Detection, Alarm, and Suppression System<br>b. CCTV System<br>c. Managed Cyber Security Services<br>d. Endpoint Security<br><br>**4. IT Infrastructure and Services**<br>a. Servers, Software Licenses, and Hyper Converged Infrastructure (HCI)<br>b. Active Directory (Installation, Configuration, Testing)<br>c. Web Server<br>d. SD-WAN and Perimeter Firewall<br>e. Network Switches and Devices<br>f. Web Application Firewall with Server Load Balancers<br>g. Managed Kubernetes and DBASS System<br><br>**5. Operational Management and Support**<br>a. Construction of NOC/SOC Center<br><br>**6. Disaster Recovery and Business Continuity**<br>a. Backup Server and Backup Software Solution<br>b. Backup Repository<br><br>**7. Data Center Storage Solution**<br>a. Data Center NAS Storage | |

| | | |
|---|---|---|
| B. | **Technical Specifications** | |
| 1 | **Infrastructure Development** | |
| 1 - A | **Component 1-A - Infrastructure Development** - Site Preparation (Civil, Mechanical and Electrical Works)<br><br>**General Scope**<br>The contractor shall renovate the existing LRA Office Space area following the proposed layout as specified under the Annex A.<br><br>1. Floor Area: This is the approximate floor area per room<br>1.1. Server Room – Approximately 100 m2<br>1.2. NOC/SOC Room – Approximately 50 m2<br>2. Site Preparation: The contractor shall conduct a structural analysis of the selected site to verify its capacity to support the Server Room effectively.<br>3. Enclosure: The contractor shall install Concrete Hollow Block (CHB) walls to enclose the glass windows and door of the server room and NOC/SOC Room as required by the design. Additionally, the contractor will demolish any existing walls as necessary to facilitate expansion for the data center<br>4. Painting: The contractor shall paint all new wall installations and re-paint refurbished existing walls, including refurbishment of existing ceiling affected by the improvement works.<br><br>**Civil Works**<br>The Contractor shall provide the following services for LRA:<br><br>5. Demolition works includes removal of existing wall, existing ceiling at Server Room, NOC Room, Storage Room & IT Room, including hauling of debris to the designated area including installation of blue sack to prevent the dust from spreading the area<br>6. Construction of dry-wall partition between Server Room and IT Room from floor to ceiling using a double wall 12mm thick gypsum board on metal studs with 2" thick rockwool insulation in between the gypsum board<br>7. Construction of dry-wall partition on metal studs between NOC Room and existing Storage Room from floor slab to ceiling using a double wall 12mm thick gypsum board on metal studs with 2" thick rockwool insulation in between the gypsum board<br>8. Construction of glass frameless partition from zocalo to ceiling between Server Room and Hallway using 12mm thick tempered glass<br>9. Construction of glass frameless partition from floor to ceiling between NOC Room and Hallway using 12mm thick tempered glass | |

| | | |
|---|---|---|
| | 10. Construction of dry-wall partition between NOC Room and existing Room from floor slab to ceiling using a double wall 12mm thick gypsum board on metal studs with 2" thick rockwool insulation in between the gypsum board to cover the existing wall<br>11. Construction of dry-wall partition on metal studs between NOC Room and existing Storage Room from floor slab to ceiling using a double wall 12mm thick gypsum board on metal studs with 2" thick rockwool insulation in between the gypsum board<br>12. Construction of dry-wall partition on metal studs between existing Storage Room and existing Room from floor slab to ceiling using a double wall 12mm thick gypsum board on metal studs with 2" thick rockwool insulation in between the gypsum board to cover the existing wall<br>13. Construction of dry-wall partition on metal studs between IT Room and existing Room from floor slab to ceiling using a double wall 12mm thick gypsum board on metal studs with 2" thick rockwool insulation in between the gypsum board to cover the existing wall<br>14. Fabrication and installation of metal door (900mm W + 300mm W x 2400mm H) complete with heavy-duty door lock and door closer<br>15. Supply and installation of metal door (900mm W x 2100mm H) complete with heavy-duty door lock and door closer from NOC Room to Storage Room<br>16. Supply and installation of metal door (900mm W x 2100mm H) complete with heavy-duty door lock and door closer from Storage Room to IT Room<br>17. Supply and installation of tempered glass door (1000mm W x 2100mm H) complete with heavy duty door lock and door closer<br>18. Supply and installation of 1/2" thick fixed gypsum board ceiling on metal studs, includes Server Room, NOC Room, Storage Room & IT Room<br>19. Supply & Installation of raised flooring, 1000 PSI, 8" high, 60cm x 60cm, high pressure laminate, complete with stringers, pedestal head and pedestal base<br>20. Fabrication and installation of metal ramp with non-skid rubber matting on top to be installed at the Main Entrance at Server Room<br>21. Supply & Installation of anti-static vinyl tiles, 60cm, 3mm thick including installation vinyl adhesive and grounding system for NOC Room, Storage Room & IT Room<br>22. Supply and installation of rubber-based board inside NOC room<br>23. Construction of zocalo wall using CHB, 4" thick, 8 " high x 800cm between Server Room and the Hallway<br>24. Construction of metal enclosure to existing electrical panel at the Main Entrance, NOC Room | |

| | | |
|---|---|---|
| | 25. Misc materials such as blue sack to cover the existing equipment and furniture to prevent dust including general cleaning<br><br>**Mechanical Works**<br>The Contractor shall design and build provision for cooling for the Data Center with a corresponding back-up system.<br><br>26. The Contractor shall deliver, install, configure and commission two (2) units of 300mm x 1000mm flexible cabinet type cooling system, 32kW capable at the Data Center.<br>27. The Contractor shall deliver, install, and commission a two (2) 2.5HP wall mounted split type inverter, at the Data Center and/or SOC room<br>28. The Contractor shall fabricate and install outdoor unit supports.<br>29. The Contractor shall install and layout the refrigerant piping system, condensate drain & humidifier line system, including required electrical works and electrical controls for A/C equipment.<br>30. The Contractor shall install and layout piping from indoor unit to the nearest tapping point including insulation and support<br>31. The Contractor shall include the power supply and control wirings including conduit and circuit breakers<br><br>**Electrical Works**<br>The Contractor shall design and build power wiring requirements of the Data Center for cooling, and Network Equipment and Components:<br><br>1. Supply and install of generator set dedicated to data center. The winning bidder shall supply genset house to secure and protect the equipment<br>2. Supply and install of automatic transfer switch<br>3. Utilize existing main distribution panel and provide replacement circuit breakers<br>4. The contractor shall supply and install a step-up transformer to deliver the required voltage for the Data Center loads.<br>5. The contractor shall supply and install a transient voltage surge suppressor to protect the electrical systems.<br>6. The contractor shall supply and install circuit breakers for upstream, transformer and various data center loads<br>7. The contractor shall supply and install panel boards as power distribution for data center loads<br>8. The contractor shall supply and install panel boards for UPS systems as power distribution for rack equipment | |

| | | |
|---|---|---|
| | 9. The contractor shall supply and install feeder wires from tapping point, upstream to downstream distribution to electrically interconnect all equipment and devices<br>10. The contractor shall supply and install twist lock outlets (male & female) at the rack units<br>11. The contractor shall supply and install lighting fixtures, LED troffer lights to provide sufficient illumination inside the Data Center<br>12. The contractor shall supply and install duplex convenience outlets at the Data Center and NOC room<br>13. The contractor shall supply and install cable trays to organize and manage cables.<br>14. The contractor shall supply and install rough-ins with appropriate hangers and supports for secure installations.<br>15. The contractor shall supply and install a grounding system for Data Center racks and equipment.<br>16. The contractor shall conduct insulation resistance (IR) tests, functionality testing, and commissioning of the systems.<br>17. The contractor shall perform termination of wires to ensure secure connections.<br>18. The contractor shall execute startup, testing, and commissioning configuration as needed<br>19. Supply and installation of wires for generator set to manual transfer switch (MTS)<br>20. Supply and installation of feeder wires from manual transfer switch (MTS) to main panel<br>21. Termination, testing and commissioning of generator set | |
| 1 -B | **Component 1-B - Infrastructure Development – Structured Cabling**<br><br>**Scope of Works**<br>Supply and installation of Cat6 UTP cable for CCTV cameras and door access component inside the Data Center and NOC room<br><br>1. Supply and installation of conduit with proper hangers and supports for CCTV cameras and door access component<br>2. Supply and installation of passive components such as UTP panels, cable managers, patch cords and connectors<br>3. End to end termination and patching<br>4. End to end harnessing, tagging and testing<br>5. Assembly and mounting of CCTV cameras and door access components at locations specified in the plan<br>6. Supply and installation of patch panel, cable managers and patch cords at racks | |

| | | |
|---|---|---|
| | **Quantity**<br>1. UTP Cat6 Cable – One (1) lot<br>2. UTP Patch Panel - One (1) lot<br>3. UTP Cat6 Patch Cords - One (1) lot<br>4. UTP Cat6a Patch Cords - One (1) lot<br>5. Multimode OM3 Fiber Patch Cords - One (1) lot<br><br>**Specifications**<br>1. **UTP Cat6 Cable**<br>a. Conductors shall be solid, annealed and bare copper with a diameter of AWG23~24 and minimum acceptable diameter shall be 0/485mm<br>b. The insulation shall be uniform and shall not have any defects; and<br>c. The diameter over the insulation shall be maximum of 1.22m<br>d. Three (3) years warranty on parts and services.<br>**4. UTP Patch Panel**<br>a. Patch panel must be in 24ports configuration<br>b. Can be mounted on 19" standard rack and must be 1RU<br>c. Easy handling by hinged wire management<br>d. Must be RoHS compliant<br>e. Must have Cat6 information outlets<br>f. Three (3) years warranty on parts and services.<br>**5. UTP Cat6 Patch Cords**<br>a. Patch cords shall consist of 26AWG wire or other, each four pair twisted at a different lay length<br>b. Must be in T568B wiring<br>c. Must be fully booted and have clip protection for simple removal; and<br>d. Must offer a high-performance alternative to satin modular line cords where crosstalk or distance may be considerations.<br>e. Three (3) years warranty on parts and services.<br>**6. UTP Cat6a Patch Cords**<br>a. Patch cords consist of 24AWG~26AWG wire, each four pair twisted at a different lay length<br>b. Must be in T568A or T568B wiring<br>c. Must be fully booted and have clip for protection for simple removal; and<br>d. Must offer a high-performance alternative to satin modular line cords where crosstalk or distance may be considerations. | |

| | | |
|---|---|---|
| | e. Three (3) years warranty on parts and services.<br>**7. Multimode OM3 Fiber Patch Cords**<br>a. Must have insertion loss and return loss is based on ANSI/TIA-568-C-3 requirements<br>b. Cable diameter must be Jumper Cord (1.8~3.0mm), Cable with One Side Connector (0.9~3.0mm) available<br>c. Link Length must be up to 300m (OM3)<br>d. Must have Ceramic (Zirconia) material of ferrules<br>e. Must be IEC 61754 & EN 50377 Standards compliant<br>f. Must be TIA-604 (FOCIS) Standards compliant<br>g. Must have High Impact Flame Retardant Plastic, UL 94V-0~2 Rated<br>h. Must have PVC or LSZH cable jacket<br>i. Three (3) years warranty on parts and services. | |
| 1-C | **Component 1-C - Infrastructure Development – Equipment / Modular Server Rack(s)**<br><br>**Scope of Works** - Supply, installation, configuration, testing and commissioning<br><br>**Quantity:** One (1) Lot<br><br>**Specifications (Rack Cabinet)**<br>1. Must be floor-mounted, 42U high, 600mm wide, 1200mm depth<br>2. Must have a frame anodized aluminum extrusion profile<br>3. Must have the option to shipped unassembled<br>4. Must have a maximum static load of up to 2000 kg<br>5. Tempered glass front door must have a swing handle multi-point lock<br>6. Must include 19” depth-adjustable mounting rails<br>7. Must have a color of RAL7035 or RAL9005<br>8. Must comply to RoHs and UL<br>9. Must have an Authorized Service Partner/Center in Metro Manila.<br>10. Three (3) years warranty on parts and services.<br><br>**Specifications (Rack Access Control)**<br>1. Must provide access control and management to all your cabinet doors or normal doors as well<br>2. Must prevents unauthorized access denying the access | |

| | | |
|---|---|---|
| | 3. Must allow doors to be opened using a proximity card or keypad code<br>4. Must automatically generate a visual alert through red & blue led indicators<br>5. Must records all the security information you need every time the door of a server cabinet is opened – by whom, where, when<br>6. Must include RS485 to TCP/IP Converter & Controller<br>7. Must include software with license; and<br>8. Must include USB Keyfob/card issuer.<br>9. Three (3) years warranty on parts and services. | |
| 1-D | **Component 1-D - Infrastructure Development – Environmental Monitoring System (EMS)**<br><br>**Scope of Works** - Supply, installation, configuration, testing and commissioning<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. Must be able to measure, monitor, record, and control; Environmental variables such as temperature, humidity, smoke, air flow<br>2. Must not need any Computer/Server connection and can work on its own. It must be compatible with industrial standard sensors and provides reliable service<br>3. Must have the ability to extend the coverage of your EMS system using the sensor multiplexer HUB, which will connect to the sensor port<br>4. Must have integrated temperature and humidity sensor<br>5. Must have integrated water leak sensor<br>6. Three (3) years warranty on parts and services. | |
| 1-E | **Component 1-E - Infrastructure Development – Energy Monitoring System**<br><br>**Scope of Works**<br>1. Installation of Energy Monitoring System<br>2. Commissioning of Hardware to get connected to Wi-Fi Network<br>3. Registration of User Access on the User Interface<br><br>**Quantity: One (1) Lot**<br><br>**Specifications**<br>1. Must monitor the Main Circuit Breaker, Sub-circuit Breakers, and Solar Inverter (if applicable) | |

| | | |
|---|---|---|
| | 2. Must be capable of supporting at least 6 Current Sensor input<br>3. Must include hardware is 4G Enabled Monitoring System that allows direct communication to the cloud<br>4. Must ensure the rating of the Current Sensor is at least the same size as the Circuit Breaker and shall be easily upgradeable in case of future expansion<br>5. Must support both Single and Three Phase configurations<br>6. Must include Data and Cloud Online Service for 1 year, with a Data Subscription option available after the initial year if needed<br>7. Must provide an API connection to LGU Cloud Server<br>8. Must be NTC certified<br>9. Must have passed CISPR 32:2015 and EN 55032 2015: Conducted Emission Test Class B.<br>10. Must have passed CISPR 32:2015 and EN 55032 2015: Radiated Emission Test Class B.<br>11. Must have passed IEC 61000-4-2:2008 Electrostatic Discharge Test.<br>12. Three (3) years warranty on parts and services. | |
| 1-F | **Component 1-F - Infrastructure Development – Door Access System**<br><br>**Scope of Works** - Supply, installation, configuration, testing and commissioning<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. Must be able to register up to 10000 faces, 10000 cards, and 3000 fingerprints<br>2. Must support AI-based face recognition all-in-one terminal<br>3. Must support live detection algorithm against most of the photos, videos, and 3D masks attack<br>4. Must have an industrial grade design, with stable performance and smooth lines<br>5. Must be IP65<br>6. Must have an anti-backlight feature<br>7. Dimensions: 174mm*84mm*18mm<br>8. Three (3) years warranty on parts and services | |
| 2 | **Power and Cooling Solutions** | |
| 2-A | **Component 2-A - Power and Cooling Solutions – Uninterruptible Power Supply (UPS)** | |

