Office of the President of the Philippines
GOVERNANCE COMMISSION
FOR GOVERNMENT OWNED OR CONTROLLED CORPORATIONS
3/F, BDO Towers Paseo, 8741 Paseo De Roxas, Makati City, Philippines 1226

BAGONG PILIPINAS

PHILIPPINE BIDDING DOCUMENTS

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, COMMISSIONING, AND SUPPORT SERVICES FOR THE ESTABLISHMENT OF NETWORK INFRASTRUCTURE FOR GCG DISASTER RECOVERY SITE AND EXTENSION OFFICE - B

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 4

Section I. Invitation to Bid 7

Section II. Instructions to Bidders 10

1. Scope of Bid 11
2. Funding Information 11
3. Bidding Requirements 11
4. Corrupt, Fraudulent, Collusive, and Coercive Practices 11
5. Eligible Bidders 12
6. Origin of Goods 12
7. Subcontracts 12
8. Pre-Bid Conference 12
9. Clarification and Amendment of Bidding Documents 12
10. Documents comprising the Bid: Eligibility and Technical Components 13
11. Documents comprising the Bid: Financial Component 13
12. Bid Prices 13
13. Bid and Payment Currencies 14
14. Bid Security 14
15. Sealing and Marking of Bids 15
16. Deadline for Submission of Bids 15
17. Opening and Preliminary Examination of Bids 15
18. Domestic Preference 15
19. Detailed Evaluation and Comparison of Bids 15
20. Post-Qualification 16
21. Signing of the Contract 16

Section III. Bid Data Sheet 17

Section IV. General Conditions of Contract 19

1. Scope of Contract 20
2. Advance Payment and Terms of Payment 20
3. Performance Security 20
4. Inspection and Tests 20
5. Liability of the Supplier 21

Section V. Special Conditions of Contract 22

Section VI. Schedule of Requirements 26

Section VII. Technical Specifications 27

Section VIII. Checklist of Technical and Financial Documents 131

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.

INVITATION TO BID FOR THE ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, COMMISSIONING, AND SUPPORT SERVICES FOR THE ESTABLISHMENT OF NETWORK INFRASTRUCTURE FOR GCG DISASTER RECOVERY SITE AND EXTENSION OFFICE - B

1. The Governance Commission for GOCCs (GCG), through the General Appropriations Act of 2024 (GAA 2024) intends to apply the total sum of Nineteen Million Nine Hundred Thousand Pesos Only (₱19,900,000.00) being the ABC to payments under the contract for procurement of One (1) Lot Supply, Delivery, Installation, Configuration, Implementation, Commissioning, and Support Services for the Establishment of Network Infrastructure for GCG Disaster Recovery Site and Extension Office - B (P.R. No. 24-0054). Bids received in excess of the ABC for each lot shall be automatically rejected at bid opening.

2. The GCG now invites bids for the above Procurement Project. The delivery of goods, project implementation, documentation, and acceptance must be completed within ninety (90) calendar days from the receipt of the Notice to Proceed. The bidder must have completed a similar contract for the supply, delivery, and installation of firewall and network devices for the past three (3) years from the date of submission and receipt of bids. 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 GCG and inspect the Bidding Documents at the address given below during the hours of 8:00am to 3:00pm, Mondays to Fridays.

5. A complete set of Bidding Documents may be acquired by interested Bidders on 15 August 2024 from the given address and website(s) below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of Twenty-Five Thousand Pesos Only (₱25,000.00). The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person, by facsimile, or through electronic means provided that the presentation of the same be done before the scheduled bid opening.

6. The GCG will hold a Pre-Bid Conference on 23 August 2024 at 10:00AM at the GCG Office, 3rd Floor, BDO Towers Paseo (formerly Citibank Center), Paseo de

Roxas, Makati City and/or through video conferencing or webcasting via Microsoft Teams, which shall be open to prospective bidders. Prospective bidders that intend to participate through video conferencing may confirm their attendance by sending their email address to procurement@gcg.gov.ph to receive the meeting invitation.

7. Bids must be duly received by the BAC Secretariat through manual submission of physical documents at the office address indicated below on or 19 September 2024, 10:00AM. Bids submitted late will 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 19 September 2024, 10:00AM at the given address. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity either physically at the given address below or through video conferencing.

10. The GCG 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. In cases involving a tie among bidders, the procuring entity will bring the concerned service providers/suppliers to agree on a method to break the tie which shall be non-discretionary/non-discriminatory and is similarly based on sheer luck or chance.

12. For further information, please refer to:

    Christian Paul N. Pinote
    Chief Administrative Officer
    Procurement Management Division
    Governance Commission for GOCCs
    3/F BDO Towers Paseo (formerly Citibank Center)
    8741 Paseo de Roxas, Makati City, Philippines 1226
    cpnpinote@gcg.gov.ph / procurement@gcg.gov.ph
    Tel. No. (632) 5328-2030 / 5318-1000 loc. 432
    Fax No. (632) 5328-2030 / 5318-1000 loc. 301
    https://gcg.gov.ph

13. You may visit the GCG website at https://gcg.gov.ph for downloading of Bidding Documents.

15 August 2024

EXEC. DIR. JOHANN CARLOS S. BARCENA
BAC Chairman

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, GCG wishes to receive Bids for the procurement of One (1) Lot Supply, Delivery, Installation, Configuration, Implementation, Commissioning, and Support Services for the Establishment of Network Infrastructure for GCG Disaster Recovery Site and Extension Office - B, with identification number P.R. No. 24-0054.

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 Nineteen Million Nine Hundred Thousand Pesos Only (₱19,900,000.00).

2.2. The source of funding is FY 2024 General Appropriations Act (GAA 2024).

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 exceeding those allowed under the rules may participate pursuant to: Citizens, corporations, or associations of a country, included in the list issued by the GPPB, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines.

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: 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 23 August 2024 at 10:00 AM** and at the **GCG Office, 3rd Floor, BDO Towers Paseo (formerly Citibank Center), Paseo de Roxas, Makati City** and/or through video conferencing or webcasting via Microsoft Teams as indicated in paragraph 6 of the **IB.**

9. Clarification and Amendment of Bidding Documents

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

10. Documents comprising the Bid: Eligibility and Technical Components

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

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within three (3) 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[1] or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and bid security shall be valid until *[indicate date].* Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

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

15. Sealing and Marking of Bids

Each Bidder shall submit one (1) original and nine (9) copies 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.

16. Deadline for Submission of Bids

The Bidders shall submit on the specified date and time to the physical address as indicated in paragraph 7 of the **IB.**

17. Opening and Preliminary Examination of Bids

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

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

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

18. Domestic Preference

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. 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

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

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: a. completed a similar contract for the supply, delivery, and installation of firewall and network devices for the past three (3) years from the date of submission and receipt of bids.
7	Subcontracting is not allowed.
12	The price of the Goods shall be quoted DDP Makati City or the applicable International Commercial Terms (INCOTERMS) for this Project.
14.1	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: a. The amount of not less than ₱398,000.00 if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or b. The amount of not less than ₱995,000.00 if bid security is in Surety Bond.
14.2	The PE may request the bidders to extend the validity of their bid securities beyond one hundred twenty (120) calendar days, prior to their expiration, if the funding source for the Procurement Project has yet to be approved and made effective. A change in the form of the bid security is allowed if this is made prior to the expiration of the bid validity sought to be extended. If the bidder refuses to extend the bid validity, the PE shall reject the bid submitted by said bidder. (GPPB Circular 06-2019)
15	Each Bidder shall submit one (1) original and nine (9) copies of the first and second components of its bid.
19.4	One Project having several items that shall be awarded as one contract.

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 Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC**, **Section 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	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: For Goods supplied from abroad, the delivery terms applicable to the Contract are DDP delivered Makati City. In accordance with INCOTERMS. For Goods supplied from within the Philippines, the delivery terms applicable to this Contract are delivered to Makati City. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination. Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative at the Project Site is Director Jaypee O. Abesamis. **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: Furnishing of tools required for assembly and/or maintenance of the supplied Goods; The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. **Spare Parts –** The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier: 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 2. in the event of termination of production of the spare parts: i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and

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

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

The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods.

Spare parts or components shall be supplied as promptly as possible, but in any case, within one (1) month of placing the order.

Packaging –

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

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

A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging.

Transportation –

Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.

Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.

	Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights –** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	Payments shall be made only upon deployment completion of each item and a certification by the Chairperson or Authorized Representative of the GCG to the effect that the goods delivered is in accordance with this Terms of Reference (TOR) and have been duly accepted. Except with the prior approval of the Chairperson of the GCG, no payment shall be made for supplies and materials not yet delivered under this TOR. Provided further that payment shall be made within twenty (20) working days from the receipt of complete documents, i.e., billing statement / statement of account, and other pertinent documents from the bidder. All payments made to the bidder will be subjected to a five percent (5%) reduction, to serve as retention money. The said amounts shall only be released after the lapse of the warranty period. GCG adopts the Expanded Modified Direct Payment Scheme (ExMDPS) as mode of payment to creditors/payees as per DBM Circular No. 2013-16. In this line, GCG uses Direct Payment Scheme (DPS) via bank debit system through the issuance of a “List of Due and Demandable Accounts Payable – Authority to Debit Account (LDDAP-ADA)” in settlement of payables due to creditors/payees. Per Section 5.9.2 of the said DBM Circular, bank charges shall be borne/paid by the Supplier/Payee concerned if the account is not maintained with Land Bank of the Philippines.

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	Total	Delivered, Weeks/Months

Section VII. Technical Specifications

Notes for Preparing the Technical Specifications

A set of precise and clear specifications is a prerequisite for Bidders to respond realistically and competitively to the requirements of the Procuring Entity without qualifying their Bids. In the context of Competitive Bidding, the specifications (*e.g.* production/delivery schedule, manpower requirements, and after-sales service/parts, descriptions of the lots or items) must be prepared to permit the widest possible competition and, at the same time, present a clear statement of the required standards of workmanship, materials, and performance of the goods and services to be procured. Only if this is done will the objectives of transparency, equity, efficiency, fairness, and economy in procurement be realized, responsiveness of bids be ensured, and the subsequent task of bid evaluation and post-qualification facilitated. The specifications should require that all items, materials and accessories to be included or incorporated in the goods be new, unused, and of the most recent or current models, and that they include or incorporate all recent improvements in design and materials unless otherwise provided in the Contract.

Samples of specifications from previous similar procurements are useful in this respect. The use of metric units is encouraged. Depending on the complexity of the goods and the repetitiveness of the type of procurement, it may be advantageous to standardize the General Technical Specifications and incorporate them in a separate subsection. The General Technical Specifications should cover all classes of workmanship, materials, and equipment commonly involved in manufacturing similar goods. Deletions or addenda should then adapt the General Technical Specifications to the particular procurement.

Care must be taken in drafting specifications to ensure that they are not restrictive. In the specification of standards for equipment, materials, and workmanship, recognized Philippine and international standards should be used as much as possible. Where other particular standards are used, whether national standards or other standards, the specifications should state that equipment, materials, and workmanship that meet other authoritative standards, and which ensure at least a substantially equal quality than the standards mentioned, will also be acceptable. The following clause may be inserted in the Special Conditions of Contract or the Technical Specifications.

Sample Clause: Equivalency of Standards and Codes

Wherever reference is made in the Technical Specifications to specific standards and codes to be met by the goods and materials to be furnished or tested, the provisions of the latest edition or revision of the relevant standards and codes shall apply, unless otherwise expressly stated in the Contract. Where such standards and codes are national or relate to a particular country or region, other authoritative standards that ensure substantial equivalence to the standards and codes specified will be acceptable.

Reference to brand name and catalogue number should be avoided as far as possible; where unavoidable they should always be followed by the words "*or at least equivalent*." References to brand names cannot be used when the funding source is the GOP.

Where appropriate, drawings, including site plans as required, may be furnished by the Procuring Entity with the Bidding Documents. Similarly, the Supplier may be requested to provide drawings or samples either with its Bid or for prior review by the Procuring Entity during contract execution.

Bidders are also required, as part of the technical specifications, to complete their statement of compliance demonstrating how the items comply with the specification.

In case of Renewal of Regular and Recurring Services, the Procuring Entity must indicate here the technical requirements for the service provider, which must include the set criteria in the conduct of its performance evaluation.

TERMS OF REFERENCE

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, COMMISSIONING, AND SUPPORT SERVICES FOR THE ESTABLISHMENT OF NETWORK INFRASTRUCTURE FOR GCG DISASTER RECOVERY SITE AND EXTENSION OFFICE - B

1. GCG DISASTER RECOVERY SITE (DRS) NETWORK INFRASTRUCTURE REQUIREMENTS

1.1. EXTERNAL FIREWALL APPLIANCES

1.1.1. The bidder must provide two (2) units of Next Generation Firewall (NGFW) appliances with complete accessories and satisfy the minimum requirements and specifications below.

1.1.2. Must have at least 8.5 Gbps of firewall throughput.

1.1.3. Must have at least 4.2 Gbps of threat prevention throughput.

1.1.4. Must have at least 4.1 Gbps of Internet Protocol Security (IPsec) Virtual Private Network (VPN) throughput.

1.1.5. Must have the capability to support 945,000 maximum sessions and at least 100,000 new sessions per second.

1.1.6. Must have at least eight (8) 10/100/1000, four (4) 1G/2.5G/5G /PoE, six (6) 1G SFP, and four (4) 1G/10G SFP/SFP+ ports for network traffic.

1.1.7. Must support high-availability (HA) setup both Active/Active and Active/Passive modes.

1.1.8. Must have at least 120 GB solid-state drive (SSD) pair, system storage.

1.1.9. Must have the following management interface options:

1.1.9.1. one (1) 10/100/1000 out-of-bond management port

1.1.9.2. one (1) HSCI 10 Gigabit High Availability port

1.1.9.3. one (1) RJ45 console port

1.1.9.4. one (1) USB port

1.1.9.5. one (1) Micro USB console port

1.1.10. Must have power supply redundancy.

1.1.11. Must have three (3) years warranty, support, and subscriptions.

1.1.12. Must have a similar operating system (OS) with the existing external firewalls of GCG to enable seamless integration and single-pane management to the existing Central Management Solution of the GCG.

1.1.13. Must have the following general and functional requirements:

1.1.13.1. The proposed NGWF must have a separate and dedicated CPU, memory, and hard drive for control plane and data plane. This is to avoid service interruption on the data processing plane when the control plane has been restarted or rebooted.

1.1.13.2. The proposed NGWF must have visibility into applications regardless of ports or protocols.

1.1.13.3. The proposed NGWF must support all the following authentication services: Directory services: Microsoft Active Directory, Microsoft Exchange, openLDAP, Novell eDirectory, RADIUS, Kerberos, TACACS+, Sun ONE Directory Server.

1.1.13.4. The proposed NGWF must support the identification of the traversing applications, regardless of port or protocol, even if the traffic is tunneled in GRE, GTP and NULL-IPSec, uses evasive tactics, or is encrypted without the need of additional software / hardware.

1.1.13.5. The proposed NGWF must allow the administrator(s) to review any policy impact for new or modified application signatures included in a content release version. This Web GUI feature will enable the administrator(s) to simultaneously update the security policies and install new content and allows for a seamless shift in policy enforcement.

1.1.13.6. The proposed NGWF must be able to block source IP addresses performing DoS attacks on the hardware INGRESS level even before consuming any CPU or packet buffer resource without any user configuration.

1.1.13.7. The proposed NGWF must have a policy optimizer which is able filter rules who are used or unused in specific time frames such as 30 days, 90 days, etc., with an external management device.

1.1.13.8. The proposed NGWF must be able to decrypt, inspect and control both inbound and outbound SSL and SSH connections to prevent unwanted activities or malicious content on the same proposed hardware, also serve as the decryption broker to other security devices.

1.1.13.9. The proposed NGWF must have the capability to define a Threshold to indicate the minimum number of hours after an update becomes available before the firewall will download it regardless of the schedule.

1.1.13.10. The proposed NGWF must include individual user activity report showing applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period without additional software and hardware modules.