| | | |
|---|---|---|
| | **Scope of Works** - Supply, installation, configuration, testing and commissioning<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. Must have double conversion mode efficiency up to 96%<br>2. Must have the functionality to reduce energy usage & CO2 emissions<br>3. Must be used as a rack or a tower model<br>4. Must have a versatile wiring: 3-3, 3-1, 1-1 mode<br>5. Must have the capability for parallel operation up to 3 models<br>6. Must have an ESS mode which achieves an efficiency level of up to 98.8% with a break time of less than 2ms<br>7. Must have a battery management technology that increases battery service life by 50%<br>8. Must be able to endure harsh environment with operating temperature up to 50ºC<br>9. Must have a maintenance bypass<br>10. The rated input and output voltage must be 1 phase 200 / 230 / 240V and 3 phase 380 / 400 / 415V<br>11. The input voltage range must be 160V-300V full load; 100 – 160v linear derating<br>12. The input frequency range must be 40Hz – 70Hz<br>13. The output frequency must be 60Hz / 70Hz<br>14. The input power factor (PF) should be >0.995 both 1 phase and 3 phases<br>15. The battery voltage must be +- 192V with 0-13A charging current<br>16. The physical dimension must be 129mm height x 438mm width x 589mm depth<br>17. Certification must have: CE / TLC / RCM for safety and CQC for energy saving<br>18. Three (3) years warranty on parts and services. | |
| 2-B | **Component 2-B - Power and Cooling Solutions – Power Distribution Units (PDUs)**<br><br>**Scope of Works** - Supply, installation, configuration, testing and commissioning<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. Vertical, Metered to PDU Level, IP PDU<br>2. 20xIEC C13 Sockets, 4xIEC C19 Sockets | |

| | | |
|---|---|---|
| | 3. With 2x Circuit Breakers, 32A<br>4. 3x4mm² 3m Cable, with IEC 60309 Commando Plug.<br>5. Three (3) years warranty on parts and services. | |
| 2-C | **Component 2-C - Power and Cooling Solutions – Precision Air-Conditioning Units**<br><br>**Scope of Works**<br>1. Supply and installation two (2) in-row cooling units inside the Data Center Room<br>2. Supply and installation of equipment support using angle bar, grip anchor, expansion shields for outdoor units<br>3. Supply and installation of refrigerant piping using hard drawn "Type L" copper tube, including insulation, piping and fittings<br>4. Supply and installation of condensate drain piping with proper hangers, supports and fittings<br>5. Charging of refrigerant to the AC system<br>6. Startup and commissioning<br><br>**Quantity:** Two (2) Units<br><br>**Specifications**<br>1. Must provide 32kW cooling capacity in 42U<br>2. Must have user-friendly 7" color touch screen with graphic display as an option<br>3. Must be up to 8 teamwork<br>4. Must have control inverter drive technology<br>5. Must have optional temperature and humidity control<br>6. Must have a maximum energy efficiency (EER>3)<br>7. Must have variable speed fans with hot-swappable EC technology<br>8. Should support SMTP and NTP<br>9. Three (3) years warranty on parts and services. | |
| 2-D | **Component 2-D - Power and Cooling Solutions – Comfort Cooling**<br><br>**Scope of Works**<br>1. Supply and installation of two (2) 2.5HP Split Type air-conditioning units<br>2. Supply and installation of refrigerant piping from indoor to outdoor unit using copper tube including pipe insulation, supports and fittings<br>3. Supply and installation of condensate drainpipe from indoor unit to be tapped to nearest drain point | |

| | | |
|---|---|---|
| | 4. Supply and installation of feeder wires and circuit breakers<br><br>**Quantity:** Two (2) Units<br><br>**Specifications**<br>1. Must be a split-type aircon<br>2. Must support at least 2.5HP<br>3. Must support at least 220-230 volts<br>4. Must be a single phase<br>5. Must support at least 60Hz<br>6. Three (3) years warranty on parts and services. | |
| 2-E | **Component 2-E - Power and Cooling Solutions – Backup Power Generator**<br><br>**Scope of Works**<br>1. Supply and Delivery: Provide a brand-new 150 kVA diesel generator with all standard accessories and documentation, delivered to the project site.<br>2. Site Preparation and Installation: Install the generator on a pre-prepared concrete pad, including anti-vibration mounts, exhaust system routing, and proper earthing.<br>3. Electrical Connections: Connect the generator to the main power system, including the installation of an Automatic Transfer Switch (ATS) and necessary cabling.<br>4. Fuel System Setup: Install and connect a fuel tank with sufficient capacity for a minimum 12-hour runtime at full load, including leak-proof fittings.<br>5. Control Panel Configuration: Install and configure the generator's digital control panel for real-time monitoring and operation.<br>6. Testing and Commissioning: Conduct pre-commissioning checks, load testing, and functional testing of the generator and ATS to ensure proper operation.<br>7. Training: Provide training for facility personnel on generator operation, maintenance, and troubleshooting.<br><br>**Quantity**<br>1. One (1) unit 150 kVA Diesel Generator Set with accessories.<br>2. One (1) lot Automatic Transfer Switch (ATS).<br>3. One (1) lot Exhaust system and piping.<br>4. One (1) lot Earthing and grounding materials. | |

| | | |
|---|---|---|
| | **Technical Specifications**<br>1. Generator Set House<br>j. Excavation works<br>k. Supply and installation of footing, pedestal columns, wall footing, beams, concrete flooring<br>l. Supply and installation of wall concrete hollow blocks (CHB)<br>m. Supply and installation of wall partitions<br>n. Supply and installation of columns and footings<br>o. Supply and installation of tubular GI bars and flat bars<br>p. Supply and installation of mesh wires<br>q. Supply and installation of corrugated roofing including fittings, gutter and paint coatings such as epoxy primer<br>r. Provision for miscellaneous and consumables<br>8. Generator Set<br>a. Must have a prime output rating is 200kVA<br>b. Must have 60Hz frequency<br>c. Must be three phases at 200~240/380~440V<br>d. Power factor must be at least 0.8 (lagging)<br>e. Must have a voltage regulation within +/- 1.5<br>f. Must have a brushless, rotating exciter (with A.V.R)<br>g. Must have a class H insulation<br>h. Engine must be vertical inline, water-cooled, 4-stroke direct injected, turbo intercooler, air intercooler<br>i. Must have 8.82L piston displacement<br>j. Must have at least 32.8L/h fuel consumption at 75% load<br>k. Must have a lube oil capacity of 19L<br>l. Must have a coolant capacity of 41L<br>m. Must have a 12V-150Ah battery capacity<br>n. Must have 330L fuel tank capacity<br>o. Sound level must be 72-75 dB at 7m<br>p. Must have a top mounted Holset Hx40W turbo-charger for increased power, fuel economy, and lower smoke and noise levels<br>q. All metal canopy parts are factory rustproof using special powder paint coating<br>r. Must have detachable side doors to provide access for maintenance and repairs<br>9. Warranty and Support | |

| | | |
|---|---|---|
| | a. Three (3) years warranty on parts and services.<br>b. Provision of preventive maintenance service during the warranty period. | |
| 3 | **Security and Safety Systems** | |
| 3-A | **Component 3-A - Security and Safety Systems – Fire Detection, Alarm, and Suppression System**<br><br>**Scope of Works** - Supply, installation, configuration, testing and commissioning<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. The solution must ensure that fire protection is focused on the core of areas with greater risk.<br>2. The solution must require no electric power or battery backup for operation.<br>3. The solution must provide continuous fire protection regardless of power outages or dead batteries.<br>4. The solution must concentrate on the protection of high-risk, high-value equipment within individual cabinets rather than the entire room.<br>5. The solution must utilize Novec 1230 (FK-5-1-12) as the extinguishing agent.<br>6. The solution must be certified by UL and CE for compliance with industry standards.<br>7. Three (3) years warranty on parts and services. | |
| 3-B | **Component 3-B - Security and Safety Systems – CCTV System**<br><br>**Scope of Works**<br>1. Supply and installation of CCTV cameras inside the Data Center only<br>2. Supply and installation of NVR and CCTV switch<br>3. Supply and installation of terminal boxes for CCTV cameras<br>4. Termination, panning, finetuning and testing of CCTV cameras<br>5. Configuration of NVR and switch<br>6. Labeling of cameras<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. **Dome Camera** | |

| | | |
|---|---|---|
| | a. 5Megapixel (2592 x 1944) resolution<br>b. 2.8mm fixed lens<br>c. 0.15Lux (Color), 0Lux (B/W, IR LED on)<br>d. H.265, H.264, MJPEG codec support, Multiple streaming<br>e. Day & Night (ICR), WDR (120dB)<br>f. Tampering, Motion detection, Defocus detection<br>g. Micro SD / SDHC / SDXC memory slot (Max. 128GB)<br>h. Hallway view, WiseStream II support<br>i. IR Viewable length 20m (65.62ft)<br>j. Imaging device ½.8" CMOS<br>**10. Network Video Recorder**<br>a. Up to 8CH, 12MP camera supported<br>b. H.265, H.264, MJPEG codec<br>c. 100Mbps network camera recording<br>d. Plug & play by 8 PoE (LAN, 10/100), 1PoE (WAN, 1Gbps)<br>e. SATA 2ea (up to 20TB)<br>f. ARB supported<br>g. P2P service (QR code connect) supported<br>h. Three (3) years warranty on parts and services. | |
| 3-C | **Component 3-C - Security and Safety Systems – Managed Cyber Security Services**<br><br>**Scope of Works**<br>1. Hardware Installation and Start Up<br>2. Installation and Configuration of Data Processor<br>3. Installation & Configuration of Sensors<br>4. Integration with Different Data Sources<br>5. Custom Reports and Dashboard Configuration<br>6. Custom Alert Creation<br>7. Knowledge Transfer<br>8. 24 x 7 x 365 Monitoring, Investigation and Analysis for the assets defined under Assets/Devices Covered<br>9. 24 x 7 x 365 Threat and Incident Notification with Expert Recommendation for identified and validated threats<br>10. 24 x 7 x 365 SOC Portal Access and Admin support<br>11. Monthly security report submission or as necessary<br>12. Alerting/Notification delivery are via Email or Call | |

| | | |
|---|---|---|
| | 13. Minimum of thirty (30) days onboarding to determine the current security posture of the organization and process alignment prior to MSOC Go Live.<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br><br>1. **General Specification of SOC Platform**<br><br>a. The solution must be a cloud-native security operation platform with built-in and fully integrated (single interface/management) next-generation NGSIEM, UEBA, NDR, FIM, Sandboxing, and SOAR capabilities, as well as open integration to existing security stacks and future security tools, to automate cybersecurity threat detection, investigation, and response across the entire attack surface.<br><br>b. The solution must be SOC 2 Type 2 Certified.<br><br>c. The solution must have NG-SIEM natively to provide a centralized location for gathering and organizing data from any existing security control, IT, and productivity tool using pre-built integrations that are easy to use and do not incur additional costs for integrating new security tools.<br><br>d. The solution must have NDR natively built-in to provide visibility into threats at the network layer to stop attacks faster to limit potential damage.<br><br>e. The solution must include UEBA natively to analyze traffic and produce security status and event information on individual users, as well as monitor network assets and analyze their behavior to detect threats.<br><br>f. The solution must include File Integrity Monitoring to track changes to specified files and directories, such as file changes, file creations, and file deletion.<br><br>g. The solution must have a built-in sandbox capable of detecting reassembled files over the wire that, if found to be malicious, will actively detonate in a Malware Sandbox to detect novel threats.<br><br>h. The solution must be able to collect data from multiple sites using distributed sensors/data collectors.<br><br>i. The solution must be able to collect data without limiting the type and number of devices to collect from.<br><br>j. The software solution must be scalable and capable to accommodate minimum of 100GB data.<br><br>k. The solution must have native sensors that can be delivered on-premise as a purpose-built appliance, a virtual appliance (VMware, Microsoft Hyper-V, or KVM), or in the cloud, such as AWS, Azure, Google Cloud Platform, or Oracle Cloud Infrastructure. | |

| | | |
|---|---|---|
| | l. The solution's native sensor must be prepackaged with network IDS, deep packet inspection, and Malware Sandbox functionality.<br>m. The solution must integrate threat intelligence and telemetry data from multiple sources with security analytics to contextualize and correlate security alerts.<br>n. The solution must be able to securely transmit collected network telemetry and logs to a secured storage.<br>o. The solution must integrate threat intelligence and telemetry data from multiple sources and other security tools with security analytics to contextualize and correlate security alerts.<br>p. The solution must have SOAR built-in to provide both manual and automated response to cyber threats using pre-defined playbooks and pre-built integrations to security, IT, and productivity products, ensuring identified threats are mitigated appropriately and consistently.<br>q. The solution must be able to automatically generate novel alerts based on input data sources and applying Machine Learning models, such as finding anomalous patterns based on parent-child process relationships, unusual application connections or usage, unusually high user command execution rates, and unusually high numbers of connections to non-standard ports for an application.<br>r. The solution must automatically integrate its own Threat Intelligence Platform (TIP) into its architecture for data enrichment in order to rapidly identify attack paths and previous interactions with known bad actors, increasing threat detection accuracy while decreasing response time.<br>s. The solution must be capable of catching, extracting, and reassembling malware that travels through the network via HTTP, FTP, SMB, and SMTP.<br>t. The solution must be capable of forwarding malicious files to an external HTTPS server.<br>u. The solution must be able to translate an IP address into a geographical location or reputation.<br>v. The solution must be able to override the geolocation gathered from geolocation databases by manually defining the geolocation associated with specified IP addresses.<br>w. The solution must have an aggregator that can be deployed as a virtual appliance and act as a proxy to forward traffic from other sensors to the central data repository.<br>x. The solution must support Geo Location Public IP look up.<br>y. The solution must have reputation-based threat intelligence that automatically enriches network data | |

| | | |
|---|---|---|
| | and logs during real-time ingestion to add context to the data, thereby improving the analyst's threat detection, investigation, and hunting.<br><br>z. The solution must be able to cut through the noise of an overwhelming volume of alerts by automating both threat detection (via AI and machine learning) and response (via automated threat hunting).<br><br>aa. The solution must have integrated threats, incident and compliance management.<br><br>bb. The solution must be capable of constructing a meaningful security context by utilizing machine learning to determine the strength of the link between an alert and a potential incident by employing multiple security artifacts such as shared entities (assets or users), properties (hashes or URLs), and time.<br><br>cc. The solution must automatically monitor for known bad events, and use sophisticated correlation via search, to find known risk patterns such brute force attacks, data leakage and even application-level fraud.<br><br>dd. The solution must be able to detect compromised hosts associated with advanced threats and malware infections.<br><br>ee. The solution must be able to find activities and events associated with successful attacks and malware infections.<br><br>ff. The solution must issue an alert upon detection of blacklisted external IP.<br><br>gg. The solution must be fully customizable when creating warning or alarms for high risks events.<br><br>hh. The solution must support Authentication Authorization Accounting (AAA).<br><br>ii. The solution must use machine learning based detections. Please provide some use cases and evidence that the app is using machine learning based algorithms<br><br>jj. The solution should include unsupervised machine learning detection model that predicts current behavior based on the historical distribution of a given detection parameter (Host, user, source IP address, etc).<br><br>kk. The solution should include an unsupervised machine learning detection model that learns steady population statistics from the past peer data and looks for irregularities that deviate from typical behavior over time.<br><br>ll. The solution should include an unsupervised machine learning detection model that examines whether the presence of a given detection parameter has appeared in the last number of days or not.<br><br>mm. The solution should include a supervised classification model that uses a set of indicators to | |

| | | |
|---|---|---|
| | determine a decision boundary between normal and suspicious data points.<br><br>nn. The solution must provide an API with the following capabilities:<br><br>1. Retrieve detailed collector information<br><br>2. Retrieve detailed incident information<br><br>3. Update incident detail<br><br>**11. Specifications of NEXT GEN SIEM (Security Information and Event Management)**<br><br>a. The solution must ensure that security events and incidents are accessible and searchable within twelve (12) months. As needed, evidence from security incidents is made available for historical analysis.<br><br>b. The solution must be capable to collect different types of metadata (e.g., logs, security events, network flows, among others) from data sources and shall include log compression and industry standard encryption at rest and in transit to ensure security of captured data from disclosure to disinterested parties.<br><br>c. The solution must automatically normalize and enrich data from any source with context including threat intelligence, user details, device information, Geographical location to enable detailed, extensible data analytics.<br><br>d. The solution must be capable of collecting and normalizing server logs, network packets, server process data, file data, and threat intelligence data into JSON-formatted records.<br><br>e. The solution must include an alert statistics dashboard that allows analysts to quickly examine any discovered alerts at a glance, such as:<br><br>1. Graph of critical vs. total alert status<br><br>2. Show the Open vs. Total alert graph.<br><br>3. Show the Alert trend<br><br>f. The solution must be capable of ingesting TLS encrypted syslog and syslog-ng logs.<br><br>g. The solution must have a sensor that can be deployed as an agent in Windows Servers (Windows Server 2008 R2, 2012, 2016, and 2019) to collect event data related to the following:<br><br>1. Hardware<br><br>2. Security<br><br>3. System<br><br>4. Windows Firewall<br><br>5. Windows Defender<br><br>6. Windows Powershell | |

| | | |
|---|---|---|
| | h. The solution must be able to integrate with domain controllers in order to enrich data collected with the relationship between users and IP addresses.<br>i. The solution must be able to integrate with a DHCP server to determine the relationship between hostnames and IP addresses and track devices when the IP address changes.<br>j. The solution must be able to ingest Windows Sysmon events.<br>k. The solution must be able to correlate traffic, processes, users, and commands in order to detect security, DDoS, and breach attempts.<br>l. The solution must have a collector that can be deployed as an agent in Linux Servers (RHEL, CentOS, Debian, Ubuntu, Amazon Linux, Oracle Linux, Suse Linux) to monitor and capture the following information:<br>1. Process info<br>2. Command execution<br>3. Files<br>4. File events<br>m. The solution must include a tool for finding and visualizing correlations between events.<br>n. The solution must have a visual tool for focusing in on a single entity (Host, IP, URL, or User) in a security event and viewing its relationship to other entities.<br>o. The solution must include out-of-the-box threat hunting templates that can be edited, copied, and exported.<br>p. The solution must be capable of removing duplicate data through packet deduplication.<br>q. The solution must be able to reduce the amount of metadata gathered for SMB commands.<br>r. The solution must automatically compress the ingested data.<br>s. The solution must be capable of sending alerts to relevant personnel regarding security issues based on correlated events.<br>t. The solution must be capable of serving any number of logical network data or log segregation based on specific departments, functionalities, or locations that the user considers to be managed separately. Not only should security information be kept completely separate, but machine learning-based threat detections should also be distinct for each department.<br>u. The solution must include data collectors that are able to send data (log/event) in real-time and batch mode. | |

| | | |
|---|---|---|
| | v. The solution must be capable of performing Server and Network Infrastructure Monitoring out of the box.<br>w. The solution must be capable of performing Application Monitoring out of the box.<br>x. The solution must be able to maintain the original timestamps for each event while handling timestamps from different time zones<br>y. The solution shall provide advance correlation capabilities to detect security incidents such as:<br>1. DDOS attacks<br>2. Worm outbreak<br>3. Port Scan<br>4. SQL injection<br>5. Brute Force attack<br>z. The solution must be able to correlate asset info with threat and vulnerability data<br>aa. The solution provides network visibility from wire data that contains critical insights about payloads, session information, errors, DNS, etc.<br>bb. The proposed solution shall be able to provide search function that support Boolean-style patterns search<br>cc. Proposed solution shall be able to allow analysts to build queries using combined search methods. A single query may contain keywords and field-based conditions.<br>dd. The proposed solution must be able to perform sub search in regard to the security on top the current search<br>ee. The solution must have a customizable widget on the dashboard<br>ff. The solution must support Email notification with content in JSON format<br>gg. The solution should include an investigative tool that allows security analysts to quickly examine any security alerts by displaying enriched alert information that includes identified MITRE ATT&CK tactic and techniques used, attack kill chain category, ML based score, alert status, key event parameters that contribute to triggering the alert, and full event details.<br>hh. The solution must have the ability to threat hunt and automate the threat hunt and apply to SOAR<br>**12. Specifications of UEBA (User Entity and Behavior Analytics)**<br>a. The solution must be capable of inspecting assets for threat data and past performance. | |

| | | |
|---|---|---|
| | b. The solution must be capable of monitoring every server, router, and host system in the private network.<br>c. The solution should provide a host-centric view of alert activity for specific hosts.<br>d. The solution must come with user behavior analytics that collect user information from Active Directory<br>e. The solution must come with entity behavior analytics that collect IP information from network traffic<br>f. The solution must track changes and secure your environment by monitoring for suspicious activity, user role changes, unauthorized access and more.<br>g. The solution, based on observed security events and asset risk profile, assigns a risk score.<br>h. The solution must discover assets dynamically across networks, endpoints, and cloud environments.<br>i. The solution must use either host names, MAC addresses, or IP addresses to uniquely identify assets.<br>j. The solution must collect and fuse user-relevant data from multiple data sources across the security infrastructure automatically.<br>k. The solution's Machine learning must be used to enable sophisticated behavioral analytics in the solution.<br>l. The solution without any rules or signatures, must detect bad behavior.<br>m. The solution must be capable of detecting the use of an unfamiliar application by an internal user who normally uses a minimal yet consistent number of applications.<br>n. The solution must be capable of detecting when an internal user has an abnormally high volume of traffic in comparison to its usual volume or that of its peers.<br>o. The solution must be capable of detecting the use of an unfamiliar app by an external user who normally uses a minimal yet consistent number of applications.<br>p. The solution must be capable of detecting when an external user has an abnormally high volume of traffic in comparison to its usual volume or that of its peers.<br>q. The solution must be able to detect a user who logs in to a new asset who typically uses a small, consistent number of assets.<br>r. The solution must be capable of detecting a user who has logged in from an unusual location. | |

| | | |
|---|---|---|
| | s. The solution for each detected and identified for asset, must provide a kill chain view of security events.<br>t. The solution must track threats based on the user rather than the threat type.<br>u. The solution must assign a risk score to each user in order to easily identify risky users<br>v. The solution must be capable of detecting a user who typically executes a small, consistent number of processes but has recently executed a new process.<br>w. The solution must be capable of detecting an internal HTTP connection made by an internal user agent that has never been observed or has only been seen on rare occasions.<br>x. The solution must be capable of detecting an external HTTP connection made by a potentially malicious user agent.<br>y. The solution must be capable of detecting a user who has logged in from locations that are geographically impossible to travel between within the time frame.<br>z. The solution must be capable of detecting a user who logs in at an unusual time.<br>aa. The solution must be able to detect an asset that started a previously unknown process, which could indicate a malware attack.<br>bb. The solution must be capable of detecting processes that typically launch a small, consistent number of child processes.<br>cc. The solution must be capable of detecting A file or files that have been created an unusually large number of times.<br>**13. Specifications of NDR (Network Detection and Response)**<br>a. The solution must be capable of monitoring suspicious traffic in both external (north/south) and internal (east/west) traffic, as well as traffic in all physical and virtual environments.<br>b. The solution must enable the user to safely inspect suspicious files in order to detect the presence of zero-day malware and advanced persistent threats.<br>c. The solution must be capable of ingesting RSPAN session flows.<br>d. The solution must be capable of ingesting GRE traffic that has been mirrored with ERSPAN.<br>e. The solution must be capable of compiling identical metadata from talkative applications into a single record to reduce traffic going to central data repository.<br>f. The solution must be capable of correlating processes running on the sensor and host and the IP address/port visible in traffic. | |

| | | |
|---|---|---|
| | g. The solution must passively collect asset information and network flow information<br>h. The solution must be capable of correlating and identifying application performance issues due to security incident (e.g. DDOS attacks, unauthorized access to the system that causing application performance issues).<br>i. The solution should have the ability to report when Data Theft occurs.<br>j. The solution's architecture has to be very extensive in network traffic analysis using both Supervised and Unsupervised learning<br>k. The solution must be capable of capturing raw network packets and reducing the data to produce valid security events without the size of a full packet capture.<br>l. The solution must be capable of collecting and correlating firewall traffic logs, IDS events, NetFlow and cloud flow logs.<br>m. The solution must be able to track the interaction between network devices, services, and applications in real time and over time.<br>n. The solution shall be able to address all Alert Types Tied to phases of Attack Life Cycle.<br>o. The solution should support integration to firewall to do Inline blocking mode (not TCP Reset).<br>p. The solution must be capable of monitoring DNS resolution changes for specified domains, so that if one of the observed domains resolves to a different IP address, the solution will populate a visual record indicating the change.<br>q. The solution must provide a visual representation of the entire attack landscape, mapping detected threats to their corresponding attack kill chain stage. The detected threat must be clearly tagged with the relevant MITRE ATT&CK framework for detailed analysis of an ongoing attack's progression.<br>r. The solution must be capable to do comprehensive network traffic analysis which includes: Network performance statistics, Server performance, Application detection and performance monitoring, Top sources & Top destinations, Asset application performance, Application processing time, Network interactions with asset, HTTP statistics, DNS statistics, Asset Discovery and Statistics, IP address, Device Manufacturer, Application Services, Time discovered and last seen, Asset tag(s) and description, Server certificate visibility<br>**14. Specification of SOAR (Security Orchestration Automation and Response)**<br>a. The solution must automatically recognize alerts from multiple sources, analyze them for similarities, and automatically add any identified connected | |

| | | |
|---|---|---|
| | alerts to a case or cases, preventing the team from duplicating efforts and hunting for details in multiple places.<br>b. The solution must have a dynamic case management tool that automates the continuous correlation of existing cases to new alerts when they are discovered to be potentially related.<br>c. The solution must be capable of storing cases for a year.<br>d. The solution must be capable of accelerating security incident management processes by automating case generation with key details such as the ones listed below.<br>1. Incident Name and Ticket ID: These must be generated automatically.<br>2. Incident Score: A score based on how serious the incident was.<br>3. Incident Severity: The incident's severity (Critical, High, Medium, or Low).<br>4. Incident Reported Time: The time when the incident occurred.<br>5. Analyst assigned to incident: The person tasked with handling the incident.<br>6. Incident Status: The incident's associated state (New, Escalated, Ongoing, Solved, Cancelled).<br>7. Incident Closed Time: The time when the incident was resolved.<br>e. The solution must have out of the box or customizable playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. Playbooks deployed shall include at least:<br>1. Phishing enrichment and response<br>2. Malware endpoint response<br>3. Internal and External Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, unusual login location, login from suspicious device)<br>4. Unusual browsing activity<br>5. Web attack profiling and blacklisting<br>6. File activity anomalies such as creation, move, delete, or change<br>7. Potential data exfiltration<br>8. C&C Connection<br>f. The solution must automatically trigger playbooks with predefined workflows that to perform a variety of instructions that could include executing scripts or integrating with other tools in the environment. | |

| | | |
|---|---|---|
| | g. The solution must have the option to create user-defined playbooks with customized workflows<br>h. The solution must include an API for pulling data from SaaS and cloud-based applications as well as pushing command responses such as firewall blocking or user disabling.<br>i. The solution must be able to track the status of analyst responses in handling assigned cases over time.<br>j. The solution must be part of a unified SOC platform to provide robust SOC workflow features in a single location including:<br>1. assignment of threat cases to analysts for review<br>2. comprehensive investigative actions<br>3. annotation for additional notes or explanation<br>4. swift remediation actions trigger<br>5. reporting of overall workflow metrics.<br>k. Three (3) years warranty on parts and services. | |
| 3-D | **Component 3-D - Security and Safety Systems - Endpoint Security**<br><br>**Scope of Works**<br>1. Registration of Client's Account to Vendor's Endpoint Protection Portal<br>2. Endpoint Protection Agent Deployment<br>3. Walkthrough on Endpoint Protection Console<br>4. Testing of Endpoint Protection Portal Features<br><br>**Quantity**: 2274 Licenses<br><br>**Specifications**<br>1. **Integrated Management**<br>a. A unified console for managing products from the same vendor.<br>b. The ability to manage security policies and administer multiple products from a single web interface.<br>**15. Multi-Platform Management**<br>a. Windows, Mac, and Linux machines must be managed from one management console.<br>b. Configure the bandwidth limit for updating.<br>c. Must have the option to enable devices to get updates from the security vendor from a cache device and communicate all policy.<br>**16. Updating and Installation Options** | |

| | | |
|---|---|---|
| | a. Deploying the endpoint agent must support the following methodologies: Email setup link, Installer link, Scripted Installation<br>**17. Role Management**<br>a. To divide security administration by responsibility level and includes the following predefined roles: Super Admin, Admin, Help Desk, Read-Only, User<br>**18. AD Synchronization**<br>a. Implement a service that maps users and groups from Active Directory to the security vendor cloud console and keeps them synced.<br>b. Synchronized with Azure Active Directory<br>c. Auto synchronization that happens every 6 hours for Azure AD<br>**19. Tamper Protection**<br>a. Must have the capability to prevent the following actions on the endpoint protection solution:<br>1. Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or security vendor live protection<br>2. Disable tamper protection<br>3. Uninstall the security vendor agent software<br>**20. Threat Protection**<br>a. Protect against malware, risky file types and websites, and malicious network traffic.<br>b. Have security vendor settings recommendation to provide the best protection a computer can have without complex configuration.<br>c. Automatically submit malware samples to security vendor online for analysis.<br>d. Do real-time scanning internet resources as users attempt to access them.<br>e. Protect against threats by detecting suspicious or malicious behavior or traffic on endpoint computers:<br>1. Documents from Ransomware<br>2. Critical functions in web browsers<br>3. Mitigate exploits in vulnerable applications<br>4. Application hijacking<br>5. Detect network traffic to command-and-control servers<br>**21. Suspicious Behavior Detection**<br>a. Monitor the behavior of code to stop malware before a specific detection update is released.<br>b. Have both pre-execution behavior analysis and runtime behavior analysis. | |

| | | |
|---|---|---|
| | c. Have a technology that is used to identify specific characteristics of files before they run, to determine whether they have malicious intent.<br><br>**22. Advanced Deep Learning Mechanism**<br><br>a. The system shall be light speed scanning; within 20 milliseconds, the model shall be able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes.<br><br>b. Protect the system even while offline and will not rely on signatures.<br><br>c. Classify files as malicious, potentially unwanted apps (PUA) or benign.<br><br>d. Should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.<br><br>e. Model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance.<br><br>f. The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, TensorFlow, and Scikit-learn.<br><br>**23. Exploit Prevention/Mitigation**<br><br>a. Must detect and stop the following known exploits:<br><br>1. Enforcement of Data Execution Protection (DEP)<br><br>2. Mandatory Address Space Layout Randomization (ASLR), Bottom-up ASLR<br><br>3. Null Page (Null Dereference Protection)<br><br>4. Heap Spray Allocation<br><br>5. Dynamic Heap Spray<br><br>6. Stack Pivot<br><br>7. Stack Exec (MemProt)<br><br>8. Stack-based ROP Mitigations (Caller)<br><br>9. Branch-based ROP Mitigations (Hardware Augmented)<br><br>10. Structured Exception Handler Overwrite Protection (SEHOP)<br><br>11. Import Address Table Access Filtering (IAF) (Hardware Augmented)<br><br>12. LoadLibrary API calls<br><br>13. Reflective DLL Injection<br><br>14. Shellcode monitoring<br><br>15. VBScript God Mode<br><br>16. WoW64 | |

| | | |
|---|---|---|
| | 17. Syscall<br>18. Hollow Process<br>19. DLL Hijacking<br>20. Application Lockdown<br>21. Java Lockdown<br>22. Squiblydoo AppLocker Bypass<br>**24. Policies**<br>a. Selected policies should be able to be applied to either users or devices.<br>b. Policies must have the capability to be enforced and whether it expires.<br>**25. Data Loss Prevention (DLP)**<br>a. Monitor and restrict the transfer of files containing sensitive data.<br>b. Specify conditions for data loss prevention to detect, action to be taken if the rules are matched, any files to be excluded from scanning.<br>c. Must have two types of rules: File & Content.<br>**26. Peripheral Control**<br>a. Control access to peripherals and removable media.<br>b. Exempt individual peripherals from that control.<br>**27. Application Control**<br>a. Detect and block applications that are not a security threat but lets the administrator decide if it is unsuitable for office use.<br>**28. Web Control**<br>a. Block by category of the site.<br>b. Block specific file types or specific websites.<br>c. Prevent access to sites that increase the risk to the organization.<br>d. Help improve productivity and potentially limit bandwidth.<br>**29. Account Health Check**<br>a. Shows whether you're using all the protection features.<br>b. Reflects account health scores when using devices or policies recommended settings.<br>c. Must have the following Account Health Check Features:<br>d. Secure the protection license in endpoint and server are installed.<br>e. Secure the threat protection policies in endpoint and server uses recommended settings. | |

f. Secure that there is no security risk associated with any exclusions in your server or endpoint threat protection rules.

g. Secure your devices' tamper prevention is activated.

h. An issue with the Account Health Check can be snooze.