1.1.14. Must have the following threat protection capabilities:

1.1.14.1. The proposed NGWF must have protection against the most recent and relevant malware with payload signatures, not hash, to block known and future variants of malware, and receive the latest security updates.

1.1.14.2. The proposed NGWF must support a protocol decoder-based analysis that stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits.

1.1.14.3. The proposed NGWF must have integrated IPS, anti-spyware, anti-malware, and Command-and-Control (C2) prevention capabilities.

1.1.14.4. The proposed NGWF must deliver inline machine learning (ML) at the network level and should block unknown threats in real time instead of waiting for a sandbox- integrated directly on the NGFW.

1.1.14.5. The proposed NGWF must support inline cloud analysis that detects command and SQL injection vulnerabilities in real time to protect users against zero-day threats.

1.1.14.6. The proposed NGWF must support local deep learning which complements cloud-based inline cloud analysis component of the solution.

1.1.15. Must have the following sandboxing capabilities:

1.1.15.1. The proposed NGWF must completely eliminate the need for standalone IPS or IDS solutions.

1.1.15.2. The proposed NGWF must prevent highly evasive malware via stealthy observation to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.

1.1.15.3. The proposed NGWF must support uncovering malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis to prevent malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing.

1.1.15.4. The proposed NGWF must support an intelligent runtime memory analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed.

1.1.15.5. The proposed NGWF must operate a series of inline cloud ML-based detection engines to analyze PE (portable executable) samples traversing through your network to detect and prevent unknown malware in real-time.

1.1.15.6. The proposed NGWF must hold files from downloading (and potentially spreading within your network) while analyzing these suspicious files for malware in the cloud, in a real-time exchange.

1.1.15.7. The proposed NGWF must operates using a lightweight forwarding mechanism on the firewall to minimize any local performance impact; and to keep up with the latest changes in the threat landscape, cloud inline ML detection models are added and updated seamlessly in the cloud, without requiring content updates or feature release support.

1.1.15.8. The proposed NGWF must support analysis of email links by extracting HTTP/HTTPS contained in SMTP and POP3 email messages.

1.1.16. Must have the following Uniform Resource Locator (URL) filtering capabilities:

1.1.16.1. The proposed NGWF must protect the GCG network and its users against malicious and evasive web-based threats—both known and unknown.

1.1.16.2. The proposed NGWF must support inline real time web threat prevention by using cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).

1.1.16.3. The proposed NGWF must support phishing image detection with ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.

1.1.16.4. The proposed NGWF must support translation site filtering that applies advanced URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.

1.1.16.5. The proposed NGWF must inspect for phishing and malicious JavaScript using local inline categorization, a firewall-based analysis solution, which can block unknown malicious web pages in real-time.

1.1.17. Must have the following Domain Name System (DNS) security capabilities:

1.1.17.1. The proposed NGFW must stop known and unknown DNS traffic with machine learning and predictive analytics.

1.1.17.2. The proposed NGFW must help identify systems that are infected/ compromised by sinkholing DNS request to a C2 server.

1.1.17.3. The proposed NGFW must protect against Domain Generation Algorithms (DGA) based attacks which generate random domains on the fly for malware to use as a way to call back to a C2 server.

1.1.17.4. The proposed NGFW must protect against DNS tunneling based attacks that utilize crafted DNS queries and response to hide malware delivery, command-and control traffic or data exfiltration/extraction.

1.1.17.5. The proposed NGFW must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.

1.1.17.6. The proposed NGFW must protect against strategically aged domains using predictive analytics. It must protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.

1.1.17.7. The proposed NGFW must prevent fast flux, technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.

1.1.17.8. The proposed NGFW must protect against domains surreptitiously added to hacked DNS zones of reputable domains.

1.1.17.9. The proposed NGFW must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.

1.1.17.10. The proposed NGFW must prevent dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.

1.1.17.11. The proposed NGFW must support the following DNS security categories: C2, Dynamic DNS (DDNS), malware, newly registered domains, phishing, grayware, parked, and proxy avoidance & anonymizers.

1.1.18. Must have the following software-defined wide area network (SDWAN) capabilities:

1.1.18.1. The proposed NGFW must be integrated into the operating system of the next generation secure-SDWAN.

1.1.18.2. The proposed NGFW must support dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss.

1.1.18.3. The proposed NGFW must support security features, such as user and application identification/control, to provide complete traffic and security control.

1.1.18.4. The proposed NGFW must support link bundling of different Internet Service Provider (ISP).

1.1.18.5. The proposed NGFW must support path quality profile for each set of business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage.

1.1.18.6. The proposed NGFW must support the following types of WAN connections that terminates as ethernet to the device's interface: ADSL/DSL, cable modem, ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, Wi-Fi, and anything that terminates as ethernet to the device's interface.

1.1.18.7. The proposed NGFW must be able to monitor business-critical Software as a Service (SaaS) application to monitor the latency, jitter, and packet loss and able to swap from available WAN links to ensure application usability.

1.1.18.8. The proposed NGFW must support forward error correction.

1.1.18.9. The proposed NGFW must support packet duplication.

1.1.18.10. The proposed NGFW must have SD-WAN traffic distribution profiles, such as: Best Available Path, Top-Down Priority, and Weighted Session Distribution.

1.1.18.11. The proposed NGFW must have direct internet access (DIA) SD-WAN.

1.1.18.12. The proposed NGFW must support Hub-and-Spoke topology.

1.1.18.13. The proposed NGFW must support Full Mesh VPN topology.

1.1.18.14. The proposed NGFW must support Full Mesh VPN Cluster with DDNS Service.

1.1.18.15. The proposed NGFW must be managed in the central management console.

1.1.18.16. The proposed NGFW must have a dashboard for visibility into your SD-WAN links and performance so that the administrator can adjust the path quality thresholds and other aspects of SD-WAN to improve its performance.

1.1.18.17. The proposed NGFW must have centralized statistics and reporting including application and link performance statistics, path health measurements and trend analysis, and focused views of application and link issues.

1.1.19. Must have the following remote client / user VPN capabilities:

1.1.19.1. The proposed NGFW must provide management functions for VPN infrastructure.

1.1.19.2. The proposed NGFW must provide security enforcement for traffic from VPN applications.

1.1.19.3. The proposed NGFW must provide application software that runs on endpoints and enables access to the GCG network resources through the VPN portals and gateways.

1.1.19.4. The proposed NGFW must perform host information profile checking to enforce security posture on endpoints.

1.1.19.5. The proposed NGFW must support identification of managed devices using the endpoint serial number on gateways.

1.1.19.6. The proposed NGFW must support mobile applications for endpoints running iOS, Android, Chrome OS, and Windows 10.

1.1.19.7. The proposed NGFW must support endpoints running Linux aside from Windows and MacOS.

1.1.19.8. The proposed NGFW must support split tunneling based on destination domain, client process, and video streaming application.

1.1.19.9. The proposed NGFW must support adding a compromised device to the quarantine list.

1.1.19.10. The proposed NGFW must provide 200 maximum Secure Sockets Layer (SSL) VPN tunnels.

1.1.19.11. The proposed NGFW must provide 1500 maximum tunnels for client VPN (SSL, IPSec, and IKE with XAUTH).

1.1.19.12. The proposed NGFW must provide secure remote access or VPN solution via single or multiple internal/external gateways.

1.1.19.13. The proposed NGFW must provide authentication via LDAP, SAML, Kerberos, RADIUS or TACACS.

1.2. WIDE AREA NETWORK (WAN) SWITCHES

1.2.1. The bidder must provide two (2) units of WAN Switch (WANS) with complete accessories and satisfy the minimum requirements and specifications below.

1.2.2. Must have enterprise-class Layer 2 connectivity with support for ACLs, robust QoS and routing.

1.2.3. Must be a 1U rack mountable switch with full density 24 x 10/100/1000Base-T ports and 4 x 1G/10G SFP ports.

1.2.4. Must have built-in high speed 1/10GbE uplinks.

1.2.5. Must be a software defined ready with REST APIs.

1.2.6. Must have simple deployment with zero touch provisioning.

1.2.7. Must simplify add, move, and change with colorless ports.

1.2.8. Must have three (3) years warranty, support, and subscriptions.

1.2.9. Must have intelligent monitoring, visibility, and remediation with analytics engine.

1.2.10. Must be manageable via single pane of glass across wired, wireless, and WAN.

1.2.11. Must support automated configuration and verification.

1.2.12. Must enable secure and simple access for users and Internet of Things (IoT).

1.2.13. Must have the following QoS requirements:

1.2.13.1. The proposed WANS must support SP queuing.

1.2.13.2. The proposed WANS must have traffic prioritization (IEEE 802.1p) for real-time classification.

1.2.13.3. The proposed WANS have Class of Service (CoS) that sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and differentiated service.

1.2.13.4. The proposed WANS must have rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.

1.2.13.5. The proposed WANS must have large buffers for graceful congestion management.

1.2.14. Must have the following Resiliency and High Availability requirements:

1.2.14.1. The proposed WANS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.

1.2.14.2. The proposed WANS must support IEEE 802.3ad LACP that supports up to 8 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm.

1.2.14.3. The proposed WANS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.

1.2.14.4. The proposed WANS must have smart link that provides easy-to-configure link redundancy of active and standby links.

1.2.15. Must have the following Performance and Connectivity requirements:

1.2.15.1. The proposed WANS must have up to 128 Gbps in non-blocking bandwidth and up to 95.2 Mpps for forwarding.

1.2.15.2. The proposed WANS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.

1.2.15.3. The proposed WANS must have 24x ports 10/100/1000Base-T ports and 4x 1G/10G SFP ports.

1.2.15.4. The proposed WANS must have the following management interface options:

1.2.15.4.1. one (1) x USB-C console port.

1.2.15.4.2. one (1) x USB Type A host port.

1.2.15.5. The proposed WANS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.

1.2.15.6. The proposed WANS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.

1.2.16. Must have the following Management requirements:

1.2.16.1. The proposed WANS must have a built-in programmable and easy-to-use REST API interface.

1.2.16.2. The proposed WANS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.

1.2.16.3. The proposed WANS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.

1.2.16.4. The proposed WANS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.

1.2.16.5. The proposed WANS must support SNMP v2c/v3 that provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.

1.2.16.6. The proposed WANS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group.

1.2.16.7. The proposed WANS must support TFTP and SFTP that offer different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.

1.2.16.8. The proposed WANS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.

1.2.16.9. The proposed WANS must support IEEE 802.1AB LLDP that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

1.2.16.10. The proposed WANS must support dual flash images that provide independent primary and secondary operating system files for backup while upgrading.

1.2.16.11. The proposed WANS must assign descriptive names to ports for easy identification.

1.2.16.12. The proposed WANS multiple configuration files can be stored to a flash image.

1.2.16.13. The proposed WANS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.

1.2.17. Must have the following Layer 2 Switching requirements:

1.2.17.1. The proposed WANS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously.

1.2.17.2. The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,220 bytes.

1.2.17.3. The proposed WANS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.

1.2.17.4. The proposed WANS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.

1.2.17.5. The proposed WANS must support MVRP that allows automatic learning and dynamic assignment of VLANs.

1.2.17.6. The proposed WANS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.

1.2.17.7. The proposed WANS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.

1.2.17.8. The proposed WANS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.

1.2.18. Must have the following Layer 3 Services and Routing requirements:

1.2.18.1. The proposed WANS must support ARP determines the MAC address of another IP host in the same subnet; supports static ARPs.

1.2.18.2. The proposed WANS must support DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

1.2.18.3. The proposed WANS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.

1.2.18.4. The proposed WANS must support Dynamic Host Configuration Protocol (DHCP) that simplifies the management of large IP networks and supports client; DHCPv4 Relay support enables DHCP operation across subnets.

1.2.18.5. The proposed WANS must have static IP routing that provides manually configured routing.

1.2.18.6. The proposed WANS must have dual stack static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routing. Dual IP stack

that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

1.2.19. Must have the following Security requirements:

1.2.19.1. The proposed WANS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.

1.2.19.2. The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.

1.2.19.3. The proposed WANS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.

1.2.19.4. The proposed WANS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.

1.2.19.5. The proposed WANS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.

1.2.19.6. The proposed WANS must support MAC-based client authentication.

1.2.19.7. The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.

1.2.19.8. The proposed WANS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.

1.2.19.9. The proposed WANS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.

1.2.19.10. The proposed WANS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.

1.2.19.11. The proposed WANS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.

1.2.19.12. The proposed WANS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.

1.2.19.13. The proposed WANS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.

1.2.20. Must have the following Multicast requirements:

1.2.20.1. The proposed WANS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.

1.2.20.2. The proposed WANS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.

1.2.20.3. The proposed WANS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.

1.3. CORE SWITCHES

1.3.1. The bidder must provide two (2) units of Core Switch (CS) with complete accessories and satisfy the minimum requirements and specifications below.

1.3.2. Must be a stackable Layer 3 switch with Border Gateway Protocol (BGP), Ethernet VPN (EVPN), Virtual eXtensible Local-Area Network (VXLAN), Virtual Routing and

Forwarding (VRF), and Open Shortest Path First (OSPF) with robust security and Quality of service (QoS).

1.3.3. Must have at least 780 Gbps system switching capacity, 580 Mega Packet Per Second (Mpps) system throughput, and up to 200 Gbps stacking bandwidth.

1.3.4. Must be a 1U rack mountable switch with full density 24 x 1G/10G SFP+ ports (LRM + MACsec), 2 x 10G/25G/50G SFP ports, and 2 x 10G/25G SFP ports (MACsec).

1.3.5. Must have built-in high speed 10GbE/25GbE/50GbE uplinks.

1.3.6. Must have three (3) years warranty, support, and subscriptions.

1.3.7. Must have intelligent monitoring, visibility, and remediation with analytics engine.

1.3.8. Must be manageable via single pane of glass across wired, wireless, and WAN.

1.3.9. Must support automated configuration and verification.

1.3.10. Must enable secure and simple access for users and Internet of Things (IoT).

1.3.11. Must have the following QoS requirements:

1.3.11.1. The proposed CS must support Strict Priority (SP) queuing and Deficit Weighted Round Robin (DWRR).

1.3.11.2. The proposed CS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.

1.3.11.3. The proposed CS transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS).

1.3.12. Must have the following Resiliency and High Availability requirements:

1.3.12.1. The proposed CS must have high performance front plane stacking for up to 10 switches.

1.3.12.2. The proposed CS must have the flexibility to mix both modular and fixed models within a single stack.

1.3.12.3. The proposed CS must have hot swappable power supplies.

1.3.12.4. The proposed CS must provide N+1 and N+N redundancy for high reliability in the event of power line or supply failures.

1.3.12.5. The proposed CS must support Virtual Router Redundancy Protocol (VRRP) that allows groups of two routers to dynamically back each other up to create highly available routed environments.

1.3.12.6. The proposed CS must support Unidirectional Link Detection (UDLD) that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.

1.3.12.7. The proposed CS must support IEEE 802.3ad Link Aggregation Control Protocol (LACP) that supports up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm.

1.3.12.8. The proposed CS must support Microsoft Network Load Balancer (NLB) for server applications.

1.3.12.9. The proposed CS must support Ethernet Ring Protection Switching (ERPS) that provides rapid protection and recovery in a ring topology.

1.3.12.10. The proposed CS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.

1.3.13. Must have the following Performance and Connectivity requirements:

1.3.13.1. The proposed CS must have up to 780 Gbps in non-blocking bandwidth and up to 580 Mpps for forwarding.

1.3.13.2. The proposed CS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.

1.3.13.3. The proposed CS must have 24x 1G/10G SFP+ ports (LRM + MACsec), 2x 10G/25G/50G SFP ports, and 2x 10G/25G SFP ports (MACsec).

1.3.13.4. The proposed CS must have the following management interface options:

1.3.13.4.1. one (1) x USB-C console port.

1.3.13.4.2. one (1) x RJ Console Port

1.3.13.4.3. one (1) x OOBM port.

1.3.13.4.4. one (1) x USB Type A host port.

1.3.13.5. The proposed CS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.

1.3.13.6. The proposed CS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.

1.3.13.7. The proposed CS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.

1.3.14. Must have the following Management requirements:

1.3.14.1. The proposed CS must have scalable application specific integrated circuit (ASIC)-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.