**30. Adaptive Attack Protection**

a. Protection feature that consists of a series of technique-focused behavioral rules intended to disrupt the actions of a threat actor.

**31. Threat Analysis Center**

a. Allows to see and analyze detection numbers and trends.

b. Must have the following Dashboard Features:

1. Total Detections
2. Total Detection Count
3. Select a breakdown view.
4. Select graph or heatmap view.
5. Top 10 entities
6. Top 10 users
7. Sensor location or detection mapped by geographical location.
8. MITRE TTP (Tactics, Techniques, Procedures)
9. Recent detections
10. Set the time range.
11. Set filters.
12. Highlight details on a graph.

**32. Remediation**

a. Detected malware are cleaned up automatically.

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

**33. Data Lake**

a. Out-of-the-box and fully customizable SQL queries

b. Store and access critical information from endpoints, servers, firewall and email.

c. Utilize device information even when the device is offline.

**34. IT Operations**

a. Must be able to determine:

1. Why a machine is running slowly.
2. Devices that have known vulnerabilities, unknown services, or unauthorized browser extensions.

| | | |
|---|---|---|
| | 3. If there are programs running that should be removed.<br>4. Identify unmanaged, guest, and IoT devices.<br>5. Why network connection is slow and what application is causing it.<br>6. Look back thirty (30) days for unusual activity on a missing or destroyed device.<br>**35. Threat Hunting**<br>a. Find out what processes are trying to make a network connection on non-standard ports.<br>b. Show processes that have recently modified files or registry keys.<br>c. List detected IoCs mapped to the MITRE ATT&CK framework.<br>d. Extend investigations to 30 days without bringing a device back online.<br>e. Use ATP and IPS detections from the firewall to investigate suspect hosts.<br>f. Compare email header information, SHAs, and other IoCs to identify malicious traffic to a domain.<br>**36. Remote Access**<br>a. Connect to devices and investigate and remediate possible security issues.<br>b. Stop suspicious processes, restart devices with pending updates, browse folders, and delete files.<br>c. See when sessions started and ended, the admin who started the session, the device that the session accessed, and the "Purpose" given when the session was started.<br>**37. Synchronized Security**<br>a. Security products of the same vendor actively work together, responding automatically to incidents and delivering enhanced security insights.<br>**38. Integration**<br>a. Can integrate other security product or third-party products.<br>**39. Certifications**<br>a. The endpoint protection manufacturer must be a Leader in the 2023 Gartner Magic Quadrant for Endpoint Protection Platforms<br>**40. License Subscription**<br>a. Three (3) years license subscription | |
| 4 | **IT Infrastructure and Services** | |
| 4-A | **Component 4-A - IT Infrastructure and Services - Hyper Converged Infrastructure (HCI)** | |

| | | |
|---|---|---|
| | **Scope of Works**<br>1. HCI AND VIRTUALIZATION SOLUTION<br>a. Node Server Setup<br>b. Mounting of Server to the Data Cabinet<br>c. Server Management Configuration<br>d. Implementation of Virtualization Solution<br>e. HCI Virtualization Solution Configuration<br>f. Implementation of Virtualization Management Solution<br>g. Virtualization Management Solution Installation<br>h. Creation & Configuration of Virtual Machine<br><br>41. WITNESS SERVER<br>a. Basic Server Setup<br>b. Mounting of Server to the Data Cabinet<br>c. Server Management Configuration<br>d. Implementation of Virtualization Solution<br>e. Configuration of Witness Server<br>f. Implementation of Virtualization Management Solution<br>g. Virtualization Management Solution Installation<br>h. Creation & Configuration of Virtual Machine<br><br>**Quantity:** One (1) Lot<br><br>**HCI Specifications**<br>1. **Hardware Specifications**<br>a. The Hyper-Converge Infrastructure must have a minimum of 3 nodes<br>b. Processor: At least 2x32 cores @2.1GHz per node<br>c. Memory: At least 16x64GB 2Rx4 PC5-4800B-R memory per node<br>d. Storage: At least 12x3.84TB SSD RI BC MV storage per node<br>e. Adapter: At least 4 port 10/25GbE SFP+ ports NIC per node<br>f. Power supply: Two (2) or more power supply (Hot-Swappable/Hot-plug) Redundant<br>g. The brand being offered must be in the five eyes alliance<br>h. Three (3) years warranty on parts and services.<br>**42. Data Efficiency**<br>a. The solution must be capable of deduplicating, compressing & optimizing all data inline, in real- | |

| | | |
|---|---|---|
| | time, across all tiers of data within a system, without an impact on the performance.<br>b. Data efficiency shall be handled at data granularity of 4KB or 8KB data blocks.<br>c. De-duplication and compression shall be completely inline and must happen before the write request from a VM hits the actual data disk or cache disk offered in a given node.<br>d. Failure of any given disk in the HCI node shall not disable the de-duplication and compression for a given node, either temporarily or permanently.<br>e. De-duplication and compression shall use the unified data block size for entire set of VM data for data efficiency and shall not use more than 8KB in size.<br>f. De-duplication and compression shall always be enabled irrespective of the nature of data without any performance impact.<br>g. De-duplication and compression shall happen inline irrespective of IO type like Sequential or random IO operations.<br>**43. Hypervisor**<br>a. Hyper-converged solution should support leading hypervisors of the industry.<br>b. Hypervisor shall be general purpose and shall not be a proprietary one. Hypervisor shall be ported on both HCI as well as non-HCI environment using appropriate licenses.<br>**44. Expansion**<br>a. Hyper-converged solution should be able to start small, for high availability, and scale-out when required.<br>b. Offered Hyper-converged solution shall be able to manage at least 96 nodes into a single federation.<br>**45. Resiliency**<br>a. The solution must be able to support multiple points of failure across multiple nodes, with no loss of function or data.<br>b. Each node should have dedicated redundant PSU's to be able to sustain single power supply failure.<br>c. Must be able to compulsorily sustain minimum of simultaneous 1-HDDs failures in each node of a cluster and across all nodes in the cluster without data loss.<br>**46. Common Features Included**<br>a. Hyper-converged solution should have a guaranteed data efficiency rating of 10:1 when managing local VM data and backups should provide in writing the Data Efficiency being committed | |

| | | |
|---|---|---|
| | b. Hyper-converged solution shall have in-built support for container storage interface (CSI) and shall be qualified to work with Container platforms based upon open-source Kubernetes.<br><br>**47. Global Unified Management**<br><br>a. Offered Hyper-converge solution shall support VM-centric management through a single pane of glass via the virtualization manager of given hypervisor.<br><br>b. Virtualization Manager of given Hypervisor shall be able to manage single or multiple clusters through single management console of hypervisor.<br><br>c. Offered hyper-converge appliance shall have the ability to manage all aspects of the Hyper-convergence for all sites through Virtualization Manager of a given Hyper-Converge.<br><br>d. Offered Hyper-converge shall be able to globally manage Backup Policies per Datastore or per VM and shall be able to control all of them directly through virtualization manager of given hypervisor.<br><br>e. Hyper-converge solution should have single upgrade management console to simplify upgrade of Hyper-converge Software, hypervisor and ability to roll back upgrades.<br><br>**48. Backup & Data Protection**<br><br>a. Backup & data protection functionality shall be an integral feature of Hyper-Converge instead of a separate server/software license.<br><br>b. Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server.<br><br>c. Integral backup shall have ability to define backup policy per datastore or specific VM<br><br>d. Integral backup shall have the ability to execute backup tasks at a specified interval like specific day of the week or day of the month.<br><br>e. The solution must be able to provide backup reports for audit purposes.<br><br>f. Offered Hyper-converge solution shall provide complete flexibility for VM-level backup instead of forcing protection at the datastore level.<br><br>**49. Data Replication**<br><br>a. Hyper converge shall also be supported to deploy as a stretched cluster with RPO of zero and RTO of seconds. Hyper converge should support stretched cluster deployment in a near site metro DC deployment out of the box.<br><br>b. Offered solution shall support capability to throttle the replication bandwidth.<br><br>**50. Security** | |

| | | |
|---|---|---|
| | a. The solution supports Data-At-Rest-Encryption for additional data security<br>b. The solution supports integration with external key management solutions to enhance data security<br>c. The solution supports FIPS 140-2 validated enterprise-class encryption solution.<br>d. For firmware security, Hyperconverged system should support remote management chip creating a fingerprint in the silicon, preventing system from booting up unless the firmware matches the fingerprint. This feature should be immutable.<br>**51. Software Licenses**<br>a. The HCI solution must include the necessary server virtualization licenses:<br>b. At least 192 virtualization licenses with 3-year subscription.<br>c. The virtualization license should have the following features/tools:<br>1. Manage infrastructure images to patch, update, or upgrade clusters using a desired state model.<br>2. Virtualizes external storage and provides VM-aware, policy-based storage management.<br>3. Provides tool to get power consumed by workloads, infrastructure services and idling time, at the host or VM level.<br>4. Supports live migration of virtual machines with no disruption to users or loss of service, eliminating the need to schedule application downtime for planned server maintenance.<br>5. Supports automatic restart of VMs following physical machine failure.<br>**Witness Server**<br>1. The bidder shall furnish separate hardware that will act as witness and maintain quorum to ensure data availability and integrity.<br>2. The hardware specifications must meet the following minimum requirements:<br>a. Form Factor: 1U Rack Server<br>b. Drive Bays: Supports 8 units of 2.5" hot swap drives<br>c. Processor: 1x8-core @2.6GHz<br>d. Memory: 2x16GB RAM 1Rx8 PC5-5600B-R<br>e. RAID Controller: Supports RAID 0, 1, 5, 6, 10, 50, 60<br>f. Storage: 2x600GB SAS 10K SFF BC MV HDD and 3x1.2TB SAS 10K SFF BC MV HDD<br>g. Adapter: with Dual port 10G SFP+ NIC | |

| | | |
|---|---|---|
| | h. Transceivers: 2x 10G SFP+<br>i. I/O Ports:<br>1. Front: One Service port<br>2. Back: One VGA port, and One Management port<br>j. Power Supply: Two (2) or more power supply (Hot-Swappable/Hot-plug) Redundant<br>k. Management: Supports cloud-native management software that is continually updated with new services, features, patches, and fixes<br>l. Security:<br>1. Supports recovery of critical firmware to known good state on detection of compromised firmware<br>2. Ability to rollback firmware<br>3. Immutable Silicon Root of Trust<br>m. Industry Standard Compliance:<br>1. Energy Star 4.0<br>2. ACPI 6.4<br>3. PCIe 5.0<br>4. Embedded TPM Support<br>5. SMBIOS 3.4<br>6. Redfish API<br>7. SNMP v3<br>8. IPMI 2.0<br>9. TLS 1.2<br>52. The brand being offered must be in the five eyes alliance.<br>53. Warranty: Three (3) years warranty on parts and services. | |
| 4-B | **Component 4-B - IT Infrastructure and Services – Active Directory Server**<br><br>**Scope of Works - ACTIVE DIRECTORY SERVER**<br>1. Mounting of Server to the Data Cabinet<br>2. Server Management Configuration<br>3. Configuration of RAID & Hardware BIOS Options<br>4. Active Directory Domain Services Implementation<br><br>**Quantity:** One (1) Lot<br><br>**Specifications**<br>1. Hardware Specifications - Active Directory Server<br>a. Form Factor: 1U Rack Server<br>b. Drive Bays: Supports 8 units of 2.5" hot swap drives | |

| | | |
|---|---|---|
| | c. Processor: 1x12-core @2.0GHz<br>d. 2x16GB RAM 1Rx8 PC5-4800B-R<br>e. RAID Controller: Supports RAID 0, 1, 5, 6, 10, 50, 60<br>f. Storage: 2x600GB SAS 10K SFF BC MV HDD<br>g. Adapter: Quad port 1G Copper NIC<br>h. I/O Ports:<br>1. Front: One Service port<br>2. Back: One VGA port, and One Management port<br>i. Power Supply: Two (2) power supply (Hot-Swappable/Hot-plug) Redundant<br>j. Management: Supports cloud-native management software that is continually updated with new services, features, patches, and fixes.<br>k. Security:<br>1. Supports recovery of critical firmware to known good state on detection of compromised firmware<br>2. Ability to rollback firmware<br>3. Immutable Silicon Root of Trust<br>l. Industry Standard Compliance:<br>1. Energy Star 4.0<br>2. ACPI 6.4<br>3. PCIe 5.0<br>4. Embedded TPM Support<br>5. SMBIOS 3.4<br>6. Redfish API<br>7. SNMP v3<br>8. IPMI 2.0<br>9. TLS 1.2<br>m. With Server Operating System latest version<br>n. At least three (3) year warranty on parts and services.<br>**54. Operating System License**<br>a. The Server operating system must be core-based licensing.<br>b. Server operating system must have a minimum of 16-core based licensing.<br>c. Server operating system must be capable of installing roles and features of a directory services.<br>d. Server operating system must be capable of installing features that allows user to automate task-based command line shell and scripting language | |

| | | |
|---|---|---|
| | with built in commands compatible on the OS' framework.<br><br>**55. Active Directory Domain Services**<br>a. Must be a server role of the operating system of the server.<br>b. Must have capabilities to store directory data.<br>c. Must be capable to make data available to network users and administrators.<br>d. Must have capabilities to store objects like user accounts' names, passwords, phone number and login names.<br>e. Must have security integrated through logon authentication and access control to objects.<br>f. Must have five (5) Flexible Single Master Operation role namely:<br>1. Schema Master<br>2. Domain naming Master<br>3. Relative ID (RID) Master<br>4. Primary domain controller (PDC) Master<br>5. Infrastructure Master<br>g. Directory services must store user and computer objects information each classified by Organizational Unit | |
| 4-C | **Component 4-C - IT Infrastructure and Services – Web Server**<br><br>**Scope of Works**<br>1. Mounting of Server to the Data Cabinet<br>2. Server Management Configuration<br>3. Configuration of RAID & Hardware BIOS Options<br>4. OS Installation & Configuration<br><br>**Quantity:** Two (2) Units<br><br>**Specifications**<br>1. Form Factor: 1U Rack Server<br>2. Drive Bays: Supports 8 units of 2.5" hot swap drives<br>3. Processor: 2x12-core @2.0GHz<br>4. Memory: 2x16GB RAM 1Rx8 PC5-4800B-R<br>5. RAID Controller: Supports RAID 0, 1, 5, 6, 10, 50, 60<br>6. Storage: 2x600GB SAS 10K SFF BC MV HDD<br>7. Adapter: Quad port 1G Copper NIC<br>8. I/O Ports: | |

| | | |
|---|---|---|
| | a. Front: One Service port<br>b. Back: One VGA port, and One Management port<br>56. Power Supply: Two (2) redundant power supply (Hot-Swappable/Hot-plug)<br>57. Management: Supports cloud-native management software that is continually updated with new services, features, patches, and fixes.<br>58. Security:<br>a. Supports recovery of critical firmware to known good state on detection of compromised firmware<br>b. Ability to rollback firmware<br>c. Immutable Silicon Root of Trust<br>d. Industry Standard Compliance:<br>1. Energy Star 4.0<br>2. ACPI 6.4<br>3. PCIe 5.0<br>4. Embedded TPM Support<br>5. SMBIOS 3.4<br>6. Redfish API<br>7. SNMP v3<br>8. IPMI 2.0<br>9. TLS 1.2<br>59. With Server Operating System latest version<br>60. License: Standard Server Operating System of latest version<br>61. Three (3) years warranty on parts and services. | |
| 4-D | **Component 4-D - IT Infrastructure and Services – Network Switches and Devices – SD-WAN and Perimeter Firewall**<br><br>**Scope of Works**<br>1. Installation of Next Generation Firewall<br>2. Initial Configuration<br>3. Network Configuration<br>4. Configuration of Security & Firewall Rules<br>5. Configuration of High Availability<br>6. Testing & Verification of the Configuration & Connectivity<br>7. Knowledge Transfer<br><br>**Quantity:** Two (2) Units<br><br>**Hardware Specification** | |

| | | |
|---|---|---|
| | 1. Form Factor: 1U sliding rails<br>2. Interface Ports:<br>a. 4x1GbE Copper<br>b. 4xSFP+ 10 GbE fiber<br>62. Must have at least 8x10G 10GbE Fiber Transceiver Short Range<br>63. Internal Hot Swappable auto-ranging AC-DC 100-240VAC, 3.7-7.4A@50-60 Hz Internal Redundant PSU<br>64. Three (3) years warranty on parts and services<br>65. Three (3) years license subscription<br><br>**Performance Specifications**<br>1. The firewalls shall support at least:<br>a. 80 Gbps of Firewall Throughput<br>b. 37 Gbps of Firewall IMIX Throughput<br>c. 36 Gbps of IPS Throughput<br>d. 31 Gbps of Threat Protection Throughput<br>e. 75 Gbps of IPsec VPN Throughput<br>f. 17 million concurrent sessions<br>g. 450,000 new connections/sec<br>**General Management**<br>1. The Firewalls shall be purpose-built and shall have streamlined user interface and firewall rule management for large rule sets with grouping and with at-a-glance rule feature and enforcement indicators.<br>2. The firewalls shall have:<br>a. Full command-line-interface (CLI) accessible from GUI<br>b. Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN<br>c. Advanced trouble-shooting tools in GUI<br>d. Automated firmware update notification with easy automated update process and roll-back features<br>e. Self-service user portal<br>f. Configuration change tracking<br>g. Remote access option from the firewall vendor support.<br>h. Cloud-based license management via Licensing Portal<br>66. The firewalls shall support:<br>a. SNMPv3 and NetFlow | |

| | | |
|---|---|---|
| | b. Central Management via Cloud-based Unified Console<br>c. API for 3rd party integration<br>d. Interface renaming<br>e. High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup<br>**Central Firewall Management**<br>1. The firewall shall include a centralized management and shall be a cloud-based management and reporting for multiple firewalls, provides group policy management and a single console for all IT security products of the same brand.<br>2. The firewall management shall support:<br>a. Group policy management which allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group.<br>b. Firmware updates which offer one-click firmware updates to be applied to any device.<br>c. Zero-touch deployment which enables the initial configuration to be performed in cloud-based management and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to the central firewall management.<br>d. The central firewall management shall have:<br>1. Task Manager for providing a full historical audit trail and status monitoring of group policy changes.<br>2. Backup Firmware Management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access.<br>**Firewall, Networking & Routing**<br>1. The firewall shall support:<br>a. DPI Engine that provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine.<br>b. High performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade polices, unique dashboard visibility, and compatibility troubleshooting<br>c. Network Flow FastPath which delivers policy-driven and intelligent acceleration of trusted traffic automatically.<br>d. Enforcement of policy across zones, networks, or by service type.<br>e. Custom zones on LAN or DMZ. | |

| | | |
|---|---|---|
| | f. Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks.<br>g. Flood protection: DoS, DDoS and portscan blocking.<br>h. Country blocking by Geo-IP.<br>i. Upstream proxy support.<br>j. Protocol independent multicast routing with IGMP snooping.<br>k. Bridging with STP support and ARP broadcast forwarding.<br>l. 802.3ad interface link aggregation.<br>m. Dynamic DNS (DDNS)<br>n. Packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing.<br>o. Default zones for LAN, WAN, DMZ, LOCAL, VPN and Wi-Fi.<br>p. VLAN DHCP support and tagging.<br>q. VLAN bridge support.<br>**SDWAN**<br>1. The firewall shall support:<br>a. Multiple WAN link options including VDSL, DSL, cable, LTE/cellular, and MPLS.<br>b. Performance-based SLAs automatically select the best WAN link based on jitter, latency, or packet loss<br>c. Zero-impact re-routing maintains application sessions when link performance falls below thresholds and a transition is made to a better performing WAN link<br>d. Application routing over preferred links via firewall rules or policy-based routing.<br>e. SD-WAN monitoring graphs provide real-time insights into latency, jitter and packet loss for all WAN links.<br>f. Unique Remote Ethernet Device Layer 2 tunnel with routing.<br>g. Robust VPN support including IPsec and SSL VPN.<br>**Base Traffic Shaping & Quotas**<br>1. The firewall shall support:<br>a. Flexible network or user-based traffic shaping (QoS)<br>b. Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical.<br>c. Real-time VoIP optimization. | |

**Authentication**

1. The firewall shall support:
    a. Sharing of currently logged in AD user IDs between the endpoints of the same brand without an agent on the AD server or client.
    b. Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+.
    c. Server authentication agents for Active Directory SSO, Transparent authentication and Thin Client Authentication.
    d. Single sign-on: Active directory, eDirectory, RADIUS Accounting
    e. Client authentication agents for Windows, Mac OS X, Linux 32/64.
    f. Browser SSO authentication: Transparent, proxy authentication (NT LAN Manager) and Kerberos.
    g. Authentication certificates for iOS and Android.
    h. API-based authentication.
    i. The firewall shall have Google Chromebook authentication support for environments with Active Directory and Google G Suite

**User Self-Serve Portal**

1. The firewall shall have a self-serve portal:
    a. To download SSL remote access client (Windows) and configuration files (other OS).
    b. To view personal internet usage
    c. For hotspot access information
    d. For changing username and password

**Base VPN Options**

1. The firewall shall have Remote access: SSL, IPsec, iPhone/iPad/Android VPN client support
2. The firewall shall support:
    a. Site-to-site VPN: SSL, IPsec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
    b. Can manage remote site with VPN appliance with robust and lightweight feature.
    c. L2TP and PPTP

**VPN Client**

1. The firewall VPN client shall support:

| | | |
|---|---|---|
| | a. Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH<br>b. Intelligent split-tunneling for optimum traffic routing.<br>c. Mac (IPsec) and Windows (SSL/IPsec) client support<br>d. The firewall VPN client shall be able to enable the connection of firewall and endpoint security and monitoring of the health status of the managed endpoints for remote connected users.<br>e. The firewalls shall have Client-monitor for graphical overview of connection status.<br><br>**Network Protection Subscription - Intrusion Prevention (IPS)**<br>1. The firewall shall have the following:<br>a. High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection.<br>b. Thousands of signatures<br>c. Support for custom IPS signatures.<br>d. IPS Policy Smart Filters which enable dynamic policies that automatically update as new patterns are added.<br>**Active Threat Response and Security Heartbeat**<br>1. The firewall shall have the following:<br>a. Active Threat Response automatically monitors/blocks APT and other threats identified via OEM Labs global threat database for advanced threat protection from bots and active adversaries attempting to contact malicious destinations using multi-layered DNS, AFC, and firewall detections<br>b. Security Heartbeat conditions can be attached to any firewall rule, automatically limiting access to network resources and segments for a device that has been compromised until it is cleaned up<br>c. Automatically initiates lateral movement protection in the event a managed endpoint is compromised by informing all healthy managed endpoints to reject traffic from the compromised device effectively stonewalling the device - even on the same LAN segment<br>**Clientless VPN**<br>1. The firewall shall support unique encrypted HTML5 self-service portal with support for RDP, SSH, Telnet, and VNC<br>**Web Protection Subscription - Web Protection and Control (Web Content Filtering)** | |

| | | |
|---|---|---|
| | 1. The firewall's Web Protection and Control shall support:<br>a. Streaming DPI web protection or explicit proxy mode inspection<br>b. Forced caching for managed endpoint updates<br>c. SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)<br>d. Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists<br>e. User/Group policy enforcement on Google Chromebooks.<br>67. The firewall web protection and control shall have:<br>a. Enhanced Advanced Threat Protection<br>b. URL Filter database with millions of sites across from at least 90 categories backed by OEM Labs<br>c. Advanced web malware protection with JavaScript emulation<br>d. Live Protection real-time in-the-cloud lookups for the latest threat intelligence<br>e. Second independent malware detection engine for dual scanning<br>f. High performance web content caching.<br>68. The firewall shall support web policy override option to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users.<br>**Cloud Application Visibility**<br>1. The firewall shall support:<br>a. Control Center widget which displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated; and<br>b. One-click access to traffic shaping policies.<br>69. The firewall shall be able to:<br>a. Discover Shadow IT at a glance<br>b. Drill down to obtain details on users, traffic, and data<br>c. Filter cloud application usage by category or volume<br>d. Provide detailed customizable cloud application usage report for full historical reporting.<br>**Application Protection and Control**<br>1. The firewall shall be able to automatically identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints of the same brand.<br>2. The firewall shall support: | |

| | | |
|---|---|---|
| | a. Signature-based application control with patterns for thousands of applications<br>b. Cloud Application Visibility and Control to discover Shadow IT<br>c. App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added<br>d. Micro app discovery and control; and<br>e. Application control based on category, characteristics, technology, and risk level.<br>**Web & App Traffic Shaping**<br>1. The firewalls shall support Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared.<br>**Zero-Day Protection Subscription - Dynamic Sandbox Analysis**<br>1. Dynamic Sandbox Analysis shall support:<br>f. Full integration into security solution dashboard<br>g. Machine Learning technology with Deep Learning scans all dropped executable files<br>h. One-time download links.<br>i. Dynamic Sandbox Analysis shall be able to:<br>j. Inspect executables and documents containing executable content including .exe, .com, and .dll, .doc, .docx, .rtf and PDF-and archives containing any of the file types listed above including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet<br>k. Provide In-depth malicious file reports and dashboard file release capability<br>l. Provide optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis<br>m. Detect sandbox evasion behavior.<br>**Reporting**<br>1. Central Firewall Reporting<br>2. The firewall must have a centralized management that shall have pre-defined reports with flexible customization options.<br>3. The firewall with centralized management shall:<br>a. Be able to provide report dashboard which has an at-a-glance view of events for at least the past 24 hours.<br>b. Be able to easily identify network activities, trends, and potential attacks.<br>c. Have easy backup of logs with quick retrieval for audit needs. | |

| | | |
|---|---|---|
| | **\Threat Intelligence Analysis**<br>1. All files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content including .exe, .com, and .dll, .doc, .docx, .docm, .rtf and PDF and archives containing any of the file types listed above including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet-are automatically sent for Threat Intelligence Analysis (TIA).<br>2. Files are checked against massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware.<br>3. Threat Intelligence Analysis shall be able to provide extensive reporting including a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model.<br>**General Specifications:**<br>1. The firewall shall have:<br>a. Machine Learning and Sandboxing File Analysis, reporting.<br>b. TLS and DPI engine, Web Security and Control, Application Control, reporting.<br>c. Networking, Unlimited Remote Access VPN, Site-to-Site VPN, reporting.<br>**Additional Requirements:**<br>1. The prospective bidder must have at least two (2) certified architects of the above solution.<br>2. The brand of the firewall must have:<br>a. At least thirty (30) years of experience and worldwide visibility of emerging threats.<br>70. The NGFW manufacturer must have certifications on the following industry standards:<br>a. FIPS 140-2<br>b. Common Criteria (ISO 15408) EAL 4+ | |
| 4-E | **Component 4-E - IT Infrastructure and Services – Network Switches and Devices – Network Switches**<br>**Scope of Works**<br>1. Installation of Physical Hardware<br>2. Initial Configuration of the Switches<br>3. Advanced Configuration of the Switches<br>4. Testing & Verification of the Configuration & Connectivity<br>5. Knowledge Transfer | |

| | | |
|---|---|---|
| | **Quantity:**<br>The brand being offered must be in the five eyes alliance:<br>1. Core Switch - Two (2) Units<br>2. WAN Switch – Two (2) Units<br>3. DMZ Switch - Two (2) Units<br>4. Top of Rack Switch (TOR) - Two (2) Units<br>5. Management Switch – One (1) Units<br><br>**Hardware Specification – Core Switch**<br>1. Switching capacity: at least 4 Tbps<br>2. CPU: at least 2.2Ghz<br>3. Memory: 16GB RAM<br>4. Flash Memory: 8GB<br>5. Hard Drive: 64GB SSD<br>6. Packet Buffer: 32MB<br>7. Interfaces:<br>a. At least 48x ports 1G/10G/25GbE (SFP/SFP+/ SFP28)<br>b. At least 8x 40G/100GbE (QSFP+/QSFP28)<br>71. Must have at least 7x 10G, 300m SFP+ OM3 MMF LC Transceivers and 2x 100Gb QSFP28 Transceivers<br>72. MAC Address: at least 98K<br>73. IPv4 unicast routes: at least 131k<br>74. IPv6 unicast routes: at least 32k<br>75. Must have at least 2x hot-swappable power supply slots and at least 6x hot-swappable fan tray slots<br>76. Must support the following:<br>a. Routing Information Protocol version 2 (RIPv2)<br>b. Open shortest path first (OSPF)<br>c. Border Gateway Protocol 4 (BGP-4)<br>d. IEEE 802.1s Multiple Spanning Trees<br>e. IEEE 802.3ad Link Aggregation Control Protocol (LACP)<br>f. IEEE 802.1Q VLANs<br>g. Remote monitoring (RMON)<br>h. SNMPv2c/v3<br>i. REST APIs and Python scripting for fine grained programmability of network tasks<br>j. Advanced Layer 2/3 feature set includes VRF-Lite, and IPv6<br>k. Jumbo frames allow for high-performance backups and disaster-recovery systems; provides a minimum frame size of at least 9,000 bytes | |

| | | |
|---|---|---|
| | l. VSX redundancy for high availability<br>m. Intelligent monitoring, visibility and remediation with Network Analytics Engine<br>n. Complete telemetry for all system information<br>o. Automation of configuration changes across multiple devices<br>p. FIPS 140-2 validated cryptography for protection of sensitive information<br>77. Full line rate with all network ports populated under worst case power conditions<br>78. The brand being offered must be in the Five Eyes alliance<br>79. Three (3) years warranty on parts and services<br>**Hardware Specification – WAN Switch**<br>1. Switching capacity: at least 128 Gbps<br>2. Throughput Capacity: up to 95 Mpps<br>3. CPU: Quad Core ARM Cortex, at least 1.8Ghz<br>4. Memory: 8GB DDR4<br>5. Flash Memory: 16GB eMMC<br>6. Packet Buffer: 8MB Total (6MB Available, 2MB Reserved)<br>7. Interfaces:<br>a. At least 24x ports 10/100/1000BASE-T Ports<br>b. At least 4x 100M/1G/10G SFP ports (2x LRM; 2x LRM/MACSec 256)<br>80. MAC Address: at least 32K<br>81. IPv4 Unicast Routes: at least 2k<br>82. IPv6 Unicast Routes: at least 1k<br>83. Must have at least 2x hot-swappable power supply slots and at least 2x hot-swappable fan tray slots<br>84. Must support simple deployment and management via a mobile app<br>85. Must support the following:<br>a. Routing Information Protocol version 2 (RIPv2)<br>b. Open shortest path first (OSPF)<br>c. IEEE 802.1s Multiple Spanning Trees<br>d. IEEE 802.3ad Link Aggregation Control Protocol (LACP)<br>e. IEEE 802.1Q VLANs<br>f. Remote monitoring (RMON)<br>g. SNMPv2c/v3<br>h. FIPS 140-2<br>i. Virtual Switching Framework stacking | |