1.3.14.2. The proposed CS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.

1.3.14.3. The proposed CS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.

1.3.14.4. The proposed CS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.

1.3.14.5. The proposed CS must support Simple Network Management Protocol (SNMP) v2c/v3 which provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.

1.3.14.6. The proposed CS must support remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.

1.3.14.7. The proposed CS must support Trivial File Transfer Protocol (TFTP) and Secure File Transfer Protocol (SFTP) that offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over a Secure Shell (SSH) tunnel to provide additional security.

1.3.14.8. The proposed CS must support Network Time Protocol (NTP) that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.

1.3.14.9. The proposed CS must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

1.3.14.10. The proposed CS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.

1.3.14.11. The proposed CS must be able to assign descriptive names to ports for easy identification.

1.3.14.12. The proposed CS multiple configuration files can be stored to a flash image.

1.3.14.13. The proposed CS ingress and egress port monitoring must enable more efficient network problem solving.

1.3.14.14. The proposed CS must support unidirectional link detection (UDLD) that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.

1.3.14.15. The proposed CS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for Voice over Internet Protocol (VoIP) tests.

1.3.14.16. The proposed CS must support precision time protocol that allows precise clock synchronization across distributed network switches as defined in IEEE 1588.

1.3.15. Must have the following Layer 2 Switching requirements:

1.3.15.1. The proposed CS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).

1.3.15.2. The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.

1.3.15.3. The proposed CS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.

1.3.15.4. The proposed CS must support Rapid Per-VLAN Spanning Tree (RPVST+) that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.

1.3.15.5. The proposed CS must support Multiple VLAN Registration Protocol (MVRP) that allows automatic learning and dynamic assignment of VLANs.

1.3.15.6. The proposed CS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.

1.3.15.7. The proposed CS must support Bridge Protocol Data Unit (BPDU) tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.

1.3.15.8. The proposed CS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.

1.3.15.9. The proposed CS must have Spanning Tree Protocol (STP) supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

1.3.15.10. The proposed CS must support Internet Group Management Protocol (IGMP) that controls and manages the flooding of multicast packets in a Layer 2 network.

1.3.15.11. The proposed CS must have IPv4 Multicast in VXLAN/EVPN overlay support which allows Protocol-Independent Multicast Sparse Mode (PIMSM)/IGMP snooping in the VXLAN overlay.

1.3.15.12. The proposed CS must have IPv6 VXLAN/EVPN overlay support which allows IPv6 traffic over the VXLAN overlay.

1.3.15.13. The proposed CS must have VXLAN Address Resolution Protocol (ARP)/ Neighbor Discovery (ND) suppression which allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network.

1.3.16. Must have the following Layer 3 Services and Routing requirements:

1.3.16.1. The proposed CS must have ARP that determines the MAC address of another IP host in the same subnet; supports static ARPs.

1.3.16.2. The proposed CS must have a DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

1.3.16.3. The proposed CS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility.

1.3.16.4. The proposed CS must have route maps that provide more control during route redistribution; allow filtering and altering of route metrics.

1.3.16.5. The proposed CS must have Border Gateway Protocol 4 (BGP-4) that delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks with graceful restart capability.

1.3.16.6. The proposed CS must have Multi-protocol BGP (MP-BGP) that enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6.

1.3.16.7. The proposed CS must have open shortest path first (OSPF) that delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery.

1.3.16.8. The proposed CS must have Equal-Cost Multipath (ECMP) that enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.

1.3.16.9. The proposed CS must have static IP routing that provides manually configured routing; includes ECMP capability.

1.3.16.10. The proposed CS must have policy-based routing that uses a classifier to select traffic that can be forwarded based on policy set by the network administrator.

1.3.16.11. The proposed CS must have IP performance optimization that provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.

1.3.16.12. The proposed CS must have dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

1.3.17. Must have the following Security requirements:

1.3.17.1. The proposed CS must have Access Control List (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.

1.3.17.2. The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.

1.3.17.3. The proposed CS must have management access security for both on- and off-box authentication for administrative access. RADIUS or Terminal Access Controller Access Control System (TACACS)+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.

1.3.17.4. The proposed CS must support Control Plane Policing (CoPP) which sets rate limit on control protocols to protect CPU overload from Denial-of-Service (DOS) attacks.

1.3.17.5. The proposed CS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.

1.3.17.6. The proposed CS must support MAC-based client authentication.

1.3.17.7. The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.

1.3.17.8. The proposed CS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.

1.3.17.9. The proposed CS must have Internet Control Message Protocol (ICMP) throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.

1.3.17.10. The proposed CS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.

1.3.17.11. The proposed CS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.

1.3.17.12. The proposed CS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.

1.3.17.13. The proposed CS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.

1.3.18. Must have the following Multicast requirements:

1.3.18.1. The proposed CS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.

1.3.18.2. The proposed CS must support Multicast Listener Discovery (MLD) that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.

1.3.18.3. The proposed CS must support Protocol Independent Multicast (PIM) that defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM Sparse Mode (SM) and Dense Mode (DM) for both IPv4 and IPv6.

1.3.18.4. The proposed CS must support IGMP that utilizes Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.

1.4. CENTRAL MANAGEMENT SOLUTION FOR NETWORK EQUIPMENT

1.4.1. The bidder must provide one (1) lot cloud-based Central Management Solution for the proposed two (2) units of WAN Switch and two (2) units of Core Switch (CS) with minimum requirements and specifications below.

1.4.2. Must be a similar platform with the existing Central Management Solution for the existing network devices of the GCG to ensure seamless integration and single-pane management of the new and existing equipment.

1.4.3. Must have three (3) years warranty, support, and subscriptions.

1.4.4. Must have unified management of wireless, wired, VPN, and SD-WAN for simplified operations.

1.4.5. Must have network fabric orchestration, intent-based policy engine, and access controls for unified policy management, automated network provisioning, and zero-trust security.

1.4.6. Must have Artificial Intelligence (AI)-based network insights for faster troubleshooting and continuous network optimization.

1.4.7. Must have client insights for inline client profiling and telemetry to close visibility gaps.

1.4.8. Must have live chat and an AI-based search engine for an enhanced support experience.

1.4.9. Must have APIs and webhooks to augment the value of other leading IT platforms in your environment.

1.4.10. Must have powerful monitoring and troubleshooting for remote or home office networks.

1.4.11. Must have integration with user experience insight to proactively monitor and improve the end-user experience.

1.4.12. Must have SaaS, on-premises, and Virtual Private Cloud managed service options for flexible consumption and financing.

1.4.13. Must have the following streamlined network operation requirements:

1.4.13.1. Provides a comprehensive single pane of glass dashboard for analyzing and improving wired and wireless LAN, and WAN performance at a global or site-level, eliminating the inefficiencies of using disjointed, domain-specific network management tools.

1.4.13.2. Provides a consistent operating model and a unified platform for efficient management of compute, storage, and networking infrastructure, while enhancing cost controls. Users can log in using Single Sign-On (SSO) and are granted role-based access (RBAC) based on permissions. An additional layer of security can also be enabled with Multi-Factor Authentication (MFA).

1.4.13.3. Supports setup wizard automatically adds account subscriptions, matches device inventory from orders, and assigns purchased licenses, improving accuracy, and saving time.

1.4.13.4. Additional visibility into key values of individual and stacked switches is provided. This includes port status, PoE consumption, VLAN assignment, device and neighbor connections, power status and trends, alerts and events and which troubleshooting actions can be performed.

1.4.13.5. Geographic availability, scalability, and resiliency as this platform is hosted across regions in multiple public clusters of AWS, Azure, and GCP, maintaining points of presence worldwide, and enabling GDPR compliance.

1.4.13.6. Supports accelerated device onboarding, configuration, and provisioning with flexible options of templates and UI groups for all supported network devices at the device, group and MSP levels.

1.4.13.7. Zero Touch Provisioning (ZTP) supports simple, intuitive workflow for setting up devices with no onsite IT involvement. Configuration parameters at a network or site-level can be defined.

1.4.13.8. Supports IP-based IoT devices that can be securely onboarded with Device Provisioning Protocol (DPP) via QR code, certified by Wi-Fi Alliance as "Easy Connect," enabling quick, compliant installations with built-in device validation.

1.4.14. Must have the following AI and advanced analytic requirements:

1.4.14.1. Supports Network Insights to automatically detect and diagnose network issues using dynamic baselines, with built-in anomaly detection for precise problem identification, root cause, and remediation with close to 95% accuracy.

1.4.14.2. Supports AI Search, a GenAI-powered, natural language search engine that provides quick and precise answers, configuration tips, troubleshooting advice and more.

1.4.14.3. Supports AI Assist that uses event-driven automation to collect diagnostics for critical failure signatures, for proactive customer support and replacement workflows.

1.4.14.4. Supports self-healing workflows can be enabled to automatically update configurations as needed, helping IT fix issues without manual intervention.

1.4.14.5. Supports Dynamic power save mode in which APs switch into a dynamic power save mode and automatically wake up at a schedule when connectivity demand arises, reducing power demands and saving money in alignment with the organization’s sustainability initiatives.

1.4.14.6. Enhance wireless coverage and capacity using air match, built in AI/ML analyzes periodic RF data across the network to adjust AP settings dynamically based on changing conditions.

1.4.14.7. Enhance traditional radio and roaming techniques with client match, a patented RF optimization technology that continually enhances client connectivity and eliminates sticky clients.

1.4.15. Must have the following monitoring, reporting and troubleshooting capabilities:

1.4.15.1. Network and client health and assurance.

1.4.15.2. Application Health – Monitor app health, prioritize critical services by enforcing acceptable usage by site, device, or location. UCC analytics provides a unified view of VoIP app performance like Zoom, Slack, and Teams, including MOS scores and insights on RF performance and capacity concerns. Additionally, by using SaaS express the branch gateways dynamically identify the optimal path to reach high-priority SaaS applications.

1.4.15.3. AI-based Connectivity Insights – Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more. For wired networks, IT administrators gain visibility on port status, PoE consumption, VLAN assignments, device and neighbor connections, power status, etc.

1.4.15.4. Wi-Fi Planning and Monitoring – Enhance Wi-Fi design, implementation, and monitoring with easy-to-use floorplans that depict accurate coverage patterns without employing extra sensors.

1.4.15.5. Extend Operations to IoT – Unifies visibility of IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices in the physical environment along with IP based IoT devices.

1.4.15.6. Live Events – Issue occurrence time, device name, type, category, description, packet logs, rich command line tools are captured and diagnostic checks such as ping tests, traceroutes and device-level performance tests are performed to troubleshoot issues.

1.4.15.7. Comprehensive Reports – Offers an extensive set of reporting capabilities on device connectivity, network and application health, throughput, usage data, device inventory, activity auditing, capacity planning, including the ability to baseline and compare user experience across various sites in the network.

1.4.15.8. Live upgrades – Simple GUI-based workflows and rules governing firmware upgrades on deployed network devices are available. These upgrades are scheduled at a site level during non-peak hours, ensuring continuous operations and reduced maintenance windows.

1.4.15.9. Extensibility through APIs and Webhooks – Customers developing network automation frameworks can automatically pull data from this solution into third-party solutions enabling IT operators to programmatically trigger actions based on certain events or conditions.

1.4.16. Must have the following Automate Security at Scale requirements:

1.4.16.1. Network wizard that simplifies the creation of underlays for campus and data-center environments. Manual errors are eliminated as network topology is automatically identified and configured with minimal user inputs.

1.4.16.2. Fabric wizard that enables IT administrators to automatically generate logical overlays without complex CLI programming, pushing inherent policies universally across wired, wireless, and WAN infrastructure for campus and data center environments.

1.4.16.3. Policy manager that empowers IT to define and maintain global policies at scale with ease, using UI-driven, intuitive workflows that automatically translate security intent into policy design and map user roles for employees, contractors, guests, and devices to their proper access privileges.

1.4.16.4. Client insights that dynamically compares devices against crowdsourced fingerprints of known clients and applies MAC range classification for unknown devices. Through deep packet inspection, network devices are automatically categorized, accurate policies are enforced based on context and behavioral information.

1.4.16.5. Cloud Auth and cloud-native NAC that streamlines end-user authentication for wired and wireless networks. IT admins have the flexibility to select from various authentication methods such as – uploading approved client MAC addresses or authenticating users through integrations with popular cloud identity stores such as Google Workspace or Azure Active Directory and assigning the appropriate level of network access based on network profile.

1.4.16.6. Unique pre-shared passwords or passphrases that can be used to onboard user devices and non-user specific devices such as IP phones, cameras, thermostats etc., without prior device registration with Multi Pre-Shared Key (MPSK).

1.4.16.7. Users can leverage captive portal authorization methods for effortless network access.

1.4.16.8. Secure wireless segmentation – Multizone provides data separation for multi-tenancy, guest/visitor access, IoT devices, and other use cases. A single AP can connect to multiple gateways and tunnel traffic for isolation without requiring extra access points or managing another wireless network.

1.4.16.9. Intrusion detection – Rogue AP Intrusion Detection Service (RAPIDS) detects and resolves rogue AP issues, correlating wired and wireless data to enhance security and incident response, with optional Risk Oriented Traffic Inspection.

1.4.16.10. Web content filtering – Rates websites by reputation and risk, empowering IT to block malicious sites, preventing phishing, DDoS, and other attacks.

1.4.16.11. The Bill of Materials (BOM) must include 3-year Foundational subscriptions on all proposed devices to enable all primary enterprise features such as monitoring, reporting, and troubleshooting, onboarding, provisioning, orchestration, AI and analytics, content filtering, guest access, UXI integration, and 24x7 TAC software support.

2. GCG EXTENSION OFFICE - B NETWORK INFRASTRUCTURE REQUIREMENTS

2.1. EXTERNAL FIREWALL APPLIANCES

2.1.1. The bidder must provide two (2) units of Next Generation Firewall (NGFW) appliances with complete accessories and satisfy the minimum requirements and specifications below.

2.1.2. Must have at least 3.3 Gbps of firewall throughput.

2.1.3. Must have at least 2.1 Gbps of threat prevention throughput.

2.1.4. Must have at least 1.7 Gbps of VPN throughput.

2.1.5. Must have the capability to support 300,000 maximum sessions and at least 48,000 new sessions per second.

2.1.6. Must have at least eight (8) 1G RJ45 ports for network traffic.

2.1.7. Must support high-availability (HA) setup both Active/Active and Active/Passive modes.

2.1.8. Must have at least 128 GB embedded multi-media card (eMMC) storage.

2.1.9. Must have the following management interface options:

2.1.9.1. one (1) 10/100/1000 out-of-bond management port

2.1.9.2. one (1) RJ45 console port

2.1.9.3. one (1) USB port

2.1.9.4. one (1) Micro USB console port

2.1.10. Must have power supply redundancy.

2.1.11. Must have three (3) years warranty, support, and subscriptions.

2.1.12. Must have a similar operating system (OS) with the existing external firewalls of GCG to enable seamless integration and single-pane management to the existing Central Management Solution of the GCG.

2.1.13. Must have the following general and functional requirements:

2.1.13.1. The proposed NGWF must have a separate and dedicated CPU, memory, and hard drive for control plane and data plane. This is to avoid service interruption on the data processing plane when the control plane has been restarted or rebooted.

2.1.13.2. The proposed NGWF must have visibility into applications regardless of ports or protocols.

2.1.13.3. The proposed NGWF must support all the following authentication services: Directory services: Microsoft Active Directory, Microsoft Exchange, openLDAP, Novell eDirectory, RADIUS, Kerberos, TACACS+, Sun ONE Directory Server.

2.1.13.4. The proposed NGWF must support the identification of the traversing applications, regardless of port or protocol, even if the traffic is tunneled in GRE, GTP and NULL-IPSec, uses evasive tactics, or is encrypted without the need of additional software / hardware.

2.1.13.5. The proposed NGWF must allow the administrator(s) to review any policy impact for new or modified application signatures included in a content release version. This Web GUI feature will enable the administrator(s) to simultaneously update the security policies and install new content and allows for a seamless shift in policy enforcement.