| | | |
|---|---|---|
| | j. Stacking up to 8 members or higher<br>k. Flexibility to mix modular and fixed switches of the same model family within a single stack<br>l. Telemetry and automation for identifying and troubleshooting issues within the network or system<br>m. Dynamic Segmentation solution enables seamless mobility, consistent policy enforcement, and automated configurations for wired and wireless clients across networks of all sizes<br>n. At least 4094 VLAN IDs<br>o. An integrated trusted platform module or equivalent<br>p. The brand being offered must be in the Five Eyes alliance<br>q. Three (3) years warranty on parts and services<br>**Hardware Specification – DMZ Switch**<br>1. Switching capacity: at least 880 Gbps<br>2. Throughput Capacity: up to 654 Mpps<br>3. CPU: Quad Core ARM Cortex A72, at least 1.8Ghz<br>4. Memory: 8GB DDR4<br>5. Flash Memory: 32GB eMMC<br>6. Packet Buffer: 8MB<br>7. Interfaces:<br>a. At least have 24x 1G/10G SFP+ ports<br>b. At least have 4x 1G/10G/25G/50G SFP ports<br>86. Must have at least 4x 10G, 300m SFP+ OM3 MMF LC Transceivers<br>87. MAC Address: at least 32K<br>88. IPv4 Unicast Routes: at least 61k<br>89. IPv6 Unicast Routes: at least 61k<br>90. IPv4 Multicast Routes: at least 8k<br>91. IPv6 Multicast Routes: at least 8k<br>92. Must have at least 2x hot-swappable power supply slots and at least 2x hot-swappable fan tray slots<br>93. Must support simple deployment and management via a mobile app<br>94. Must support the following:<br>a. Routing Information Protocol version 2 (RIPv2)<br>b. Open shortest path first (OSPF)<br>c. IEEE 802.1s Multiple Spanning Trees<br>d. IEEE 802.3ad Link Aggregation Control Protocol (LACP)<br>e. IEEE 802.1Q VLANs<br>f. Remote monitoring (RMON) | |

| | | |
|---|---|---|
| | g. SNMPv2c/v3<br>h. FIPS 140-2<br>i. Virtual Switching Framework stacking<br>j. Stacking up to 8 members or higher<br>k. Flexibility to mix modular and fixed switches of the same model family within a single stack<br>l. Intelligent monitoring, visibility and remediation with Networking Analytics Engine<br>m. Complete telemetry for all system information<br>n. At least 4094 VLAN IDs<br>o. Secure and simple access for IoT and users<br>p. Enforcement of unified policies<br>q. An integrated trusted platform module or equivalent<br>r. The brand being offered must be in the Five Eyes alliance<br>s. Three (3) years warranty on parts and services<br>**Hardware Specification – TOR Switch**<br>1. Switching capacity: at least 4.8 Tbps<br>2. Processing Capacity: at least 3.5 Bpps<br>3. System Memory: 8GB<br>4. SSD Memory: 32GB<br>5. Packet Buffer: 42MB<br>6. Interfaces:<br>a. At least have 48x 1G/10G/25G SFP28 ports<br>b. At least have 12x 40G/100G QSFP28 ports<br>95. Must have at least have 36x 10G SFP+ SR Transceiver<br>96. Must have at least have 10x 10GBASE-T SFP+ RJ45 30m Cat6A Transceiver<br>97. Must have at least have 8x 1G SFP RJ45 T 100m Cat5e Transceiver<br>98. Must have at least 2x 100G QSFP28 100m Transceiver<br>99. Must have at least 2x hot-swappable power supply slots<br>100. Must support zero-touch installation and provisioning<br>101. Must support VM and host mobility<br>102. Must be able to run multiple network paths without needing multiple switches<br>103. Must support VXLAN, including VXLAN routing and VXLAN head-end replication<br>104. Must support the following orchestration packages: Ansible, Chef, CFEngine, and Puppet<br>105. The brand being offered must be in the Five Eyes alliance<br>106. Three (3) years warranty on parts and services | |

| | | |
|---|---|---|
| | **Hardware Specification – Management Switch**<br>1. Switching capacity: at least 128 Gbps<br>2. Throughput Capacity: up to 95 Mpps<br>3. CPU: Quad Core ARM Cortex, at least 1.8Ghz<br>4. Memory: 8GB DDR4<br>5. Flash Memory: 16GB eMMC<br>6. Packet Buffer: 8MB Total (6MB Available, 2MB Reserved)<br>7. Interfaces:<br>a. At least 24x ports 10/100/1000BASE-T Ports<br>b. At least 4x 100M/1G/10G SFP ports (2x LRM; 2x LRM/MACSec 256)<br>107. MAC Address: at least 32K<br>108. IPv4 Unicast Routes: at least 2k<br>109. IPv6 Unicast Routes: at least 1k<br>110. Must have at least 2x hot-swappable power supply slots and at least 2x hot-swappable fan tray slots<br>111. Must support simple deployment and management via a mobile app<br>112. Must support the following:<br>a. Routing Information Protocol version 2 (RIPv2)<br>b. Open shortest path first (OSPF)<br>c. IEEE 802.1s Multiple Spanning Trees<br>d. IEEE 802.3ad Link Aggregation Control Protocol (LACP)<br>e. IEEE 802.1Q VLANs<br>f. Remote monitoring (RMON)<br>g. SNMPv2c/v3<br>h. FIPS 140-2<br>i. Virtual Switching Framework stacking<br>j. Stacking up to 8 members or higher<br>k. Flexibility to mix modular and fixed switches of the same model family within a single stack<br>l. At least 4094 VLAN IDs<br>m. An integrated trusted platform module or equivalent<br>n. Three (3) years warranty on parts and services<br>o. The brand being offered must be in the Five Eyes alliance<br>p. Three (3) years license subscription | |
| 4-F | **Component 4-F - IT Infrastructure and Services – Network Switches and Devices – Web Application Firewall with Server Load Balancers** | |

**Scope of Works**

1. Installation of Web Application Firewall
2. Initial Configuration
3. Establish High Availability Link / Peering
4. Configuration of Interfaces & Routing
5. Configuration of Load Balancer
6. Configuration of Web Application Firewall (WAF)
7. Testing & Verification of the Configuration & Connectivity
8. Knowledge Transfer

**Quantity:** Two (2) Units

**Specification**

1. **Must have the following minimum specifications:**
    a. Form Factor: Rack-mountable 1U
    b. Layer 4 Throughput: At least 15 Gbps
    c. Layer 7 Throughput: At least 15 Gbps
    d. Concurrent Layer 4 Connections: At least 35M
    e. Concurrent Layer 7 Connections: At least 262K
    f. Layer 7 HTTP Requests/second: at least 1M
    g. Layer 4 Requests/second: at least 2M
    h. Layer 4 Connections/second: at least 600k
    i. SSL TPS (2K keys): At least 15K
    j. CPU: at least four-core, eight-threads @3.8Ghz
    k. Storage: At least 2 x 1TB HDD (RAID 1)
    l. Memory: At least 32GB RAM
    m. Interfaces/Ports:
        1. Supports at least 16x 1GbE + 4x 10GbE ports

**113. Real-time application threat mitigation**

    a. Updated reputation data daily
    b. Threats mitigated: Cookie tampering, Cross site request forgery, Cross site scripting, Data loss prevention, SQL injection, PCI-DSS Section 6.6 compliance

**114. L4-L7 Application Delivery**

    a. Server Load Balancing (SLB) for TCP/UDP based protocols
    b. TLS (SSL) Offload,
    c. Layer 7 Content Switching
    d. Transparent caching for HTTP/HTTPS

| | | |
|---|---|---|
| | e. Compression of static and dynamic HTTP/HTTPS content, HTTP/2 Support<br>f. NAT-based forwarding<br>g. Support for Direct Server Return (DSR) Configurations<br>h. Configurable S-NAT support, VLAN Trunking (802.1Q), Link interface bonding (802.3ad), USGv6 certified, IPv6 support for addressing and features, IPv6 to IPv4 gateway/proxy using a NIST USGv6 network stack<br>**115. Health Checking**<br>a. Aggregated health checks, ICMP health checking, Layer 7 checking against any target server port, Active/Hot Standby configurations for High Availability, Stateful Failover, Scale-out Clustering<br>**116. Session Persistence**<br>a. Source IP (L4)<br>b. TLS (SSL) SessionID (L4)<br>c. HTTP/HTTPS Browser-session (L7)<br>d. HTTP/HTTPS WebClient-session (L7)<br>e. RDP Login ID (L7)<br>f. Port Following for mixed HTTP/HTTPS sessions<br>**117. Scheduling and Balancing Methods**<br>a. Round Robin<br>b. Weighted Round Robin<br>c. Least Connection<br>d. Weighted Least Connection<br>e. Agent-based Adaptive<br>f. Chained Failover (Fixed Weighting)<br>g. Source-IP Hash, Layer 7 Content Switching<br>h. Global Server Load Balancing (GSLB)<br>i. SSL/TLS Features<br>j. Configurable TLS (1.0, 1.1, 1.2, 1.3) and SSL (2.0, 3.0)<br>k. Support for Extended Validation (EV) certificates<br>l. Server Name Identification (SNI) support<br>118. Administration<br>a. Web User Interface (WUI)<br>b. Context based help (WUI)<br>c. SNMP support, SSH Console<br>d. RESTful and PowerShell APIs<br>e. Change Auditing | |

| | | |
|---|---|---|
| | f. Real time display of performance and availability, Application templates, Automated configuration backup, Connection draining, Diagnostic shell with in-line TCPdump<br><br>119. Security<br><br>a. Common Criteria (ISO/IEC 15408) Certified, Allow/Deny List (Access Control List), IP address filtering, IPsec Tunnel support, DDoS mitigation, including L7 rate-based attacks, IPSec VPN to Azure, AWS, and public clouds, Authenticated NTP<br><br>120. Warranty<br><br>a. Three (3) years warranty on parts and services and three (3) years license subscription<br><br>b. With at least three (3)-year support subscription including:<br><br>1. 24x7 Customer Support<br><br>2. Software Updates, Security Patches<br><br>3. L4-L7 Application Delivery<br><br>4. Network Telemetry<br><br>5. Intrusion Prevention<br><br>6. Web Application Firewall (WAF) with updated reputation data daily | |
| 4-G | **Component 4-G - IT Infrastructure and Services – Managed Kubernetes System and DBAAS System**<br><br>**Scope of Works**<br><br>1. Installation and configuration of the Kubernetes platform, including CI/CD pipelines and DBAAS<br><br>2. Ensuring the high availability and optimal performance of Kubernetes clusters and related services<br><br>3. Configure proactive monitoring to maintain infrastructure reliability<br><br>4. Continuous improvement through automation and performance optimization<br><br>5. Capacity planning to support scalability and disaster recovery measures<br><br>**Quantity:** One (1) Lot<br><br>**Number of Environment**<br><br>1. Non-Prod<br><br>2. Prod<br><br>3. Disaster Recovery<br><br>**Required Kubernetes Platform Components**<br><br>1. Container Runtime<br><br>2. Container Management/Orchestration | |

| | | |
|---|---|---|
| | 3. DBAAS<br>4. Logging<br>5. Monitoring<br>6. API Gateway<br>7. CI/CD<br>8. Container Registry<br>9. Version Control<br>10. Incident Management/On Call<br><br>**Specification for the Managed Kubernetes System**<br>The service provider will be responsible for the following tasks:<br>1. **Discovery & Design:**<br>a. Conduct on-site assessment (up to two weeks) to understand requirements and decide on platform capabilities<br>**121. Installation & Configuration:**<br>a. Set up Kubernetes clusters and platform components<br>b. Configure and provision a working CI/CD pipelines<br>c. Configure DBAAS to support the deployment of apps<br>**122. System Monitoring & Alerting:**<br>a. Set up monitoring tools and define alerting mechanisms<br>b. Setup monitoring for DBAAS<br>c. Implement incident escalation and response protocols<br>**123. Incident Management & Resolution:**<br>a. Promptly respond to incidents, troubleshoot failures, and perform root cause analysis during the managed services duration<br>**124. Capacity Planning & Performance Optimization**<br>a. Analyze system performance and forecast resource needs for scalability based on observed capacity usage<br>**125. Infrastructure Automation**<br>a. Implement automation tools for infrastructure management and routine tasks.<br>**126. Disaster Recovery & Business Continuity:**<br>a. Develop a disaster recovery plan, perform backups, and test failover mechanisms.<br>**127. Warranty** | |

| | | |
|---|---|---|
| | a. One (1) year Managed Services for the operation of the LRA's Kubernetes System including the delivery of the following services:<br>1. Set up the platform – including Kubernetes Clusters, Platform Components – CI/CD, Logging, Monitoring and Alerts<br>2. Incident reports with resolution details during managed services duration.<br>3. Performance and availability reports with recommendations.<br>4. Documentation of system configurations and response procedures.<br><br>**Specification for the Managed DBAAS System**<br>1. Tenderer shall propose a solution that is 100% opensource with Enterprise Support.<br>2. The proposed solution must be cloud agnostic and cloud native and is able to support deployments in bare metal, VMs or Kubernetes on premise as well as across cloud for at least the following options:<br>a. VMware vSphere, AWS, Google Cloud Platform, Microsoft Azure<br>128. The proposed solution must be able to synchronize the data across multiple sites, and support multiple advanced replication architectures<br>129. The solution must be deployed in an active-active manner to ensure minimal disruption to services and is able to support the following failure scenarios:<br>a. Virtual Machine Failure<br>b. Server Rack Failure<br>c. Container/Kubernetes node Failure<br>d. Data Center or Availability Zone Failure<br>130. The proposed solution must support both the SQL and NoSQL API's under a common storage substrate to ensure support for different database services currently and in future<br>131. The proposed solution must enable client applications to auto-discover cluster nodes and cluster topology<br>132. The proposed solution must be able to support a single synchronous cluster stretched across multiple AZ's/regions/data centers/ cross clouds, and support multiple advanced replication architectures for resiliency of the system<br>133. The proposed solution must be capable of horizontally scaling with no downtime to support adhoc peak workloads or increase in sizing without interruption<br>134. The proposed solution must offer a single user interface across various clouds with simplified database management and monitoring like DB upgrades, backups, | |

| | | |
|---|---|---|
| | security & on-demand scaling of nodes to simplify operation and management<br>135. The proposed solution must support distributed ACID with both serializable & snapshot isolation<br>136. The proposed solution must include minimum 1 years Enterprise 24x7 Support<br>137. The proposed solution must provide ability to increase computing capacity in a linear fashion by adding new nodes to the existing database system with no downtime | |
| 5 | **Operational Management and Support** | |
| 5-A | **Component 5-A - Operational Management and Support – Construction of NOC/SOC Center**<br><br>**Scope of Works -** Supply, installation, configuration, testing and commissioning of LRA NOC/SOC Center<br><br>**Quantity:** One (1) Lot<br><br>1. Professional Videowall Display Units – Four (4) units<br>2. Video Matrix System – One (1) unit<br>3. Furniture – One (1) lot<br>4. Laptop – Five (5) units<br>5. Secondary Monitor – Five (5) units<br><br>**Specifications**<br>1. **Professional Videowall Display**<br>a. Screen Size: at least 55"<br>b. Panel Technology: IPS<br>c. Aspect Ratio: 16:9<br>d. Native Resolution: at least 1,920 x 1,080 (FHD)<br>e. Brightness (Typ.): at least 700nits<br>f. Contrast Ratio: 1,100:1<br>g. Viewing Angle (H x V):178 X 178<br>h. Surface Treatment (Haze): 28%<br>i. Operation Hours (Hours / Days): 24/7<br>j. Portrait / Landscape: Yes / Yes<br>k. Must have video pop out bracket for installation<br>**138. Video Matrix System**<br>a. HDMI cables as required<br>b. Connects any of 8 HDMI sources to any of 8 HDMI displays<br>c. Unifies video formats to provide continuous video streams, real-time switching and stable signal transmissions | |

| | | |
|---|---|---|
| | d. HDMI (3D, Deep color); HDCP 1.4 compatible<br>e. Multiple Control Methods – system management via front-panel pushbuttons, IR, RS-232 and Ethernet (Telnet / Web GUI) connections<br>f. ESD protection for HDMI<br>g. Video resolution – at least 1080p (1920 x 1080)<br>**139. Furniture**<br>a. The bidder shall supply 4 sets of tables with the following specifications:<br>1. 1200mm width x 60mm depth<br>2. White or wood color<br>3. With 3-layer pedestal<br>**140. Laptop**<br>a. The processor should have the following specifications:<br>1. E-Core: 8x cores @3.6Ghz Max Turbo Frequency<br>2. P-Core: 2x cores @4.3Ghz Max Turbo Frequency<br>3. L3 Cache: 12MB<br>4. Memory: 1x16HB 5600 DDR5 memory<br>5. Graphics: Integrated Graphics<br>6. Storage: 1TB PCIe Gen4x4N NVMe M2. SSD<br>**7.** Screen: 14inch 1920x1200 WUXGA LED UWVA 300, 60Hz, with anti-glare, 400 nits and low power usage<br>b. Preloaded with the latest version of a professional operating system<br>c. Should include an integrated 5MP IR camera<br>d. Should include an integrated dual array microphones and dual stereo speakers with discrete amplifiers<br>e. At least 3 Cell and 56 watt-hour Fast Charging battery<br>f. AC Adapter / Power Supply: 45W nPFC USB-C Straight AC Adapter<br>g. Spill-resistant Backlit Keyboard<br>h. Should have a wireless slim mouse<br>i. Wi-Fi 6E, Bluetooth® 5.3 wireless card<br>j. 2x USB Type-C® 20Gbps signaling rate, 2x USB Type-A 5Gbps signaling rate, 1x HDMI 2.1, 1x stereo headphone/microphone combo jack, 1x RJ-45<br>k. Must have a top load bag<br>l. The brand being offered must be compliant with ENERGY STAR certified, EPEAT registered | |

| | | |
|---|---|---|
| | **141. Secondary Monitor**<br>a. Display size: 23.8"<br>b. Resolution (maximum): FHD (1920 x 1080 @ 75 Hz)<br>c. Power consumption: 30 W (maximum), 20 W (typical), 0.5 W (standby)<br>d. ENERGY STAR certified, EPEAT registered<br>e. Three (3) years warranty on parts and services. | |
| 6 | **Disaster Recovery and Business Continuity** | |
| 6-A | **Component 6-A - Disaster Recovery and Business Continuity – Backup Server and Backup Software Solution**<br><br>**Scope of Works**<br>1. Mounting of Server to the Data Center<br>2. Server Management Configuration<br>3. Configuration of RAID & Hardware BIOS Options<br>4. OS Installation & Configuration<br>5. Installation & Configuration of Backup Software<br><br>**Quantity: One (1) Lot**<br><br>**Hardware Specifications - Backup Server**<br>1. Form Factor: 1U Rack Server<br>2. Drive Bays: Supports 8 units of 2.5" hot swap drives<br>3. Processor: 1x12-core @2.0GHz<br>4. Memory: 2x16GB 1Rx8 PC5-4800B-R<br>5. RAID Controller: Supports RAID 0, 1, 5, 6, 10, 50, 60<br>6. Storage: 2x600GB SAS 10K SFF BC MV HDD<br>7. Adapter: Quad port 1G Copper NIC<br>8. I/O Ports Front: One Service port<br>9. Back: One Management port<br>10. Power Supply: Two (2) power supply (Hot-Swappable/Hot-plug) Redundant<br>11. Management: Supports cloud-native management software that is continually updated with new services, features, patches, and fixes.<br>12. Security:<br>a. Supports recovery of critical firmware to known good state on detection of compromised firmware<br>b. Ability to rollback firmware<br>c. Immutable Silicon Root of Trust<br>142. Industry Standard Compliance: | |

| | | |
|---|---|---|
| | a. Energy Star 4.0,<br>b. ACPI 6.4,<br>c. PCIe 5.0,<br>d. Embedded TPM Support,<br>e. SMBIOS 3.4,<br>f. Redfish API,<br>g. SNMP v3,<br>h. IPMI 2.0<br>i. With Server Operating System latest version<br>j. The brand being offered must be included in Five Eyes alliance.<br>k. Three (3) year warranty on parts and services for backup server<br>**Backup Software Specification**<br>The Backup Software Solution must support:<br>1. Built-in data deduplication and compression to decrease the backup storage requirements and network traffic<br>2. Agentless protection without the need to install individual agents inside each Guest VMs<br>3. Ability to do instant VM recovery by running directly from compressed and deduplicated backup files<br>4. Direct attached storage, Network attached storage, deduplicating storage appliances and Object storage as backup repositories<br>143. The Backup Software Solution should provide:<br>a. A centralized console to coordinate backup, replication, recovery verification and restore tasks. It is also used to set up and manage backup infrastructure components.<br>b. License calculated based per instance, up to 20 instances<br>c. Built-in AES 256-bit encryption, compression, and deduplication in a single product without an additional option to purchase<br>d. Three (3) years subscriptions for backup software | |
| 6-B | **Component 6-B - Disaster Recovery and Business Continuity – Backup Repository**<br><br>**Scope of Work**<br>1. Mounting of Storage to the Data Cabinet<br>2. Storage Management Configuration<br>3. Expanding of Existing Storage Pool<br>4. Configuration of LUNs / File System<br>5. Mapping of LUN to Host | |

| | | |
|---|---|---|
| | **Quantity: One (1) Lot**<br><br>**Hardware Specifications - Backup Repository**<br>1. Quantity: 1 unit<br>2. Form Factor: 2U Rackmount<br>3. Processor: at least 4x cores @3.35 GHz<br>4. Memory: at least 2x16GB DDR4 (32GB total)<br>5. RAID: Supports RAID 0, 1, 5, 6, 10<br>6. Hard Drive: at least 11x 20TB Enterprise-grade SATA HDD<br>7. NIC:<br>a. Dual-port 1GbE Base-T<br>b. Single-port 10GbE Base-T<br>c. Additional Network Card – Dual-port 10GbE Base-T<br>144. Ports:<br>a. Two USB 3.2 ports<br>b. One Mini-SAS Expansion port<br>145. Expansion Unit: 1x 12-bay SATA<br>146. Accessory: 2x Sliding Rail Kit<br>147. Must support the following:<br>a. File System: BTRFS, ext4<br>b. Protocols:<br>c. SMB1, SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized Sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV,<br>d. Shared Accounts and Folders:<br>e. Up to 2048 Local User Accounts<br>f. Up to 256 Local Groups and up to 512 Shared Folders<br>g. File Services: 2000 concurrent connections<br>h. At least three (3) year warranty on parts and services | |
| 7 | **Data Center Storage Solution** | |
| 7-A | **Component 7-A – Data Center Storage Solution – Data Center NAS Storage**<br><br>**Scope of Works**<br>1. Mounting of Server to the Data Cabinet<br>2. Storage Node Cluster Setup<br>3. Configuration of Storage Node Cluster<br>4. Configuration of IP Addresses | |

| | | |
|---|---|---|
| | **Quantity: One (1) Lot**<br><br>**Specifications of Storage Solution**<br><br>1. The scale-out storage solution must be a multi-controller scale-out Network attach storage being sold as an integrated appliance with required compute, network and storage hardware.<br>2. The vendor of the storage solution must be listed as a leader in Gartner's in 2023 Magic Quadrant for Distributed File Systems and Object Storage.<br>3. The storage solution must have a scale-out capability that can provide linear performance and capacity together, as well grow node-by-node.<br>4. The storage solution must scale from at least 4 nodes, up to 250+ nodes, with zero downtime and no data migration.<br>5. The system must be able to load balance the requests coming from multiple clients amongst nodes in the cluster.<br>6. Each node must support at least 10 Floating IP addresses.<br>7. The system must have at least 116TB usable storage capacity after the desired performance and protection policies are applied<br>8. The storage solution must be supplied with 800GB NVMe SSD, 240GB SATA SSD, and 8TB HDD<br>9. Each node must be supplied with 64GB memory and 2x 10G/25G Network Ports<br>10. Must be able to use 100% of the usable storage capacity without any impact.<br>11. Must tolerate 2 drive failures per node and 1 node failure<br>12. The usable capacity of the storage solution must be provided in a "single namespace" and must be scalable by adding required nodes and hardware accessories within a given cluster.<br>13. The storage solution must be truly scalable and tuned for both small and large files and must support more than four billion files into any given directory.<br>14. The storage solution must be able to support extremely large file sizes<br>15. The system must eliminate time and resource intensive "file system tree walks" for the following processes: SSD failure, HDD failure, Node failure, Node Add<br>16. The system must support NFS V3 & V4.1, SMB 3, and S3 API natively.<br>17. The system must support at least 64000 NFS exports and 40000 SMB shares.<br>18. The system must support NTFS ACLs and Share Level Permissions (SHACLs) for preventing access/security issues and must be compatible with LDAP and Active Directory. | |

| | | |
|---|---|---|
| | 19. The system must support Kerberos-based authentication for NFSv4 clients by using a key-and-ticket system to securely authenticate users from Active Directory.<br>20. The system must support non-disruptive node expansion.<br>21. The system must utilize a hybrid architecture of SSD for performance in combination with the traditional spinning disk. All writes should be written to SSD and then staged to spinning disk<br>22. The system must use erasure coding for data protection for any size of the file and must utilize block layer protection that allows the file system to scale to billions of files and millions of directories without compromising data protection, performance or scalability.<br>23. The system must have an audit log and must be able to direct these logs to an external Syslog supported system.<br>24. The system must be a fully consistent POSIX-compliant filesystem that supports instantaneous directory renaming and directory-level snapshots.<br>25. The storage solution must support at least 40000 snapshots.<br>26. The system must provide AES 256-bit encryption for Data at rest, Data in transit and replicating data to another location or public cloud.<br>27. The storage solution must provide the functionality for rotating the key encryption key, if required by the security and compliance team.<br>28. The storage solution must be FIPS 140-2 qualified from the National Institute of Standards and Technology (NIST).<br>29. The storage solution must support network multi-tenancy so that physical system can be configured into multiple Virtual tenants and each tenant shall have separate management protocol access.<br>30. The system must provide built-in file system analytics that gives the administrator real-time information on capacity usage, performance, data characteristics, and historical trends without the need for third-party tools or file system scans.<br>31. The system must have cross protocol permissions that manage SMB and NFS clients accessing the same files at the same time.<br>32. The system must support Container Storage Interface (CSI) for integrating the container application running on Kubernetes clusters.<br>33. The system must efficiently handle small and large files. Small files (<128K) must not require more than 50% protection overhead, and drive rebuild times must not materially increase as average file sizes decrease.<br>34. The system must include a fully programmable REST API that allows for manipulation of data, retrieval of | |

| | | |
|---|---|---|
| | usage and performance data, as well as programmability of the entire storage environment.<br>35. Quotas must be able to be applied to pre-existing directories instantaneously without running a file scan.<br>36. All existing and future features must be included over the term of the software subscription.<br>37. The storage solution must be deployable in the public cloud and on premises.<br>38. The brand being offered must be included in five eyes alliance<br>39. Three (3) years warranty on parts and services<br>40. Three (3) years subscriptions for storage solution software | |
| 8 | **Warranties of the Bidder**<br>For the procurement of the project, the warranties shall include the following:<br>1. The bidder warrants that it shall strictly conform to the terms and conditions of this Detailed Technical Specifications.<br>2. The bidder warrants that the technical staff assigned are qualified to provide the deliverables required to the satisfaction of the LRA.<br>3. The bidder shall secure and maintain, at its own expense, all registrations, licenses, or permits required by national or local laws. The contractor shall also comply with the rules, regulations, and directives of regulatory authorities and Commissions. It shall undertake to pay all fees or charges payable to any government instrumentality or any other duly constituted authorities related to the use or operation of the installation.<br>4. The bidder's technical staff assigned to support the LRA shall take all necessary precautions to ensure the safety of all persons and properties at or near their area of work and shall comply with all standard and established safety regulations, rules, and practices.<br>5. The bidder's technical staff assigned to support the LRA shall coordinate with the relevant LRA departments in the implementation of this project.<br>6. The bidder shall be liable for any loss, damage, or injury caused directly or indirectly due to the fault or negligence of its technical staff. It shall assume full responsibility, thereby fully releasing the LRA from any liability arising therefrom.<br>7. The bidder shall neither assign, transfer, pledge, nor subcontract any part of or interest in the contract being bid out.<br>8. The bidder shall identify certified technical staff who will be authorized to access and operate the Data Center and its components. The LRA shall be informed, through a | |

| | | |
|---|---|---|
| | formal notice within five (5) calendar days of any change or replacement of technical staff assigned.<br><br>**Warranty and Software Subscription Requirements**<br><br>1. The winning bidder warrants that all deliverables will fully comply with the terms and conditions outlined in this Terms of Reference.<br>2. The winning bidder shall provide a comprehensive three (3) year warranty on all hardware, unless otherwise specified in the Terms of Reference. This warranty shall cover both parts and labor, as well as maintenance and support services throughout the warranty period. For each product/item, the winning bidder must submit a warranty certificate that clearly outlines the scope of coverage, warranty terms, and duration.<br>3. The winning bidder must assign a dedicated focal person for the LRA throughout the warranty and support period. This individual must be a bona fide employee of the winning bidder. The winning bidder shall submit the complete details of the focal person, including name, position, and contact information. Should there be any changes to the assigned focal person, the winning bidder shall notify the LRA in writing.<br>4. Software Subscription Requirements<br>The winning bidder shall provide a three (3) year subscription for all software included in the project deliverables except if otherwise specified in the Terms of Reference. The software subscription will be activated either upon the LRA's request or upon the formal turnover and acceptance of the project, whichever occurs first. If the software provided is open-source, the contractor must commit to supporting this software for a minimum of one (1) year, ensuring all maintenance, updates, and issue resolutions are handled within the support period. | |
| 9 | **Project Timeline**<br>This project will run for ninety (90) calendar days from the issuance of the Notice to Proceed (NTP). This project shall have six (6) implementation stages. These stages are as follows:<br><br>1. **Project Kickoff and Planning**<br>a. Activities: Initial meeting with stakeholders, defining project goals, setting timelines, and outlining roles and responsibilities.<br>2. **Equipment and Supplies Delivery**<br>a. Activities: Procurement and delivery of all necessary equipment, supplies, and materials to the project site.<br>3. **Implementation**<br>a. Includes the following key sub-phases: | |

| | | |
|---|---|---|
| | **1. Civil Works**<br>a. Activities: Site preparation, construction, and modifications to accommodate equipment installation.<br>**1. Equipment Installations**<br>a. Activities: Installation of all hardware including servers, racks, UPS, PDUs, and cooling solutions.<br>4. **Equipment Configuration**<br>a. Activities: Physical hardware setup, including network switches, power distribution, and system connections.<br>5. **Software Configuration**<br>a. Activities: Installation and configuration of necessary software, including server software, storage management, security systems, and other required applications.<br>6. **Testing**<br>a. Activities: System testing, including hardware and software functionality tests, load tests, and cybersecurity checks.<br>7. **Training and Documentation**<br>a. Activities: Conducting hands-on training sessions for LRA personnel on system operations and providing detailed documentation/manuals.<br>8. **Project Inspection and Acceptance**<br>a. Activities: Final inspection by the LRA project team, ensuring all systems and equipment are functioning as expected. Formal acceptance of the project.<br>9. **Warranty, Maintenance, and Technical Support**<br>b. Duration: Ongoing for 1-3 years<br>c. Activities: Provision of technical support, periodic maintenance and ensuring the warranties for equipment and software are upheld. | |
| 10 | **Confidentiality of Data**<br>1. All technical staff assigned by the contractor shall be required to sign a Non-Disclosure Agreement (NDA).<br>2. The LRA Data Center Project, its components, parts, and all products, product samples, specifications, data, ideas, technologies and technical/non-technical materials, all or any of which may be derived from any of the foregoing are strictly confidential.<br>3. The contractor agrees to hold all the aforementioned information in strict confidence and further agrees not to reproduce or disclose any confidential information to | |