2.1.13.6. The proposed NGWF must be able to block source IP addresses performing DoS attacks on the hardware INGRESS level even before consuming any CPU or packet buffer resource without any user configuration.

2.1.13.7. The proposed NGWF must have a policy optimizer which is able filter rules who are used or unused in specific time frames such as 30 days, 90 days, etc., with an external management device.

2.1.13.8. The proposed NGWF must be able to decrypt, inspect and control both inbound and outbound SSL and SSH connections to prevent unwanted activities or malicious content on the same proposed hardware, also serve as the decryption broker to other security devices.

2.1.13.9. The proposed NGWF must have the capability to define a Threshold to indicate the minimum number of hours after an update becomes available before the firewall will download it regardless of the schedule.

2.1.13.10. The proposed NGWF must include individual user activity report showing applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period without additional software and hardware modules.

2.1.14. Must have the following threat protection capabilities:

2.1.14.1. The proposed NGWF must have protection against the most recent and relevant malware with payload signatures, not hash, to block known and future variants of malware, and receive the latest security updates.

2.1.14.2. The proposed NGWF must support a protocol decoder-based analysis that stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits.

2.1.14.3. The proposed NGWF must have integrated IPS, anti-spyware, anti-malware, and C2 prevention capabilities.

2.1.14.4. The proposed NGWF must deliver inline machine learning (ML) at the network level and should block unknown threats in real time instead of waiting for a sandbox- integrated directly on the NGFW.

2.1.14.5. The proposed NGWF must support inline cloud analysis that detects command and SQL injection vulnerabilities in real time to protect users against zero-day threats.

2.1.14.6. The proposed NGWF must support local deep learning which complements cloud-based inline cloud analysis component of the solution.

2.1.15. Must have the following sandboxing capabilities:

2.1.15.1. The proposed NGWF must completely eliminate the need for standalone IPS or IDS solutions.

2.1.15.2. The proposed NGWF must prevent highly evasive malware via stealthy observation to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.

2.1.15.3. The proposed NGWF must support uncovering malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis to prevent malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing.

2.1.15.4. The proposed NGWF must support an intelligent runtime memory analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed.

2.1.15.5. The proposed NGWF must operate a series of inline cloud ML-based detection engines to analyze PE samples traversing through your network to detect and prevent unknown malware in real-time.

2.1.15.6. The proposed NGWF must hold files from downloading (and potentially spreading within your network) while analyzing these suspicious files for malware in the cloud, in a real-time exchange.

2.1.15.7. The proposed NGWF must operates using a lightweight forwarding mechanism on the firewall to minimize any local performance impact; and to keep up with the latest changes in the threat landscape, cloud inline ML detection models are added and updated seamlessly in the cloud, without requiring content updates or feature release support.

2.1.15.8. The proposed NGWF must support analysis of email links by extracting HTTP/HTTPS contained in SMTP and POP3 email messages.

2.1.16. Must have the following URL filtering capabilities:

2.1.16.1. The proposed NGWF must protect the GCG network and its users against malicious and evasive web-based threats—both known and unknown.

2.1.16.2. The proposed NGWF must support inline real time web threat prevention by using cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).

2.1.16.3. The proposed NGWF must support phishing image detection with ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.

2.1.16.4. The proposed NGWF must support translation site filtering that applies advanced URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.

2.1.16.5. The proposed NGWF must inspect for phishing and malicious JavaScript using local inline categorization, a firewall-based analysis solution, which can block unknown malicious web pages in real-time.

2.1.17. Must have the following DNS security capabilities:

2.1.17.1. The proposed NGFW must stop known and unknown DNS traffic with machine learning and predictive analytics.

2.1.17.2. The proposed NGFW must help identify systems that are infected/ compromised by sinkholing DNS request to a C2 server.

2.1.17.3. The proposed NGFW must protect against DGA based attacks which generate random domains on the fly for malware to use as a way to call back to a C2 server.

2.1.17.4. The proposed NGFW must protect against DNS tunneling based attacks that utilize crafted DNS queries and response to hide malware delivery, command-and control traffic or data exfiltration/extraction.

2.1.17.5. The proposed NGFW must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.

2.1.17.6. The proposed NGFW must protect against strategically aged domains using predictive analytics. It must protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.

2.1.17.7. The proposed NGFW must prevent fast flux, technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.

2.1.17.8. The proposed NGFW must protect against domains surreptitiously added to hacked DNS zones of reputable domains.

2.1.17.9. The proposed NGFW must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.

2.1.17.10. The proposed NGFW must prevent dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.

2.1.17.11. The proposed NGFW must support the following DNS security categories: C2, DDNS, malware, newly registered domains, phishing, grayware, parked, and proxy avoidance & anonymizers.

2.1.18. Must have the following SDWAN capabilities:

2.1.18.1. The proposed NGFW must be integrated into the operating system of the next generation secure-SDWAN.

2.1.18.2. The proposed NGFW must support dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss.

2.1.18.3. The proposed NGFW must support security features, such as user and application identification/control, to provide complete traffic and security control.

2.1.18.4. The proposed NGFW must support link bundling of different ISP.

2.1.18.5. The proposed NGFW must support path quality profile for each set of business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage.

2.1.18.6. The proposed NGFW must support the following types of WAN connections that terminates as ethernet to the device's interface: ADSL/DSL, cable modem, ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, Wi-Fi, and anything that terminates as ethernet to the device's interface.

2.1.18.7. The proposed NGFW must be able to monitor business-critical SaaS application to monitor the latency, jitter, and packet loss and able to swap from available WAN links to ensure application usability.

2.1.18.8. The proposed NGFW must support forward error correction.

2.1.18.9. The proposed NGFW must support packet duplication.

2.1.18.10. The proposed NGFW must have SD-WAN traffic distribution profiles, such as: Best Available Path, Top-Down Priority, and Weighted Session Distribution.

2.1.18.11. The proposed NGFW must have DIA SD-WAN.

2.1.18.12. The proposed NGFW must support Hub-and-Spoke topology.

2.1.18.13. The proposed NGFW must support Full Mesh VPN topology.

2.1.18.14. The proposed NGFW must support Full Mesh VPN Cluster with DDNS Service.

2.1.18.15. The proposed NGFW must be managed in the central management console.

2.1.18.16. The proposed NGFW must have a dashboard for visibility into your SD-WAN links and performance so that the administrator can adjust the path quality thresholds and other aspects of SD-WAN to improve its performance.

2.1.18.17. The proposed NGFW must have centralized statistics and reporting including application and link performance statistics, path health measurements and trend analysis, and focused views of application and link issues.

2.1.19. Must have the following remote client / user VPN capabilities:

2.1.19.1. The proposed NGFW must provide management functions for VPN infrastructure.

2.1.19.2. The proposed NGFW must provide security enforcement for traffic from VPN applications.

2.1.19.3. The proposed NGFW must provide application software that runs on endpoints and enables access to the GCG network resources through the VPN portals and gateways.

2.1.19.4. The proposed NGFW must perform host information profile checking to enforce security posture on endpoints.

2.1.19.5. The proposed NGFW must support identification of managed devices using the endpoint serial number on gateways.

2.1.19.6. The proposed NGFW must support mobile applications for endpoints running iOS, Android, Chrome OS, and Windows 10.

2.1.19.7. The proposed NGFW must support endpoints running Linux aside from Windows and MacOS.

2.1.19.8. The proposed NGFW must support split tunneling based on destination domain, client process, and video streaming application.

2.1.19.9. The proposed NGFW must support adding a compromised device to the quarantine list.

2.1.19.10. The proposed NGFW must provide 200 maximum SSL VPN tunnels.

2.1.19.11. The proposed NGFW must provide 1500 maximum tunnels for client VPN (SSL, IPSec, and IKE with XAUTH).

2.1.19.12. The proposed NGFW must provide secure remote access or VPN solution via single or multiple internal/external gateways.

2.1.19.13. The proposed NGFW must provide authentication via LDAP, SAML, Kerberos, RADIUS or TACACS.

2.2. WIDE AREA NETWORK (WAN) SWITCH

2.2.1. The bidder must provide one (1) unit of WAN Switch (WANS) with complete accessories and satisfy the minimum requirements and specifications below.

2.2.2. Must have enterprise-class Layer 2 connectivity with support for ACLs, robust QoS and routing.

2.2.3. Must be a 1U rack mountable switch with full density 24 x 10/100/1000Base-T ports and 4 x 1G/10G SFP ports.

2.2.4. Must have built-in high speed 1/10GbE uplinks.

2.2.5. Must be a software defined ready with REST APIs.

2.2.6. Must have simple deployment with zero touch provisioning.

2.2.7. Must simplify add, move, and change with colorless ports.

2.2.8. Must have three (3) years warranty, support, and subscriptions.

2.2.9. Must have intelligent monitoring, visibility, and remediation with analytics engine.

2.2.10. Must be manageable via single pane of glass across wired, wireless, and WAN.

2.2.11. Must support automated configuration and verification.

2.2.12. Must enable secure and simple access for users and Internet of Things (IoT).

2.2.13. Must have the following QoS requirements:

2.2.13.1. The proposed WANS must support SP queuing.

2.2.13.2. The proposed WANS must have traffic prioritization (IEEE 802.1p) for real-time classification.

2.2.13.3. The proposed WANS have Class of Service (CoS) that sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and differentiated service.

2.2.13.4. The proposed WANS must have rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.

2.2.13.5. The proposed WANS must have large buffers for graceful congestion management.

2.2.14. Must have the following Resiliency and High Availability requirements:

2.2.14.1. The proposed WANS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.

2.2.14.2. The proposed WANS must support IEEE 802.3ad LACP that supports up to 8 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm.

2.2.14.3. The proposed WANS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.

2.2.14.4. The proposed WANS must have smart link that provides easy-to-configure link redundancy of active and standby links.

2.2.15. Must have the following Performance and Connectivity requirements:

2.2.15.1. The proposed WANS must have up to 128 Gbps in non-blocking bandwidth and up to 95.2 Mpps for forwarding.

2.2.15.2. The proposed WANS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.

2.2.15.3. The proposed WANS must have 24x ports 10/100/1000Base-T ports and 4x 1G/10G SFP ports.

2.2.15.4. The proposed WANS must have the following management interface options:

2.2.15.4.1. one (1) x USB-C console port.

2.2.15.4.2. one (1) x USB Type A host port.

2.2.15.5. The proposed WANS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.

2.2.15.6. The proposed WANS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.

2.2.16. Must have the following Management requirements:

2.2.16.1. The proposed WANS must have a built-in programmable and easy-to-use REST API interface.

2.2.16.2. The proposed WANS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.

2.2.16.3. The proposed WANS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.

2.2.16.4. The proposed WANS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.

2.2.16.5. The proposed WANS must support SNMP v2c/v3 that provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.

2.2.16.6. The proposed WANS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group.

2.2.16.7. The proposed WANS must support TFTP and SFTP that offer different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.

2.2.16.8. The proposed WANS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.

2.2.16.9. The proposed WANS must support IEEE 802.1AB LLDP that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

2.2.16.10. The proposed WANS must support dual flash images that provide independent primary and secondary operating system files for backup while upgrading.

2.2.16.11. The proposed WANS must assign descriptive names to ports for easy identification.

2.2.16.12. The proposed WANS multiple configuration files can be stored to a flash image.

2.2.16.13. The proposed WANS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.

2.2.17. Must have the following Layer 2 Switching requirements:

2.2.17.1. The proposed WANS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously.

2.2.17.2. The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,220 bytes.

2.2.17.3. The proposed WANS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.

2.2.17.4. The proposed WANS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.

2.2.17.5. The proposed WANS must support MVRP that allows automatic learning and dynamic assignment of VLANs.

2.2.17.6. The proposed WANS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.

2.2.17.7. The proposed WANS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.

2.2.17.8. The proposed WANS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.

2.2.18. Must have the following Layer 3 Services and Routing requirements:

2.2.18.1. The proposed WANS must support ARP determines the MAC address of another IP host in the same subnet; supports static ARPs.

2.2.18.2. The proposed WANS must support DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

2.2.18.3. The proposed WANS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.

2.2.18.4. The proposed WANS must support Dynamic Host Configuration Protocol (DHCP) that simplifies the management of large IP networks and supports client; DHCPv4 Relay support enables DHCP operation across subnets.

2.2.18.5. The proposed WANS must have static IP routing that provides manually configured routing.

2.2.18.6. The proposed WANS must have dual stack static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routing. Dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

2.2.19. Must have the following Security requirements:

2.2.19.1. The proposed WANS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.

2.2.19.2. The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.

2.2.19.3. The proposed WANS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.

2.2.19.4. The proposed WANS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.

2.2.19.5. The proposed WANS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.

2.2.19.6. The proposed WANS must support MAC-based client authentication.

2.2.19.7. The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.

2.2.19.8. The proposed WANS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.

2.2.19.9. The proposed WANS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.

2.2.19.10. The proposed WANS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.

2.2.19.11. The proposed WANS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.

2.2.19.12. The proposed WANS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.

2.2.19.13. The proposed WANS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.

2.2.20. Must have the following Multicast requirements:

2.2.20.1. The proposed WANS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.

2.2.20.2. The proposed WANS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.

2.2.20.3. The proposed WANS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.

2.3. CORE SWITCHES

2.3.1. The bidder must provide two (2) units of Core Switch (CS) with complete accessories and satisfy the minimum requirements and specifications below.

2.3.2. Must be a stackable Layer 3 switch with BGP, EVPN, VXLAN, VRF, and OSPF with robust security and QoS.

2.3.3. Must have at least 448 Gbps system switching capacity, 334 Mpps system throughput, and up to 200 Gbps stacking bandwidth.

2.3.4. Must be a 1U rack mountable switch with full density 24 x 10/100/1000Base-T ports and 4 x 1G/10G/25G/50G SFP ports.

2.3.5. Must have power-to-port switch bundle with back-to-front air flow, ideal for data center 1GbE top-of-rack (ToR) and out-of-band management (OOBM) deployments.

2.3.6. Must have built-in high speed 10GbE/25GbE/50GbE uplinks.

2.3.7. Must have three (3) years warranty, support, and subscriptions.

2.3.8. Must have intelligent monitoring, visibility, and remediation with analytics engine.

2.3.9. Must be manageable via single pane of glass across wired, wireless, and WAN.

2.3.10. Must support automated configuration and verification.

2.3.11. Must enable secure and simple access for users and Internet of Things (IoT).

2.3.12. Must have the following QoS requirements:

2.3.12.1. The proposed CS must support SP queuing and DWRR.

2.3.12.2. The proposed CS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.

2.3.12.3. The proposed CS transmission rates of egressing frames can be limited on a per-queue basis using EQS.

2.3.13. Must have the following Resiliency and High Availability requirements:

2.3.13.1. The proposed CS must have high performance front plane stacking for up to 10 switches.

2.3.13.2. The proposed CS must have the flexibility to mix both modular and fixed models within a single stack.

2.3.13.3. The proposed CS must have hot swappable power supplies.

2.3.13.4. The proposed CS must provide N+1 and N+N redundancy for high reliability in the event of power line or supply failures.

2.3.13.5. The proposed CS must support VRRP that allows groups of two routers to dynamically back each other up to create highly available routed environments.

2.3.13.6. The proposed CS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.

2.3.13.7. The proposed CS must support IEEE 802.3ad LACP that supports up to 54 LAGs, each with eight links per group with a user-selectable hashing algorithm.

2.3.13.8. The proposed CS must support Microsoft NLB for server applications.

2.3.13.9. The proposed CS must support ERPS that provides rapid protection and recovery in a ring topology.

2.3.13.10. The proposed CS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.

2.3.14. Must have the following Performance and Connectivity requirements:

2.3.14.1. The proposed CS must have up to 448 Gbps in non-blocking bandwidth and up to 334 Mpps for forwarding.

2.3.14.2. The proposed CS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.

2.3.14.3. The proposed CS must have 24x ports 10/100/1000Base-T ports and 4x 1G/10G/25G/50G SFP ports.

2.3.14.4. The proposed CS must have the following management interface options:

2.3.14.4.1. one (1) x USB-C console port.

2.3.14.4.2. one (1) x OOBM port.

2.3.14.4.3. one (1) x USB Type A host port.

2.3.14.5. The proposed CS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.

2.3.14.6. The proposed CS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.

2.3.14.7. The proposed CS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.

2.3.15. Must have the following Management requirements:

2.3.15.1. The proposed CS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.

2.3.15.2. The proposed CS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.

2.3.15.3. The proposed CS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.

2.3.15.4. The proposed CS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.

2.3.15.5. The proposed CS must support SNMP v2c/v3 which provides SNMP read and trap support of industry standard MIB, and private extensions.

2.3.15.6. The proposed CS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.

2.3.15.7. The proposed CS must support TFTP and SFTP – offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over a Secure Shell (SSH) tunnel to provide additional security.

2.3.15.8. The proposed CS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among

all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.

2.3.15.9. The proposed CS must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

2.3.15.10. The proposed CS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.

2.3.15.11. The proposed CS must be able to assign descriptive names to ports for easy identification.

2.3.15.12. The proposed CS multiple configuration files can be stored to a flash image.

2.3.15.13. The proposed CS ingress and egress port monitoring must enable more efficient network problem solving.

2.3.15.14. The proposed CS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.

2.3.15.15. The proposed CS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for VoIP tests.

2.3.15.16. The proposed CS must support precision time protocol that allows precise clock synchronization across distributed network switches as defined in IEEE 1588.

2.3.16. Must have the following Layer 2 Switching requirements:

2.3.16.1. The proposed CS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).

2.3.16.2. The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.

2.3.16.3. The proposed CS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.

2.3.16.4. The proposed CS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+

2.3.16.5. The proposed CS must support MVRP that allows automatic learning and dynamic assignment of VLANs.

2.3.16.6. The proposed CS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.

2.3.16.7. The proposed CS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.

2.3.16.8. The proposed CS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.

2.3.16.9. The proposed CS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.

2.3.16.10. The proposed CS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.

2.3.16.11. The proposed CS must have IPv4 Multicast in VXLAN/EVPN overlay support which allows PIMSM/IGMP snooping in the VXLAN overlay.

2.3.16.12. The proposed CS must have IPv6 VXLAN/EVPN overlay support which allows IPv6 traffic over the VXLAN overlay.

2.3.16.13. The proposed CS must have VXLAN ARP/ND suppression which allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network.

2.3.17. Must have the following Layer 3 Services and Routing requirements:

2.3.17.1. The proposed CS must have ARP that determines the MAC address of another IP host in the same subnet; supports static ARPs.

2.3.17.2. The proposed CS must have a DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

2.3.17.3. The proposed CS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility.

2.3.17.4. The proposed CS must have route maps that provide more control during route redistribution; allow filtering and altering of route metrics.

2.3.17.5. The proposed CS must have BGP-4 that delivers an implementation of the EGP utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks with graceful restart capability.

2.3.17.6. The proposed CS must have MP-BGP that enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6.

2.3.17.7. The proposed CS must have OSPF that delivers faster convergence; uses link-state routing IGP, which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery.

2.3.17.8. The proposed CS must have ECMP that enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.

2.3.17.9. The proposed CS must have static IP routing that provides manually configured routing; includes ECMP capability.

2.3.17.10. The proposed CS must have policy-based routing that uses a classifier to select traffic that can be forwarded based on policy set by the network administrator.

2.3.17.11. The proposed CS must have IP performance optimization that provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.

2.3.17.12. The proposed CS must have dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

2.3.18. Must have the following Security requirements:

2.3.18.1. The proposed CS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.

2.3.18.2. The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.

2.3.18.3. The proposed CS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.

2.3.18.4. The proposed CS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.

2.3.18.5. The proposed CS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.

2.3.18.6. The proposed CS must support MAC-based client authentication.

2.3.18.7. The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.

2.3.18.8. The proposed CS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.

2.3.18.9. The proposed CS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.

2.3.18.10. The proposed CS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.

2.3.18.11. The proposed CS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.

2.3.18.12. The proposed CS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.

2.3.18.13. The proposed CS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.

2.3.19. Must have the following Multicast requirements:

2.3.19.1. The proposed CS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.

2.3.19.2. The proposed CS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.

2.3.19.3. The proposed CS must support PIM that defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM SM and DM for both IPv4 and IPv6.

2.3.19.4. The proposed CS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.

2.4. LOCAL AREA NETWORK (LAN) ACCESS SWITCHES

2.4.1. The bidder must provide two (2) units of LAN Access Switch (LAS) with complete accessories and satisfy the minimum requirements and specifications below.

2.4.2. Must have enterprise-class connectivity with support for ACLs, robust QoS and common protocols such as static and Access OSPF routing.

2.4.3. Must have scalability with 8-member switch Virtual Switching Framework (VSF) stacking for up to 384 downlink ports.

2.4.4. Must have 36 x 10/100/1000Base-T Class 6 Power over Ethernet (PoE) ports, supporting up to 60W per port.

2.4.5. Must have 12 x smart rate 100M/1G/2.5G/5GBase-T Class 6 PoE ports supporting up to 60W per port.

2.4.6. Must have 4 x 100M/1G/10G SFP ports (2x LRM; 2x LRM/MACSec 256).

2.4.7. Must have supports to PoE Standards IEEE 802.3af, 802.3at, 802.3bt (up to 60W).

2.4.8. Must have three (3) years warranty, support, and subscriptions.

2.4.9. Must have intelligent monitoring, visibility, and remediation with analytics engine.

2.4.10. Must be manageable via single pane of glass across wired, wireless, and WAN.

2.4.11. Must support automated configuration and verification.

2.4.12. Must enable secure and simple access for users and Internet of Things (IoT).

2.4.13. Must have the following QoS requirements:

2.4.13.1. The proposed LANS must support SP queuing and DWRR.

2.4.13.2. The proposed LANS must have traffic prioritization (IEEE 802.1p) for real-time classification.

2.4.13.3. The proposed LANS transmission rates of egressing frames can be limited on a per-queue basis using EQS.

2.4.13.4. The proposed LANS must have rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.

2.4.14. Must have the following Resiliency and High Availability requirements:

2.4.14.1. The proposed LANS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.

2.4.14.2. The proposed LANS must support IEEE 802.3ad LACP that supports up to 32 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm.

2.4.14.3. The proposed LANS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.

2.4.14.4. The proposed LANS must IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking support static and dynamic trunks where each trunk supports up to eight links (ports) per static trunk.

2.4.14.5. The proposed LANS must support the VRRP that allows groups of two routers to dynamically back each other up to create highly available routed environments.

2.4.14.6. The proposed LANS must have hot-patching support for standalone and VSF stacked switches.

2.4.15. Must have the following Performance and Connectivity requirements:

2.4.15.1. The proposed LANS must have up to 272 Gbps in non-blocking bandwidth and up to 202 Mpps for forwarding.

2.4.15.2. The proposed LANS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.

2.4.15.3. The proposed LANS must have 36 x ports 10/100/1000Base-T Class 6 Power over Ethernet (PoE) ports, supporting up to 60W per port.

2.4.15.4. The proposed LANS must have 12 x ports smart rate 100M/1G/2.5G/5GBase-T Class 6 PoE ports supporting up to 60W per port.

2.4.15.5. The proposed LANS must have 4x 100M/1G/10G SFP ports (2x LRM; 2x LRM/MACSec 256).

2.4.15.6. The proposed LANS must have supports to PoE Standards IEEE 802.3af, 802.3at, 802.3bt (up to 60W).

2.4.15.7. The proposed LANS must have the following management interface options:

2.4.15.7.1. one (1) x RJ-45 console port.

2.4.15.7.2. one (1) x USB-C console port.

2.4.15.7.3. one (1) x OOBM port.

2.4.15.7.4. one (1) x USB Type A host port.

2.4.15.8. The proposed LANS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.

2.4.15.9. The proposed LANS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.

2.4.15.10. The proposed LANS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.

2.4.16. Must have the following Management requirements:

2.4.16.1. The proposed LANS must have built-in programmable and easy-to-use REST API interface.

2.4.16.2. The proposed LANS must have simple day zero provisioning.

2.4.16.3. The proposed LANS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.

2.4.16.4. The proposed LANS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.

2.4.16.5. The proposed LANS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.

2.4.16.6. The proposed LANS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.

2.4.16.7. The proposed LANS must support SNMP (v2c/v3) and a wide range of read, write, and trap capabilities for industry standard Management Information Base (MIB), private extensions, and common use cases, such as system, port, PoE and VLAN management.

2.4.16.8. The proposed LANS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.

2.4.16.9. The proposed LANS must support TFTP and SFTP that offer different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.

2.4.16.10. The proposed LANS must have debug and sampler utility that supports ping and traceroute for IPv4 and IPv6.

2.4.16.11. The proposed LANS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network.

2.4.16.12. The proposed LANS must support IEEE 802.1AB LLDP that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.

2.4.16.13. The proposed LANS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.

2.4.16.14. The proposed LANS ingress and egress port monitoring must enable more efficient network problem solving.

2.4.16.15. The proposed LANS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.

2.4.16.16. The proposed LANS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for VoIP tests.

2.4.17. Must have the following Layer 2 Switching requirements:

2.4.17.1. The proposed LANS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).

2.4.17.2. The proposed LANS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.

2.4.17.3. The proposed LANS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.

2.4.17.4. The proposed LANS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.

2.4.17.5. The proposed LANS must support MVRP that allows automatic learning and dynamic assignment of VLANs.

2.4.17.6. The proposed LANS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.

2.4.17.7. The proposed LANS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.

2.4.17.8. The proposed LANS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.

2.4.17.9. The proposed LANS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.

2.4.17.10. The proposed LANS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.

2.4.18. Must have the following Layer 3 Services and Routing requirements:

2.4.18.1. The proposed LANS must have a loopback interface address defines an address in OSPF, improving diagnostic capability.

2.4.18.2. The proposed LANS must support ARP determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network.

2.4.18.3. The proposed LANS must support DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.

2.4.18.4. The proposed LANS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.

2.4.18.5. The proposed LANS must support RIPv2 that provides an easy to configure routing protocol for small networks as while RIPng provides support for small IPv6 networks

2.4.18.6. The proposed LANS must support OSPF that delivers faster convergence; uses link-state routing IGP, which supports NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery.

2.4.18.7. The proposed LANS must have static IP routing that provides manually configured routing.

2.4.18.8. The proposed LANS must have IP performance optimization that provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.

2.4.18.9. The proposed LANS must have dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.

2.4.18.10. The proposed LANS must have Multicast Domain Name System Gateway that enables discovery vof mDNS groups across L3 boundaries

2.4.18.11. The proposed LANS must support Equal-Cost Multipath (ECMP) that enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.

2.4.19. Must have the following Security requirements:

2.4.19.1. The proposed LANS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or

permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.

2.4.19.2. The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.

2.4.19.3. The proposed LANS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.

2.4.19.4. The proposed LANS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.

2.4.19.5. The proposed LANS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.

2.4.19.6. The proposed LANS must support MAC-based client authentication.

2.4.19.7. The proposed LANS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.

2.4.19.8. The proposed LANS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.

2.4.19.9. The proposed LANS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.

2.4.19.10. The proposed LANS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.

2.4.19.11. The proposed LANS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.

2.4.19.12. The proposed LANS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.

2.4.19.13. The proposed LANS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.

2.4.20. Must have the following Multicast requirements:

2.4.20.1. The proposed LANS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.

2.4.20.2. The proposed LANS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.

2.4.20.3. The proposed LANS must support PIM that defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM SM and DM for both IPv4 and IPv6.

2.4.20.4. The proposed LANS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.

2.5. WIRELESS ACCESS POINTS

2.5.1. WIRELESS ACCESS POINTS FOR WORKFORCE AREA

2.5.1.1. The bidder must provide five (5) units of Wireless Access Point (AP) for the Workforce Area with complete accessories and satisfy the minimum requirements and specifications below.

2.5.1.2. Must be an indoor AP type with dual radio, 5GHz 802.11ax 4x4 Multiple Input, Multiple Output (MIMO) and 2.4GHz 802.11ax 2x2 MIMO.

2.5.1.3. For 5GHz radio:

2.5.1.3.1. Four (4) spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate to individual 4SS HE160.

2.5.1.3.2. 802.11ax client devices (max): Two (2) spatial stream Single User (SU) MIMO for up to 1.2Gbps wireless data rate to individual 2SS HE80.

2.5.1.3.3. 802.11ax client devices (typical): Four (4) spatial stream Multi User (MU) MIMO for up to 4.8Gbps wireless data rate to up to four 1SS or two 2SS HE160 802.11ax DL-MU-MIMO capable client devices simultaneously (max); Four (4) spatial stream MU MIMO for up to 2.4Gbps wireless data rate to up to four 1SS or two 2SS HE80 802.11ax DL-MU-MIMO capable client devices simultaneously (typical).

2.5.1.4. For 2.4GHz radio:

2.5.1.4.1. Two (2) spatial stream SU MIMO for up to 574Mbps wireless data rate to 2SS HE40 802.11ax client devices (max).

2.5.1.4.2. Two spatial stream Single User (SU) MIMO for up to 287Mbps wireless data rate to 2SS HE20 802.11ax client devices (typical).

2.5.1.5. Must have three (3) years warranty, support, and subscriptions.

2.5.1.6. Must support at least up to 512 associated client devices per radio, and up to 16 Basic Service Set Identifier (BSSID)s per radio.

2.5.1.7. Must support the dynamic frequency selection (DFS) which optimizes the use of available radio frequency (RF) spectrum including Zero-Wait DFS (ZWDFS) to accelerate channel change.

2.5.1.8. Must support the following radio technologies:

2.5.1.8.1. 802.11b: Direct-sequence spread-spectrum (DSSS).

2.5.1.8.2. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM).

2.5.1.8.3. 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to thirty-seven (37) resource units (for an 80MHz channel).

2.5.1.9. Must support the following modulation types:

2.5.1.9.1. 802.11b: BPSK, QPSK, CCK.

2.5.1.9.2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.

2.5.1.9.3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.

2.5.1.9.4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.

2.5.1.10. Must support 802.11n high-throughput support: HT20/40.

2.5.1.11. Must support 802.11ac very high throughput support: VHT20/40/80/160.

2.5.1.12. Must support 802.11ax high efficiency support: HE20/40/80/160.

2.5.1.13. Must support 802.11n/ac packet aggregation: A-MPDU, A-MSDU.

2.5.1.14. Must have transmit power that is configurable in increments of 0.5 dBm.

2.5.1.15. Must support the following maximum transmit power:

2.5.1.15.1. 2.4 GHz band: +24 dBm (18dBm per chain).

2.5.1.15.2. 5 GHz band: +24 dBm (18 dBm per chain).

2.5.1.16. Must have four integrated dual-band down tilt omni- directional antennas for 4x4 MIMO with peak antenna gain of 3.5dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The down tilt angle for maximum gain is roughly 30 degrees. Combining the patterns of each of the antennas of the MIMO radios, the peak

gain of the combined, average pattern is 1.9dBi in 2.4GHz and 3.5dBi in 5GHz.

2.5.1.17. Must have at least two (2) multi-gigabit ports:

2.5.1.17.1. Port 1

2.5.1.17.1.1. Must be smart rate port with maximum negotiated speed of 2.5Gbps.

2.5.1.17.1.2. Must be auto-sensing link speed (100/1000/2500/5000BASE-T) and MDI/MDX.

2.5.1.17.1.3. Must be 2.5Gbps speeds that comply with NBase-T and 802.3bz specifications.

2.5.1.17.1.4. Must be 48Vdc (nominal) 802.3at/bt POE-PD (class 3 or higher).

2.5.1.17.1.5. Must be 802.3az Energy Efficient Ethernet (EEE).

2.5.1.17.2. Port 2

2.5.1.17.2.1. Must be 10/100/1000BASE-T Ethernet network interface (RJ-45).

2.5.1.17.2.2. Must be auto-sensing link speed and MDI/MDX.

2.5.1.17.2.3. Must be 802.3az Energy Efficient Ethernet (EEE).

2.5.1.18. Must have LACP support between both network ports for redundancy and increased capacity.

2.5.1.19. Must have DC power interface: 12Vdc (nominal, +/- 5%), accepts 2.1mm/5.5mm center-positive circular plug with 9.5mm length.