| | | |
|---|---|---|
| | third parties without prior written approval from the LRA. | |
| 11 | **Site Preparation and Facility Development Requirements**<br><br>1. The contractor may request to set up temporary facilities within the LRA campus. The use of utilities such as water supply and electricity must be coordinated with the LRA Project Manager.<br>2. The contractor guarantees that its services, along with its personnel, are reliable, qualified, and dedicated to meeting the requirements of the LRA. All employees deployed for this project must be well-behaved, professional, and must wear identification badges at all times while on-site. The contractor is prohibited from employing any active LRA staff for any role under this contract.<br>3. The contractor's personnel must observe all necessary safety precautions to protect people and property in and around their work areas. They must comply with all established safety regulations, standards, and best practices. Coordination with the LRA Project Manager or authorized representative is required to ensure smooth project execution.<br>4. The contractor shall be held liable for any loss, damage, or injury caused directly by the fault or negligence of its personnel. The LRA shall be fully released from any responsibility or liability arising from such incidents.<br>5. The contractor shall provide all necessary signage, including informational and safety signages which must be displayed in all implementation areas. | |
| 12 | **Technical Support and Maintenance Requirements**<br><br>1. The contractor shall provide comprehensive technical support, either through an on-site presence or via telephone, to resolve technical and related issues. Resolution may be delivered through phone assistance, electronic support, or on-site services and must satisfy the LRA's requirements for problem resolution.<br>2. The contractor must resolve hardware or network issues within the timeframe stipulated in the Service Level Agreement (SLA) as signed and approved by the LRA Project Management Team. The response time shall start once the issue has been reported by an authorized LRA representative from the main site via fax, telephone, or email.<br>3. **Technical Support Services**<br>Technical support shall be provided as follows:<br>a. **Year 1:** The winning bidder must provide On-site support to address technical issues within one (1) hour from the report of the incident | |

| | | |
|---|---|---|
| | b. **Years 2 and 3:** The winning bidder must provide remote support through telephone and email. Onsite support will be available upon request of LRA.<br>4. Support services must be available 24/7, ensuring round-the-clock assistance every day of the week (Monday to Sunday) to guarantee timely issue resolution.<br>5. Response Time Commitments:<br>a. **Telephone and Email Support:** Response within one (1) hour of the reported issue.<br>b. **On-Site Support (Year 1) :** Response time of less than one (1) hour from the initial report.<br>c. **On-Site Support (Year 2-3):** Response time of less than four (4) hours from the initial report. | |
| 13 | **Technical Support and Maintenance Requirements**<br>1. The contractor shall provide comprehensive technical support, either through an on-site presence or via telephone, to resolve technical and related issues. Resolution may be delivered through phone assistance, electronic support, or on-site services and must satisfy the LRA's requirements for problem resolution.<br>2. The contractor must resolve hardware or network issues within the timeframe stipulated in the Service Level Agreement (SLA) as signed and approved by the LRA Project Management Team. The response time shall start once the issue has been reported by an authorized LRA representative from the main site via fax, telephone, or email.<br>3. Technical support must be available on-site, via telephone, and through email for 8 hours per day (8:00 AM to 5:00 PM), 6 days a week (Monday to Saturday) to ensure timely problem resolution. The type of support provided will depend on the severity and priority of the issue. Response time shall be within one (1) hour for telephone and email support and less than four (4) hours for on-site support. | |
| 14 | **SYSTEM TESTING and COMMISSIONING**<br>The contractor shall perform testing and commissioning for the following components. Upon successful completion of the system testing, a comprehensive report must be submitted to the LRA:<br>1. **Infrastructure Development**<br>a. Equipment/Modular Racks<br>b. Environmental Monitoring System<br>c. Electrical Monitoring System<br>d. Door Access System | |

| | | |
|---|---|---|
| | 2. Power and Cooling Solutions<br>a. Uninterruptible Power Supply (UPS)<br>b. Power Distribution Units (PDUs)<br>c. Precision Air-Conditioning Units (PACU)<br>3. Security (Physical & Data) and Safety Systems<br>a. Fire Detection, Alarm, and Suppression System<br>b. CCTV System<br>c. Managed Cyber Security Services<br>d. Endpoint Security<br>4. IT Infrastructure and Services<br>a. Servers, Licenses, Storage, and Hyper-Converged Infrastructure (HCI) Services<br>b. Network Switches and Devices<br>c. Active Directory<br>d. Managed Kubernetes System and DBAAS System<br>e. Backup System<br>f. Data Center NAS Storage | |
| 15 | **AS-BUILT PLANS & DOCUMENTATION**<br>The contractor shall submit the following documentation upon project completion:<br>1. Engineering Plans (on standard A1 paper size)<br>2. Operation manuals and technical data sheets for all equipment and components, as applicable. | |
| 16 | **Bidder's Qualification**<br>1. The bidder must be duly established in the Philippines with at least twenty (20) years' experiences in the supply, delivery and installation of ICT equipment.<br>2. The bidder must submit five (5) list of project deployment for Structured Cabling, Network & Security and Data Center projects for both government and private companies. The bidder must attach any proof of transaction such as copy of purchase order, notice to proceed and/or contract.<br>3. For the managed SOC, the prospective bidder must submit names of at least three (3) full-time regular employees for at least two (2) years with the following SOC analyst certifications for the Managed SOC requirement:<br>a. Comptia SEC+ Certified<br>b. Comptia CYSA + Certified<br>c. ISC Certified in Cybersecurity | |

| | | |
|---|---|---|
| | d. Let's Defend Blue Team Certified<br>e. Certified Associate of the SOC Platform<br>4. The bidder must submit names of full-time regular employees for at least two (2) years with the following qualifications for the Data Center and ICT Equipment:<br>f. At least two (2) Certified Project Management Professional (PMP);<br>g. At least two (2) Certified Data Center Professionals (CDCP);<br>h. At least one (1) Certified Infrastructure/Solutions Professional of the Data Center solution;<br>i. At least two (2) Certified Architect of the Endpoint Security solution;<br>j. At least two (2) Electronics and Communications Engineer (PRC License)<br>k. At least one (1) Electrical Engineer (PRC License)<br>l. At least two (2) Certified Architect of the NGFW;<br>m. At least one (1) Certified Switching Professional of the Network solution;<br>n. At least one (1) Certified Mobility Associate of the Network solution;<br>o. At least one (1) Certified Mobility Professional of the Network solution;<br>p. At least two (2) Accredited Technical Professional for Hybrid Cloud of the Network Solution<br>q. At least one (1) Certified ITILv3 from the project management team<br>r. At least one (1) Certified ITILv3 from the implementation and support team.<br>5. The bidder should have a dedicated project management office to assure smooth implementation of the project. The Project Manager (PM) shall be appointed as the single point of contact by the bidder during the implementation of the project to oversee the project and shall be required to attend all site meetings and project meetings.<br>6. The bidder must submit a certificate of regular employment and copies of proof of employment such as but not limited to: SSS, PAG-IBIG or Income Tax Return (ITR) of the personnel.<br>7. The winning bidder must submit a detailed work plan specifying design, installation detailed activities, connectivity diagram and implementation from end-user premises up to the last mile. It must be approved by the Land Registration Authority before the commencement of the implementation. | |
| 17 | Other Documentary Submission (to be submitted during bid opening) | |

| | | |
|---|---|---|
| | 1. Manufacturer's Authorization Form (MAF) / Letter of Support from the Manufacturer for the following components:<br>a. Infrastructure Development<br>i. Equipment/Modular Racks<br>ii. Environmental Monitoring System<br>iii. Electrical Monitoring System<br>iv. Door Access System<br>b. Power and Cooling Solutions<br>i. Uninterruptible Power Supply (UPS)<br>ii. Power Distribution Units (PDUs)<br>iii. Precision Air-Conditioning Units (PACU)<br>c. Security (Physical & Data) and Safety Systems<br>i. Fire Detection, Alarm, and Suppression System<br>ii. CCTV System<br>iii. Managed Cyber Security Services<br>d. IT Infrastructure and Services<br>i. Servers, Licenses, Storage, and Hyper-Converged Infrastructure<br>ii. (HCI) Services<br>iii. Network Switches and Devices<br>iv. Active Directory<br>v. Managed Kubernetes System and DBAAS System<br>vi. Data Center Backup Solution<br>vii. Data Center NAS Storage<br>2. Project Proposal and Plan<br>The winning bidder shall submit a comprehensive Project Proposal and Plan that includes the following key elements:<br>a. **Timeline**: A detailed schedule outlining the phases of implementation, key milestones, and completion dates.<br>b. **Implementation Plan**: A step-by-step strategy for executing the project, including resource allocation, methodologies and risk management.<br>c. **Hardware**: A complete list of all hardware to be delivered, including specifications, quantities and warranties. | |

<table>
<tr><td></td><td>d. Services: A breakdown of all services to be provided such as installation, configuration, technical support and maintenance.<br>e. Software Subscription: Clear details on the software deliverables, subscription terms, and activation timelines, including provisions for open-source software support, where applicable<br>3. Manpower Requirements for the project as listed in Item 16 “Bidder’s Qualification”.</td><td></td></tr>
<tr><td>18</td><td>Payment Schedule
<table>
<tr><th>Milestone</th><th>Particulars</th><th>Payment %</th><th>Document Required for Payments</th></tr>
<tr><td>1</td><td>Mobilization/ Project Planning</td><td>15%</td><td>Submission of Project Plan</td></tr>
<tr><td>2</td><td>Civil Works</td><td>25%</td><td>Submission of As Built Plans (Civil & Electrical)</td></tr>
<tr><td>3</td><td>Equipment Delivery</td><td>35%</td><td>Delivery Receipts duly received by LRA</td></tr>
<tr><td>4</td><td>System Configuration</td><td>15%</td><td>System Testing and Commissioning report</td></tr>
<tr><td>5</td><td>Knowledge Transfer & Final Acceptance</td><td>10%</td><td>Knowledge Transfer Certificates, Warranty Certificates, Final Acceptance Report</td></tr>
</table></td><td></td></tr>
</table>

## REMINDER ON STATEMENT OF COMPLIANCE:

*[Bidders must state here either “Comply” or “Not Comply” against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. 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 Bidder's 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 applicable laws and issuances.]*

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

| _____ | _____ | _____ |
|---|---|---|
| **Name of Company/Bidder** | **Signature Over Printed Name Of Representative** | **Date** |

# *Section VIII. Checklist of Technical and Financial Documents*

## Notes on the Checklist of Technical and Financial Documents

The prescribed documents in the checklist are mandatory to be submitted in the Bid, but shall be subject to the following:

a. GPPB Resolution No. 09-2020 on the efficient procurement measures during a State of Calamity or other similar issuances that shall allow the use of alternate documents in lieu of the mandated requirements; or

b. Any subsequent GPPB issuances adjusting the documentary requirements after the effectivity of the adoption of the PBDs.

The BAC shall be checking the submitted documents of each Bidder against this checklist to ascertain if they are all present, using a non-discretionary "pass/fail" criterion pursuant to Section 30 of the 2016 revised IRR of RA No. 9184.

# Checklist of Technical and Financial Documents

## I. TECHNICAL COMPONENT ENVELOPE

***Class "A" Documents***

*Legal Documents*

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

*Technical Documents*

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

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

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

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

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

*Financial Documents*

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

***Class "B" Documents***

☐ (h) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence **or** duly notarized statements from all the

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

## II. FINANCIAL COMPONENT ENVELOPE

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

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

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

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

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

# Bid Form for the Procurement of Goods

***[shall be submitted with the Bid]***

---

## BID FORM

Date : _____
Project Identification No. : _____

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

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers *[insert numbers]*, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center** in conformity with the said PBDs for the sum of **TWO HUNDRED SEVENTY TWO MILLION PESOS ONLY (Php 272,000,000.00),** VAT inclusive. of the total calculated bid price, as evaluated and corrected for computational errors and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: *[specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties]*, which are itemized herein or in the Price Schedules,

If our Bid is accepted, we undertake:

a. to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);

b. to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;

c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

*[Insert this paragraph if Foreign-Assisted Project with the Development Partner:*
Commissions or gratuities, if any, paid or to be paid by us to agents relating to this Bid, and to contract execution if we are awarded the contract, are listed below:

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

(if none, state "None") *]*

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

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

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

The undersigned is authorized to submit the bid on behalf of *[name of the bidder]* as evidenced by the attached *[state the written authority]*.

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

Name: _____

Legal capacity: _____

Signature: _____

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

Date: _____

# BID PROPOSAL FORM

**Name of Company:** _____

**Address:** _____

| Lot No. | Description | Quantity (a) | Unit Cost (VAT Inclusive) (b) | Total Cost (VAT Inclusive) (a x b) |
|---|---|---|---|---|
| 1 | **Supply, Delivery, Installation, Configuration, Testing and Commissioning of a Data Center** | One (1) lot | | |

**Certified Correct:**

_____

**Name and Signature of Bidder/Representative**

# Bid Securing Declaration Form

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

---

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

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

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

I/We, the undersigned, declare that:

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

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

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

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

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

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

***[Jurat]***

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

# Contract Agreement Form for the Procurement of Goods (Revised)

***[Not required to be submitted with the Bid, but it shall be submitted within ten (10) days after receiving the Notice of Award]***

---

## CONTRACT AGREEMENT

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

WHEREAS, the Entity invited Bids for certain goods and ancillary services, particularly [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 in specified currency]* (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 as required by the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of this Agreement, *viz.*:

   i. Philippine Bidding Documents (PBDs);
      i. Schedule of Requirements;
      ii. Technical Specifications;
      iii. General and Special Conditions of Contract; and
      iv. Supplemental or Bid Bulletins, if any

   ii. Winning bidder's bid, including the Eligibility requirements, Technical and Financial Proposals, and all other documents or statements submitted;

   Bid form, including all the documents/statements contained in the Bidder's bidding envelopes, as annexes, and all other documents submitted (*e.g.*, Bidder's response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;

   iii. Performance Security;

   iv. Notice of Award of Contract; and the Bidder's conforme thereto; and

   v. Other contract documents that may be required by existing laws and/or the Procuring Entity concerned in the PBDs. **Winning bidder agrees that additional contract documents or information prescribed by the GPPB that are subsequently required for submission after the contract execution, such as the Notice to Proceed, Variation Orders, and Warranty Security, shall likewise form part of the Contract.**

3. In consideration for the sum of *[total contract price in words and figures]* or such other sums as may be ascertained, *[Named of the bidder]* agrees to *[state the object of the contract]* in accordance with his/her/its Bid.

4. The *[Name of the procuring entity]* agrees to pay the above-mentioned sum in accordance with the terms of the Bidding.

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.

| | |
|---|---|
| *[Insert Name and Signature]* | *[Insert Name and Signature]* |
| *[Insert Signatory's Legal Capacity]* | *[Insert Signatory's Legal Capacity]* |
| *for:* | *for:* |
| *[Insert Procuring Entity]* | *[Insert Name of Supplier]* |

**Acknowledgment**

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

# Omnibus Sworn Statement (Revised)

***[shall be submitted with the Bid]***

---

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

## AFFIDAVIT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    a. Carefully examining all of the Bidding Documents;
    b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
    c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
    d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

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

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

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

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

***[Jurat]***

# Performance Securing Declaration (Revised)

***[if used as an alternative performance security but it is not required to be submitted with the Bid, as it shall be submitted within ten (10) days after receiving the Notice of Award]***

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

**PERFORMANCE SECURING DECLARATION**

Invitation to Bid: [Insert Reference Number indicated in the Bidding Documents]
To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, to guarantee the faithful performance by the supplier/distributor/manufacturer/contractor/consultant of its obligations under the Contract, I/we shall submit a Performance Securing Declaration within a maximum period of ten (10) calendar days from the receipt of the Notice of Award prior to the signing of the Contract.

0. I/We accept that: I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of one (1) year for the first offense, or two (2) years **for the second offense**, upon receipt of your Blacklisting Order if I/We have violated my/our obligations under the Contract;

0. I/We understand that this Performance Securing Declaration shall cease to be valid upon:

    1. issuance by the Procuring Entity of the Certificate of Final Acceptance, subject to the following conditions:
        1. Procuring Entity has no claims filed against the contract awardee;
        2. It has no claims for labor and materials filed against the contractor; and
        3. Other terms of the contract; or

    b. replacement by the winning bidder of the submitted PSD with a performance security in any of the prescribed forms under Section 39.2 of the 2016 revised IRR of RA No. 9184 as required by the end-user.

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

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

***[Jurat]***

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


Republic of the Philippines
gppb
Government Procurement Policy Board