2.5.1.20. Must have USB 2.0 host interface (Type A connector).

2.5.1.21. Must support Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio (2.4GHz).

2.5.1.22. Must have visual indicators (two multi-color LEDs): for System and Radio status.

2.5.1.23. Must have reset button: factory reset, LED mode control (normal/off).

2.5.1.24. Must have serial console interface (micro-B USB physical jack).

2.5.1.25. Must have Kensington security slot.

2.5.1.26. Must have maximum power consumption: DC powered: 16.0W, PoE powered (802.3af, IPM enabled): 13.5W, PoE powered (802.3at/bt): 20.8W, and all numbers above are without an external USB device connected. When sourcing the full 5W power budget to such a device, the incremental power consumption for the AP is up to 5.7W (PoE powered) or 5.5W (DC powered).

2.5.1.27. Must have maximum power consumption in idle mode: 12.6W (POE) or 9.7W (DC).

2.5.1.28. Must have maximum power consumption in deep-sleep mode: 5.9W (POE) or 1.5W (DC).

2.5.1.29. Must have Mean Time Between Failure (MTBF): 560,000hrs (64yrs) at +25C operating temperature.

2.5.1.30. Must support up to 2.69 Gbps combined peak data rate.

2.5.1.31. Must support WPA3 and Enhanced Open security.

2.5.1.32. Must have Built-in Client Match technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices.

2.5.1.33. Must be IoT-ready Bluetooth 5 and Zigbee support.

2.5.1.34. Must have embedded ranging technology for accurate indoor location measurements.

2.5.1.35. Must be designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.

2.5.1.36. Must have maximum data rates of 2.4 Gbps in the 5 GHz band and 287 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.69 Gbps).

2.5.1.37. Must support Orthogonal Frequency Division Multiple Access (OFDMA), multi-user MIMO (MU-MIMO), and cellular optimization with up to 4 spatial streams (4SS) and 160MHz channel bandwidth (VHT160).

2.5.1.38. Must support downlink MU-MIMO (5GHz radio) to maximize the use of its MIMO radio capabilities by simultaneously exchanging data with multiple single or dual stream client devices.

2.5.1.39. Must have flexibility to operate as standalone access points or with a gateway for greater scalability, security, and manageability.

2.5.1.40. Must support Air Match that allows organizations to automate network optimization using machine learning.

2.5.1.41. Must come with built-in Bluetooth Low-Energy (BLE) and Zigbee radio that enables a wide range of IOT use cases, such as asset tracking and mobile engagement.

2.5.1.42. Must provide enhanced device assurance with Trusted Platform Module (TPM) for secure credential and key storage, and secure boot.

2.5.1.43. Must support Intelligent Power Monitoring (IPM) enabling the AP to continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.

2.5.1.44. Must have Advanced Cellular Coexistence (ACC) to minimize the impact of interference from cellular networks.

2.5.1.45. Must support Maximum Ratio Combining (MRC) for improved receiver performance.

2.5.1.46. Must support Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance.

2.5.1.47. Must support Space-time block coding (STBC) for increased range and improved reception.

2.5.1.48. Must support Low-Density Parity Check (LDPC) for high-efficiency error correction and increased throughput.

2.5.1.49. Must support Transmit Beam-Forming (TxBF) for increased signal reliability and range.

2.5.1.50. Must support 802.11ax Target Wait Time (TWT) to support low-power client devices.

2.5.2. WIRELESS ACCESS POINTS FOR MEETING ROOMS

2.5.2.1. The bidder must provide two (2) units of Wireless Access Point (AP) for Meeting Rooms with complete accessories and satisfy the minimum requirements and specifications below.

2.5.2.2. Must be a mid-range dual radio Wi-Fi 6 hospitality AP with 1+2 Ethernet ports.

2.5.2.3. For 5GHz radio: two (2) SS SU-MIMO for up to 1.2Gbps wireless data rate (HE80).

2.5.2.4. For 2.4GHz radio: two (2) SS SU-MIMO for up to 287Mbps wireless data rate (HE20).

2.5.2.5. Must have three (3) years warranty, support, and subscriptions.

2.5.2.6. Must support up to 256 associated client devices per radio, and up to 16 BSSIDs per radio.

2.5.2.7. Must support the DFS which optimizes the use of available RF spectrum including Zero-Wait DFS (ZWDFS) to accelerate channel change.

2.5.2.8. Must support the following radio technologies:

2.5.2.8.1. 802.11b: DSSS.

2.5.2.8.2. 802.11a/g/n/ac: OFDM.

2.5.2.8.3. 802.11ax: OFDMA with up to eight (8) resource units.

2.5.2.9. Must support the following modulation types:

2.5.2.9.1. 802.11b: BPSK, QPSK, CCK.

2.5.2.9.2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.

2.5.2.9.3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.

2.5.2.9.4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.

2.5.2.10. Must support 802.11n high-throughput support: HT20/40.

2.5.2.11. Must support 802.11ac very high throughput support: VHT20/40/80.

2.5.2.12. Must support 802.11ax high efficiency support: HE20/40/80.

2.5.2.13. Must support 802.11n/ac packet aggregation: A-MPDU, A-MSDU.

2.5.2.14. Must have transmit power that is configurable in increments of 0.5 dBm.

2.5.2.15. Must support the following maximum transmit power:

2.5.2.15.1. 2.4 GHz band: +20 dBm (17 dBm per chain).

2.5.2.15.2. 5 GHz band: +21 dBm (18 dBm per chain).

2.5.2.16. Two integrated semi-directional antennas for 2x2 MIMO with peak single antenna gain of 5.2dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for vertical wall or desk mounted orientation of the AP. Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 3.3dBi in 2.4GHz and 2.9dBi in 5GHz.

2.5.2.17. Must have two (2) multi-gigabit ethernet wired network ports.

2.5.2.17.1. auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDX.

2.5.2.17.2. 802.3az Energy Efficient Ethernet (EEE).

2.5.2.17.3. PoE-PSE: 802.3af/at PoE output; dual 802.3af (both ports) or single 802.3at.

2.5.2.18. Must have DC power interface: 48Vdc (nominal, +/- 5%), accepts 1.35mm/3.5mm center-positive circular plug with 9.5mm length.

2.5.2.19. Must have USB 2.0 host interface (Type A connector).

2.5.2.20. Must support Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio (2.4GHz).

2.5.2.21. Must have visual indicators (two multi-color LEDs): for System and Radio status.

2.5.2.22. Must have reset button: factory reset, LED mode control (normal/off).

2.5.2.23. Must have serial console interface (micro-B USB physical jack).

2.5.2.24. Must have Kensington security slot.

2.5.2.25. Must have maximum power consumption: DC powered: 14W / 50W, PoE powered (802.3bt): 14W / 51W, PoE powered (802.3at): 14W / 25.5W, and PoE powered (802.3af): 13.5W / 13.5.

2.5.2.26. Must have maximum power consumption in idle mode (without USB or PSE): 6.2W (PoE).

2.5.2.27. Must have MTBF: 780khrs (88yrs) at +25C operating temperature.

2.5.2.28. Must have combine wireless and wired access in a single compact form factor.

2.5.2.29. Must provide high-performance connectivity for any organization experiencing growing mobile, cloud and IoT requirements with a wireless aggregate data rate of up to 1.5 Gbps and gigabit local wired ports.

2.5.2.30. Must support WPA3 and Enhanced Open security.

2.5.2.31. Must have Built-in Client Match technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices.

2.5.2.32. Must be IoT-ready Bluetooth 5 and Zigbee support.

2.5.2.33. Must be designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.

2.5.2.34. Must support OFDMA, MU-MIMO, and cellular optimization with up to 2 spatial streams (2SS) and 80MHz channel bandwidth.

2.5.2.35. Must have flexibility to operate as standalone access points or with a gateway for greater scalability, security, and manageability.

2.5.2.36. Must come with built-in BLE and Zigbee radio that enables a wide range of IOT use cases.

2.5.2.37. Must provide enhanced device assurance with TPM for secure credential and key storage, and secure boot.

2.5.2.38. Must support IPM enabling the AP to continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.

2.5.2.39. Must have ACC to minimize the impact of interference from cellular networks.

2.5.2.40. Must support MRC for improved receiver performance.

2.5.2.41. Must support CDD/CSD for improved downlink RF performance.

2.5.2.42. Must support STBC for increased range and improved reception.

2.5.2.43. Must support LDPC for high-efficiency error correction and increased throughput.

2.5.2.44. Must support TxBF for increased signal reliability and range.

2.5.2.45. Must support 802.11ax TWT to support low-power client devices.

2.6. CENTRAL MANAGEMENT SOLUTION FOR NETWORK EQUIPMENT

2.6.1. The bidder must provide one (1) lot cloud-based Central Management Solution for the proposed one (1) unit of WAN Switch (WANS), two (2) units of Core Switch (CS), two (2) units of LAN Access Switch, five (5) units of Wireless Access Point (AP) for the Workforce Area, and two (2) units of Wireless Access Point (AP) for Meeting Rooms with minimum requirements and specifications below.

2.6.2. Must be a similar platform with the existing Central Management Solution for the existing network devices of the GCG to ensure seamless integration and single-pane management of the new and existing equipment.

2.6.3. Must have three (3) years warranty, support, and subscriptions.

2.6.4. Must have unified management of wireless, wired, VPN, and SD-WAN for simplified operations.

2.6.5. Must have network fabric orchestration, intent-based policy engine, and access controls for unified policy management, automated network provisioning, and zero-trust security.

2.6.6. Must have Artificial Intelligence (AI)-based network insights for faster troubleshooting and continuous network optimization.

2.6.7. Must have client insights for inline client profiling and telemetry to close visibility gaps.

2.6.8. Must have live chat and an AI-based search engine for an enhanced support experience.

2.6.9. Must have APIs and webhooks to augment the value of other leading IT platforms in your environment.

2.6.10. Must have powerful monitoring and troubleshooting for remote or home office networks.

2.6.11. Must have integration with user experience insight to proactively monitor and improve the end-user experience.

2.6.12. Must have SaaS, on-premises, and Virtual Private Cloud managed service options for flexible consumption and financing.

2.6.13. Must have the following streamlined network operation requirements:

2.6.13.1. Provides a comprehensive single pane of glass dashboard for analyzing and improving wired and wireless LAN, and WAN performance at a global

or site-level, eliminating the inefficiencies of using disjointed, domain-specific network management tools.

2.6.13.2. Provides a consistent operating model and a unified platform for efficient management of compute, storage, and networking infrastructure, while enhancing cost controls. Users can log in using Single Sign-On (SSO) and are granted role-based access (RBAC) based on permissions. An additional layer of security can also be enabled with Multi-Factor Authentication (MFA).

2.6.13.3. Supports setup wizard automatically adds account subscriptions, matches device inventory from orders, and assigns purchased licenses, improving accuracy, and saving time.

2.6.13.4. Additional visibility into key values of individual and stacked switches is provided. This includes port status, PoE consumption, VLAN assignment, device and neighbor connections, power status and trends, alerts and events and which troubleshooting actions can be performed.

2.6.13.5. Geographic availability, scalability, and resiliency as this platform is hosted across regions in multiple public clusters of AWS, Azure, and GCP, maintaining points of presence worldwide, and enabling GDPR compliance.

2.6.13.6. Supports accelerated device onboarding, configuration, and provisioning with flexible options of templates and UI groups for all supported network devices at the device, group and MSP levels.

2.6.13.7. Zero Touch Provisioning (ZTP) supports simple, intuitive workflow for setting up devices with no onsite IT involvement. Configuration parameters at a network or site-level can be defined.

2.6.13.8. Supports IP-based IoT devices that can be securely onboarded with Device Provisioning Protocol (DPP) via QR code, certified by Wi-Fi Alliance as "Easy Connect," enabling quick, compliant installations with built-in device validation.

2.6.14. Must have the following AI and advanced analytic requirements:

2.6.14.1. Supports Network Insights to automatically detect and diagnose network issues using dynamic baselines, with built-in anomaly detection for precise problem identification, root cause, and remediation with close to 95% accuracy.

2.6.14.2. Supports AI Search, a GenAI-powered, natural language search engine that provides quick and precise answers, configuration tips, troubleshooting advice and more.

2.6.14.3. Supports AI Assist that uses event-driven automation to collect diagnostics for critical failure signatures, for proactive customer support and replacement workflows.

2.6.14.4. Supports self-healing workflows can be enabled to automatically update configurations as needed, helping IT fix issues without manual intervention.

2.6.14.5. Supports Dynamic power save mode in which APs switch into a dynamic power save mode and automatically wake up at a schedule when connectivity demand arises, reducing power demands and saving money in alignment with the organization’s sustainability initiatives.

2.6.14.6. Enhance wireless coverage and capacity using air match, built in AI/ML analyzes periodic RF data across the network to adjust AP settings dynamically based on changing conditions.

2.6.14.7. Enhance traditional radio and roaming techniques with client match, a patented RF optimization technology that continually enhances client connectivity and eliminates sticky clients.

2.6.15. Must have the following monitoring, reporting and troubleshooting capabilities:

2.6.15.1. Network and client health and assurance.

2.6.15.2. Application Health – Monitor app health, prioritize critical services by enforcing acceptable usage by site, device, or location. UCC analytics

provides a unified view of VoIP app performance like Zoom, Slack, and Teams, including MOS scores and insights on RF performance and capacity concerns. Additionally, by using SaaS express the branch gateways dynamically identify the optimal path to reach high-priority SaaS applications.

2.6.15.3. AI-based Connectivity Insights – Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more. For wired networks, IT administrators gain visibility on port status, PoE consumption, VLAN assignments, device and neighbor connections, power status, etc.

2.6.15.4. Wi-Fi Planning and Monitoring – Enhance Wi-Fi design, implementation, and monitoring with easy-to-use floorplans that depict accurate coverage patterns without employing extra sensors.

2.6.15.5. Extend Operations to IoT – Unifies visibility of IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices in the physical environment along with IP based IoT devices.

2.6.15.6. Live Events – Issue occurrence time, device name, type, category, description, packet logs, rich command line tools are captured and diagnostic checks such as ping tests, traceroutes and device-level performance tests are performed to troubleshoot issues.

2.6.15.7. Comprehensive Reports – Offers an extensive set of reporting capabilities on device connectivity, network and application health, throughput, usage data, device inventory, activity auditing, capacity planning, including the ability to baseline and compare user experience across various sites in the network.

2.6.15.8. Live upgrades – Simple GUI-based workflows and rules governing firmware upgrades on deployed network devices are available. These upgrades are scheduled at a site level during non-peak hours, ensuring continuous operations and reduced maintenance windows.

2.6.15.9. Extensibility through APIs and Webhooks – Customers developing network automation frameworks can automatically pull data from this solution into third-party solutions enabling IT operators to programmatically trigger actions based on certain events or conditions.

2.6.16. Must have the following Automate Security at Scale requirements:

2.6.16.1. Network wizard that simplifies the creation of underlays for campus and data-center environments. Manual errors are eliminated as network topology is automatically identified and configured with minimal user inputs.

2.6.16.2. Fabric wizard that enables IT administrators to automatically generate logical overlays without complex CLI programming, pushing inherent policies universally across wired, wireless, and WAN infrastructure for campus and data center environments.

2.6.16.3. Policy manager that empowers IT to define and maintain global policies at scale with ease, using UI-driven, intuitive workflows that automatically translate security intent into policy design and map user roles for employees, contractors, guests, and devices to their proper access privileges.

2.6.16.4. Client insights that dynamically compares devices against crowdsourced fingerprints of known clients and applies MAC range classification for unknown devices. Through deep packet inspection, network devices are automatically categorized, accurate policies are enforced based on context and behavioral information.

2.6.16.5. Cloud Auth and cloud-native NAC that streamlines end-user authentication for wired and wireless networks. IT admins have the flexibility to select from various authentication methods such as – uploading approved client MAC addresses or authenticating users through integrations with popular cloud

identity stores such as Google Workspace or Azure Active Directory and assigning the appropriate level of network access based on network profile.

2.6.16.6. Unique pre-shared passwords or passphrases that can be used to onboard user devices and non-user specific devices such as IP phones, cameras, thermostats etc., without prior device registration with Multi Pre-Shared Key (MPSK).

2.6.16.7. Users can leverage captive portal authorization methods for effortless network access.

2.6.16.8. Secure wireless segmentation – Multizone provides data separation for multi-tenancy, guest/visitor access, IoT devices, and other use cases. A single AP can connect to multiple gateways and tunnel traffic for isolation without requiring extra access points or managing another wireless network.

2.6.16.9. Intrusion detection – Rogue AP Intrusion Detection Service (RAPIDS) detects and resolves rogue AP issues, correlating wired and wireless data to enhance security and incident response, with optional Risk Oriented Traffic Inspection.

2.6.16.10. Web content filtering – Rates websites by reputation and risk, empowering IT to block malicious sites, preventing phishing, DDoS, and other attacks.

2.6.16.11. The Bill of Materials (BOM) must include 3-year Foundational subscriptions on all proposed devices to enable all primary enterprise features such as monitoring, reporting, and troubleshooting, onboarding, provisioning, orchestration, AI and analytics, content filtering, guest access, UXI integration, and 24x7 TAC software support.

3. BUDGET REQUIREMENTS

3.1. The budget for the procurement of One (1) Lot Supply, Delivery, Installation, Configuration, Implementation, Commissioning, and Support Services for the Establishment of Network Infrastructure for GCG Disaster Recovery Site and Extension Office - B is Nineteen Million Nine Hundred Thousand Pesos Only (₱19,900,000.00).

4. BIDDER REQUIREMENTS

4.1. General Requirements

4.1.1. The bidder must provide the following documents during the post-qualification:

4.1.1.1. a certification issued by the product manufacturer that they are a certified partner and able to extend direct technical support to end-user for each product brand being offered; and

4.1.1.2. copy of company's latest General Information Sheet (GIS).

4.1.2. The bidder must have at least five (5) years of continuous existence and engagement in the IT business.

4.1.3. The bidder must have completed a similar contract for the supply, delivery, and installation of firewall and network devices for the past three (3) years from the date of submission and receipt of bids.

4.1.4. The bidder must be a Platinum PhilGEPS registered supplier.

4.1.5. Subcontractors are prohibited.

4.2. Manpower Requirements

4.2.1. During post-qualification period, the bidder must provide a list of locally based manpower for the supply, delivery, installation, configuration, and commissioning of the proposed establishment of network infrastructure for GCG Disaster Recovery Site and Extension Office - B, with each personnel being a regular employee of the bidder for at least three (3) years:

4.2.1.1. two (2) certified network professionals of the proposed network devices;

4.2.1.2. two (2) certified internetworks of the proposed network devices; and

4.2.1.3. two (2) certified accredited engineers of the proposed NGFW.

4.2.2. The bidder must provide a photocopy of valid certifications, resume, and company ID of the identified local manpower during post-qualification.

4.3. Prior to submission of bid, the prospective bidder is required to conduct an ocular inspection of the GCG Main and Extension Office - B. The purpose of this inspection is to allow the bidder to be familiarized with the conditions and requirements for the feasibility of the project.

4.3.1. The bidder must send an email request to the GCG at procurement@gcg.gov.ph at least a day prior to their proposed schedule of mandatory ocular inspection. The email must contain the company name and the names of bidder representatives (maximum of 2). This is to secure in advance the required gate pass and permit to enter the office building prior to the scheduled date of ocular inspection.

4.3.2. The bidder must obtain a Certificate of Appearance as proof of their attendance at the ocular inspection. The certificate shall be issued by the designated representative of the GCG present during the inspection.

4.3.3. The Certificate of Appearance must be included in the bidder's submission along with the bid documents. Bids submitted without the Certificate of Appearance will be considered as non-compliant.

4.3.4. The GCG reserves the right to verify the accuracy of the information provided in the Certificate of Appearance. Any falsification of attendance will result in disqualification and other appropriate actions.

5. SCOPE OF WORK

The Winning Bidder (hereafter referred to as simply the "bidder") must:

5.1. Perform the supply, delivery, installation, configuration, implementation, commission, and support services of the proposed network infrastructure for the GCG Disaster Recovery Site and GCG Extension Office - B at 8th Floor BDO Towers Paseo (formerly Citibank Center) 8741 Paseo de Roxas Makati City.

5.2. Cover all cables, structured cabling, civil works, licenses and/or subscriptions needed for the establishment of network infrastructure of the GCG Disaster Recovery Site, including, but not limited to the following:

5.2.1. install, configure, and implement the proposed two (2) units of WAN Switches with complete integration to its proposed cloud-based Central Management Solution;

5.2.2. install, configure, and implement the proposed two (2) units of Next Generation Firewalls with complete integration to its proposed two (2) units of WAN Switches, to the existing two (2) units of External Firewalls in the GCG Main Office (Palo Alto 3220), and to the existing External Firewall Central Management Solution of the GCG;

5.2.3. install, configure, and implement the proposed two (2) units of Core Switches with complete integration to its proposed two (2) units of Next Generation Firewalls and to its proposed cloud-based Central Management Solution; and

5.2.4. install, integrate, and implement the existing GCG Hyperconverged Infrastructure System Solution for Disaster Recovery to its proposed Core Switches;

5.3. Cover all cables, structured cabling, civil works, licenses and/or subscriptions needed for the establishment of network infrastructure of the GCG Extension Office - B, including, but not limited to the following:

5.3.1. install, configure, and implement the proposed one (1) unit of WAN Switch with complete integration to its proposed cloud-based Central Management Solution;

5.3.2. install, configure, and implement the proposed two (2) units of Next Generation Firewalls with complete integration to its proposed one (1) unit of WAN Switch, to the existing two (2) units of External Firewalls in the GCG Main Office (Palo Alto 3220), and to the existing External Firewall Central Management Solution of the GCG;

5.3.3. install, configure, and implement the proposed two (2) units of Core Switches with complete integration to its proposed two (2) units of Next Generation Firewalls and to its proposed cloud-based Central Management Solution; and

5.3.4. install, configure, and implement the proposed two (2) units of LAN Access Switches with complete integration to its proposed two (2) units of Core Switches and to its proposed cloud-based Central Management Solution;

5.3.5. install, configure, and implement the proposed five (5) units of Wireless Access Points for the Workforce Area with complete integration to its proposed two (2) units of Core Switches and to its proposed cloud-based Central Management Solution;

5.3.6. install, configure, and implement the proposed two (2) units of Wireless Access Points for Meeting Rooms with complete integration to its proposed two (2) units of Core Switches and to its proposed cloud-based Central Management Solution; and

5.3.7. install the horizontal cabling distribution needed for the deployment of the new network equipment in the GCG Extension Office - B;

5.4. Deliver and pre-configure all equipment for the establishment of GCG Disaster Recovery Site at the GCG Office Main Office until such time that the new datacenter colocation becomes available.

5.5. Covers the transfer and re-deployment of the existing GCG Hyperconverged Infrastructure System Solution for Disaster Recovery from its current location (Luzon) to the new datacenter colocation site which will be located anywhere in Luzon.

5.6. Conduct Project Management using the below framework:

5.6.1. create a project team for the GCG and the bidder;

5.6.2. formulate project implementation plan;

5.6.3. conduct project kick-off;

5.6.4. implement and coordinate project milestones identified in the project implementation plan;

5.6.5. provide weekly/monthly/milestone project updates;

5.6.6. conduct hands-on technical training on the supplied equipment; and

5.6.7. provide and execute user acceptance and test plans.

5.7. Submit detailed project documentation in hard and soft copies:

5.7.1. Project Implementation Plan;

5.7.2. As built drawing;

5.7.3. Technical Reports;

5.7.4. UAT Test Plan;

5.7.5. Service Level Agreement; and

5.7.6. Warranty Agreement.

6. TRAINING REQUIREMENTS

6.1. The bidder shall provide in-depth knowledge transfer on product installation, configuration, administration, maintenance, management, and operation of each proposed equipment for the establishment of network infrastructure for GCG Disaster Recovery Site and Extension Office - B to be conducted by a designated product expert.

7. WARRANTY, MAINTENANCE, AND SUPPORT

7.1. The bidder must warrant that the Goods supplied are brand-new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the GCG provides otherwise.

7.2. The bidder must further warrant that all Goods supplied shall have no defect, arising from design, materials, or workmanship or from any act or omission of the bidder that may develop under normal use of the supplied Goods.

7.3. To ensure that manufacturing defects shall be corrected by the bidder, warranty, support services, and required subscriptions for all equipment and solutions shall be required from the bidder for a minimum period of three (3) years.

7.4. The GCG shall promptly notify the bidder in writing of any claims arising under this warranty. Upon receipt of such notice, the bidder shall, within the period specified and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the GCG.

7.5. If the bidder, having been notified, fails to remedy the defect(s) within the period specified, the GCG may proceed to take such remedial action as may be necessary, at the bidder’s risk and

expense and without prejudice to any other rights which the GCG may have against the bidder under the Contract and under the applicable laws.

7.6. In the event of any equipment failure, the bidder shall repair or automatically replace the defective products with the same product at no additional cost/charge to GCG.

7.7. A functional and workable service unit that is equivalent or higher in specification should be provided in case replacement of hardware would take more than twenty-four (24) hours or if repair requires pull out the equipment from GCG premises.

7.8. The bidder must provide a signed after sales service support certificate that the bidder will be supported by their principal in terms of parts and services.

7.9. The bidder must provide full-time support and managed services during the warranty period as specified:

7.9.1. single point of contact for all hardware and software components;

7.9.2. twenty-four hours by seven days (24x7) service desk support via telephone, email, or online chat portal;

7.9.3. at least one (1) hour response time upon receipt of issue escalation and four (4) hours for onsite support, if necessary;

7.9.4. if the problem was not resolved by service desk support, the bidder must provide an onsite technical support;

7.9.5. procedures on support and issue escalation; and

7.9.6. service report every after the onsite support.

8. TERMS OF PAYMENT

8.1. Payments shall be made only upon deployment completion of each item and a certification by the Chairperson or Authorized Representative of the GCG to the effect that the goods delivered is in accordance with this Terms of Reference (TOR) and have been duly accepted. Except with the prior approval of the Chairperson of the GCG, no payment shall be made for supplies and materials not yet delivered under this TOR.

8.2. Provided further that payment shall be made within twenty (20) working days from the receipt of complete documents, i.e., billing statement / statement of account, and other pertinent documents from the bidder.

8.3. All payments made to the bidder will be subjected to a five percent (5%) reduction, to serve as retention money. The said amounts shall only be released after the lapse of the warranty period.

9. CONFIDENTIALITY

9.1. Information or rights acquired and obtained from the GCG, including but not limited to any and all obligations prior to the termination or expiration hereof and provisions on confidentiality and proprietary rights, will remain in effect after termination of the services rendered to the GCG. Hence, the undertaking of the bidder not to disclose and to keep information confidential shall subsist even after the expiration or termination of its obligation to the GCG nor can the bidder, at any time, disclose items mentioned or enumerated in Section 9.2 or any information it acquires by virtue of the contract which the GCG deems confidential.

9.2. Records, documents, reports, and relevant data, such as diagrams, plans, designs, estimates, specifications, and other supporting records of materials complied and prepared in the courses of the performance of the services shall be absolute properties of GCG and shall not be used by the bidder for purposes not related to this agreement without prior written approval of GCG. Copies of such documents as required in this TOR shall be turned over to GCG upon completion of the project except that the bidder shall have the right to retain a copy of the same.

10. DELIVERY AND IMPLEMENTATION SCHEDULE

10.1. The delivery of goods, project implementation, documentation, and acceptance must be completed within ninety (90) calendar days from the receipt of the Notice to Proceed.

10.2. The bidder shall be subjected to evaluation by the end-user after the implementation of the project.

Statement of Conformity with Technical Specifications

Item	Specification	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.]

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, COMMISSIONING, AND SUPPORT SERVICES FOR THE ESTABLISHMENT OF NETWORK INFRASTRUCTURE FOR GCG DISASTER RECOVERY SITE AND EXTENSION OFFICE - B

ITEM	SPECIFICATION	STATEMENT OF COMPLIANCE
1. GCG DISASTER RECOVERY SITE (DRS) NETWORK INFRASTRUCTURE REQUIREMENTS		
1.1 EXTERNAL FIREWALL APPLIANCES		
	1.1.1 The bidder must provide two (2) units of Next Generation Firewall (NGFW) appliances with complete accessories and satisfy the minimum requirements and specifications below.	
	1.1.2 Must have at least 8.5 Gbps of firewall throughput.	
	1.1.3 Must have at least 4.2 Gbps of threat prevention throughput.	
	1.1.4 Must have at least 4.1 Gbps of Internet Protocol Security (IPsec) Virtual Private Network (VPN) throughput.	
	1.1.5 Must have the capability to support 945,000 maximum sessions and least 100,000 new sessions per second.	
	1.1.6 Must have at least eight (8) 10/100/1000, four (4) 1G/2.5G/5G /PoE, six (6) 1G SFP, and four (4) 1G/10G SFP/SFP+ ports for network traffic.	
	1.1.7 Must support high-availability (HA) setup both Active/Active and Active/Passive modes.	
	1.1.8 Must have at least 120 GB solid-state drive (SSD) pair, system storage.	
	1.1.9 Must have the following management interface options:	
	1.1.9.1 one (1) 10/100/1000 out-of-bond management port	
	1.1.9.2 one (1) HSCI 10 Gigabit High Availability port	
	1.1.9.3 one (1) RJ45 console port	
	1.1.9.4 one (1) USB port	
	1.1.9.5 one (1) Micro USB console port	
	1.1.10 Must have power supply redundancy.	
	1.1.11 Must have three (3) years warranty, support, and subscriptions.	
	1.1.12 Must have a similar operating system (OS) with the existing external firewalls of GCG to enable seamless integration and single-pane management to the existing Central Management Solution of the GCG.	
	1.1.13 Must have the following general and functional requirements:	
	1.1.13.1 The proposed NGWF must have a separate and dedicated CPU, memory, and hard drive for control plane and data plane. This is to avoid service interruption on the data processing plane when the control plane has been restarted or rebooted.	
	1.1.13.2 The proposed NGWF must have visibility into applications regardless of ports or protocols.	

	1.1.13.3	The proposed NGWF must support all the following authentication services: Directory services: Microsoft Active Directory, Microsoft Exchange, openLDAP, Novell eDirectory, RADIUS, Kerberos, TACACS+, Sun ONE Directory Server.	
	1.1.13.4	The proposed NGWF must support the identification of the traversing applications, regardless of port or protocol, even if the traffic is tunneled in GRE, GTP and NULL-IPSec, uses evasive tactics, or is encrypted without the need of additional software / hardware.	
	1.1.13.5	The proposed NGWF must allow the administrator(s) to review any policy impact for new or modified application signatures included in a content release version. This Web GUI feature will enable the administrator(s) to simultaneously update the security policies and install new content and allows for a seamless shift in policy enforcement.	
	1.1.13.6	The proposed NGWF must be able to block source IP addresses performing DoS attacks on the hardware INGRESS level even before consuming any CPU or packet buffer resource without any user configuration.	
	1.1.13.7	The proposed NGWF must have a policy optimizer which is able filter rules who are used or unused in specific time frames such as 30 days, 90 days, etc., with an external management device.	
	1.1.13.8	The proposed NGWF must be able to decrypt, inspect and control both inbound and outbound SSL and SSH connections to prevent unwanted activities or malicious content on the same proposed hardware, also serve as the decryption broker to other security devices.	
	1.1.13.9	The proposed NGWF must have the capability to define a Threshold to indicate the minimum number of hours after an update becomes available before the firewall will download it regardless of the schedule.	
	1.1.13.10	The proposed NGWF must include individual user activity report showing applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period without additional software and hardware modules.	
	1.1.14	Must have the following threat protection capabilities:	
	1.1.14.1	The proposed NGWF must have protection against the most recent and relevant malware with payload signatures, not hash, to block known and future variants of malware, and receive the latest security updates.	
	1.1.14.2	The proposed NGWF must support a protocol decoder-based analysis that stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits.	
	1.1.14.3	The proposed NGWF must have integrated IPS, anti-spyware, anti-malware, and Command-and-Control (C2) prevention capabilities.	
	1.1.14.4	The proposed NGWF must deliver inline machine learning (ML) at the network level and should block unknown threats	

	in real time instead of waiting for a sandbox- integrated directly on the NGFW.	
	1.1.14.5 The proposed NGWF must support inline cloud analysis that detects command and SQL injection vulnerabilities in real time to protect users against zero-day threats.	
	1.1.14.6 The proposed NGWF must support local deep learning which complements cloud-based inline cloud analysis component of the solution.	
	1.1.15 Must have the following sandboxing capabilities:	
	1.1.15.1 The proposed NGWF must completely eliminate the need for standalone IPS or IDS solutions.	
	1.1.15.2 The proposed NGWF must prevent highly evasive malware via stealthy observation to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.	
	1.1.15.3 The proposed NGWF must support uncovering malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis to prevent malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing.	
	1.1.15.4 The proposed NGWF must support an intelligent runtime memory analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed.	
	1.1.15.5 The proposed NGWF must operate a series of inline cloud ML-based detection engines to analyze PE (portable executable) samples traversing through your network to detect and prevent unknown malware in real-time.	
	1.1.15.6 The proposed NGWF must hold files from downloading (and potentially spreading within your network) while analyzing these suspicious files for malware in the cloud, in a real-time exchange.	
	1.1.15.7 The proposed NGWF must operates using a lightweight forwarding mechanism on the firewall to minimize any local performance impact; and to keep up with the latest changes in the threat landscape, cloud inline ML detection models are added and updated seamlessly in the cloud, without requiring content updates or feature release support.	
	1.1.15.8 The proposed NGWF must support analysis of email links by extracting HTTP/HTTPS contained in SMTP and POP3 email messages.	
	1.1.16 Must have the following Uniform Resource Locator (URL) filtering capabilities:	
	1.1.16.1 The proposed NGWF must protect the GCG network and its users against malicious and evasive web-based threats—both known and unknown.	
	1.1.16.2 The proposed NGWF must support inline real time web threat prevention by using cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring	

		protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).	
	1.1.16.3	The proposed NGWF must support phishing image detection with ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.	
	1.1.16.4	The proposed NGWF must support translation site filtering that applies advanced URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.	
	1.1.16.5	The proposed NGWF must inspect for phishing and malicious JavaScript using local inline categorization, a firewall-based analysis solution, which can block unknown malicious web pages in real-time.	
	1.1.17	Must have the following Domain Name System (DNS) security capabilities:	
	1.1.17.1	The proposed NGFW must stop known and unknown DNS traffic with machine learning and predictive analytics.	
	1.1.17.2	The proposed NGFW must help identify systems that are infected/ compromised by sinkholing DNS request to a C2 server.	
	1.1.17.3	The proposed NGFW must protect against Domain Generation Algorithms (DGA) based attacks which generate random domains on the fly for malware to use as a way to call back to a C2 server.	
	1.1.17.4	The proposed NGFW must protect against DNS tunneling based attacks that utilize crafted DNS queries and response to hide malware delivery, command-and control traffic or data exfiltration/extraction.	
	1.1.17.5	The proposed NGFW must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.	
	1.1.17.6	The proposed NGFW must protect against strategically aged domains using predictive analytics. It must protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.	
	1.1.17.7	The proposed NGFW must prevent fast flux, technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.	
	1.1.17.8	The proposed NGFW must protect against domains surreptitiously added to hacked DNS zones of reputable domains.	
	1.1.17.9	The proposed NGFW must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.	
	1.1.17.10	The proposed NGFW must prevent dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.	

	1.1.17.11 The proposed NGFW must support the following DNS security categories: C2, Dynamic DNS (DDNS), malware, newly registered domains, phishing, grayware, parked, and proxy avoidance & anonymizers.	
	1.1.18 Must have the following software-defined wide area network (SDWAN) capabilities:	
	1.1.18.1 The proposed NGFW must be integrated into the operating system of the next generation secure-SDWAN.	
	1.1.18.2 The proposed NGFW must support dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss.	
	1.1.18.3 The proposed NGFW must support security features, such as user and application identification/control, to provide complete traffic and security control.	
	1.1.18.4 The proposed NGFW must support link bundling of different Internet Service Provider (ISP).	
	1.1.18.5 The proposed NGFW must support path quality profile for each set of business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage.	
	1.1.18.6 The proposed NGFW must support the following types of WAN connections that terminates as ethernet to the device's interface: ADSL/DSL, cable modem, ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, Wi-Fi, and anything that terminates as ethernet to the device's interface.	
	1.1.18.7 The proposed NGFW must be able to monitor business-critical Software as a Service (SaaS) application to monitor the latency, jitter, and packet loss and able to swap from available WAN links to ensure application usability.	
	1.1.18.8 The proposed NGFW must support forward error correction.	
	1.1.18.9 The proposed NGFW must support packet duplication.	
	1.1.18.10 The proposed NGFW must have SD-WAN traffic distribution profiles, such as: Best Available Path, Top-Down Priority, and Weighted Session Distribution.	
	1.1.18.11 The proposed NGFW must have direct internet access (DIA) SD-WAN.	
	1.1.18.12 The proposed NGFW must support Hub-and-Spoke topology.	
	1.1.18.13 The proposed NGFW must support Full Mesh VPN topology.	
	1.1.18.14 The proposed NGFW must support Full Mesh VPN Cluster with DDNS Service.	
	1.1.18.15 The proposed NGFW must be managed in the central management console.	

	1.1.18.16 The proposed NGFW must have a dashboard for visibility into your SD-WAN links and performance so that the administrator can adjust the path quality thresholds and other aspects of SD-WAN to improve its performance.	
	1.1.18.17 The proposed NGFW must have centralized statistics and reporting including application and link performance statistics, path health measurements and trend analysis, and focused views of application and link issues.	
	1.1.19 Must have the following remote client / user VPN capabilities:	
	1.1.19.1 The proposed NGFW must provide management functions for VPN infrastructure.	
	1.1.19.2 The proposed NGFW must provide security enforcement for traffic from VPN applications.	
	1.1.19.3 The proposed NGFW must provide application software that runs on endpoints and enables access to the GCG network resources through the VPN portals and gateways.	
	1.1.19.4 The proposed NGFW must perform host information profile checking to enforce security posture on endpoints.	
	1.1.19.5 The proposed NGFW must support identification of managed devices using the endpoint serial number on gateways.	
	1.1.19.6 The proposed NGFW must support mobile applications for endpoints running iOS, Android, Chrome OS, and Windows 10.	
	1.1.19.7 The proposed NGFW must support endpoints running Linux aside from Windows and MacOS.	
	1.1.19.8 The proposed NGFW must support split tunneling based on destination domain, client process, and video streaming application.	
	1.1.19.9 The proposed NGFW must support adding a compromised device to the quarantine list.	
	1.1.19.10 The proposed NGFW must provide 200 maximum Secure Sockets Layer (SSL) VPN tunnels.	
	1.1.19.11 The proposed NGFW must provide 1500 maximum tunnels for client VPN (SSL, IPSec, and IKE with XAUTH).	
	1.1.19.12 The proposed NGFW must provide secure remote access or VPN solution via single or multiple internal/external gateways.	
	1.1.19.13 The proposed NGFW must provide authentication via LDAP, SAML, Kerberos, RADIUS or TACACS.	
1.2 WIDE AREA NETWORK (WAN) SWITCHES		
	1.2.1 The bidder must provide two (2) units of WAN Switch (WANS) with complete accessories and satisfy the minimum requirements and specifications below.	
	1.2.2 Must have enterprise-class Layer 2 connectivity with support for ACLs, robust QoS and routing.	
	1.2.3 Must be a 1U rack mountable switch with full density 24 x 10/100/1000Base-T ports and 4 x 1G/10G SFP ports.	

	1.2.4 Must have built-in high speed 1/10GbE uplinks.	
	1.2.5 Must be a software defined ready with REST APIs.	
	1.2.6 Must have simple deployment with zero touch provisioning.	
	1.2.7 Must simplify add, move, and change with colorless ports.	
	1.2.8 Must have three (3) years warranty, support, and subscriptions.	
	1.2.9 Must have intelligent monitoring, visibility, and remediation with analytics engine.	
	1.2.10 Must be manageable via single pane of glass across wired, wireless, and WAN.	
	1.2.11 Must support automated configuration and verification.	
	1.2.12 Must enable secure and simple access for users and Internet of Things (IoT).	
	1.2.13 Must have the following QoS requirements:	
	1.2.13.1 The proposed WANS must support SP queuing.	
	1.2.13.2 The proposed WANS must have traffic prioritization (IEEE 802.1p) for real-time classification.	
	1.2.13.3 The proposed WANS have Class of Service (CoS) that sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and differentiated service.	
	1.2.13.4 The proposed WANS must have rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.	
	1.2.13.5 The proposed WANS must have large buffers for graceful congestion management.	
	1.2.14 Must have the following Resiliency and High Availability requirements:	
	1.2.14.1 The proposed WANS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
	1.2.14.2 The proposed WANS must support IEEE 802.3ad LACP that supports up to 8 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm.	
	1.2.14.3 The proposed WANS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
	1.2.14.4 The proposed WANS must have smart link that provides easy-to-configure link redundancy of active and standby links.	
	1.2.15 Must have the following Performance and Connectivity requirements:	
	1.2.15.1 The proposed WANS must have up to 128 Gbps in non-blocking bandwidth and up to 95.2 Mpps for forwarding.	

	1.2.15.2	The proposed WANS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.	
	1.2.15.3	The proposed WANS must have 24x ports 10/100/1000Base-T ports and 4x 1G/10G SFP ports.	
	1.2.15.4	The proposed WANS must have the following management interface options: 1.2.15.4.1 one (1) x USB-C console port. 1.2.15.4.2 one (1) x USB Type A host port.	
	1.2.15.5	The proposed WANS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
	1.2.15.6	The proposed WANS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
	1.2.16	Must have the following Management requirements:	
	1.2.16.1	The proposed WANS must have a built-in programmable and easy-to-use REST API interface.	
	1.2.16.2	The proposed WANS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	
	1.2.16.3	The proposed WANS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
	1.2.16.4	The proposed WANS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
	1.2.16.5	The proposed WANS must support SNMP v2c/v3 that provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.	
	1.2.16.6	The proposed WANS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group.	
	1.2.16.7	The proposed WANS must support TFTP and SFTP that offer different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.	
	1.2.16.8	The proposed WANS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	

	1.2.16.9 The proposed WANS must support IEEE 802.1AB LLDP that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
	1.2.16.10 The proposed WANS must support dual flash images that provide independent primary and secondary operating system files for backup while upgrading.	
	1.2.16.11 The proposed WANS must assign descriptive names to ports for easy identification.	
	1.2.16.12 The proposed WANS multiple configuration files can be stored to a flash image.	
	1.2.16.13 The proposed WANS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
	1.2.17 Must have the following Layer 2 Switching requirements:	
	1.2.17.1 The proposed WANS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously.	
	1.2.17.2 The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,220 bytes.	
	1.2.17.3 The proposed WANS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
	1.2.17.4 The proposed WANS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.	
	1.2.17.5 The proposed WANS must support MVRP that allows automatic learning and dynamic assignment of VLANs.	
	1.2.17.6 The proposed WANS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.	
	1.2.17.7 The proposed WANS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.	
	1.2.17.8 The proposed WANS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
	1.2.18 Must have the following Layer 3 Services and Routing requirements:	
	1.2.18.1 The proposed WANS must support ARP determines the MAC address of another IP host in the same subnet; supports static ARPs.	
	1.2.18.2 The proposed WANS must support DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
	1.2.18.3 The proposed WANS must support internal loopback testing for maintenance purposes and increased	

		availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.	
	1.2.18.4	The proposed WANS must support Dynamic Host Configuration Protocol (DHCP) that simplifies the management of large IP networks and supports client; DHCPv4 Relay support enables DHCP operation across subnets.	
	1.2.18.5	The proposed WANS must have static IP routing that provides manually configured routing.	
	1.2.18.6	The proposed WANS must have dual stack static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routing. Dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.	
	1.2.19	Must have the following Security requirements:	
	1.2.19.1	The proposed WANS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
	1.2.19.2	The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
	1.2.19.3	The proposed WANS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
	1.2.19.4	The proposed WANS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.	
	1.2.19.5	The proposed WANS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
	1.2.19.6	The proposed WANS must support MAC-based client authentication.	
	1.2.19.7	The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
	1.2.19.8	The proposed WANS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.	
	1.2.19.9	The proposed WANS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	
	1.2.19.10	The proposed WANS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	

	1.2.19.11 The proposed WANS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.	
	1.2.19.12 The proposed WANS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
	1.2.19.13 The proposed WANS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	
	1.2.20 Must have the following Multicast requirements:	
	1.2.20.1 The proposed WANS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
	1.2.20.2 The proposed WANS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
	1.2.20.3 The proposed WANS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
1.3 CORE SWITCHES		
	1.3.1 The bidder must provide two (2) units of Core Switch (CS) with complete accessories and satisfy the minimum requirements and specifications below.	
	1.3.2 Must be a stackable Layer 3 switch with Border Gateway Protocol (BGP), Ethernet VPN (EVPN), Virtual eXtensible Local-Area Network (VXLAN), Virtual Routing and Forwarding (VRF), and Open Shortest Path First (OSPF) with robust security and Quality of service (QoS).	
	1.3.3 Must have at least 780 Gbps system switching capacity, 580 Mega Packet Per Second (Mpps) system throughput, and up to 200 Gbps stacking bandwidth.	
	1.3.4 Must be a 1U rack mountable switch with full density 24 x 1G/10G SFP+ ports (LRM + MACsec), 2 x 10G/25G/50G SFP ports, and 2 x 10G/25G SFP ports (MACsec).	
	1.3.5 Must have built-in high speed 10GbE/25GbE/50GbE uplinks.	
	1.3.6 Must have three (3) years warranty, support, and subscriptions.	
	1.3.7 Must have intelligent monitoring, visibility, and remediation with analytics engine.	
	1.3.8 Must be manageable via single pane of glass across wired, wireless, and WAN.	
	1.3.9 Must support automated configuration and verification.	
	1.3.10 Must enable secure and simple access for users and Internet of Things (IoT).	
	1.3.11 Must have the following QoS requirements:	
	1.3.11.1 The proposed CS must support Strict Priority (SP) queuing and Deficit Weighted Round Robin (DWRR).	

	1.3.11.2 The proposed CS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.	
	1.3.11.3 The proposed CS transmission rates of egressing frames can be limited on a per-queue basis using Egress Queue Shaping (EQS).	
	1.3.12 Must have the following Resiliency and High Availability requirements:	
	1.3.12.1 The proposed CS must have high performance front plane stacking for up to 10 switches.	
	1.3.12.2 The proposed CS must have the flexibility to mix both modular and fixed models within a single stack.	
	1.3.12.3 The proposed CS must have hot swappable power supplies.	
	1.3.12.4 The proposed CS must provide N+1 and N+N redundancy for high reliability in the event of power line or supply failures.	
	1.3.12.5 The proposed CS must support Virtual Router Redundancy Protocol (VRRP) that allows groups of two routers to dynamically back each other up to create highly available routed environments.	
	1.3.12.6 The proposed CS must support Unidirectional Link Detection (UDLD) that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
	1.3.12.7 The proposed CS must support IEEE 802.3ad Link Aggregation Control Protocol (LACP) that supports up to 54 link aggregation groups (LAGs), each with eight links per group with a user-selectable hashing algorithm.	
	1.3.12.8 The proposed CS must support Microsoft Network Load Balancer (NLB) for server applications.	
	1.3.12.9 The proposed CS must support Ethernet Ring Protection Switching (ERPS) that provides rapid protection and recovery in a ring topology.	
	1.3.12.10 The proposed CS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
	1.3.13 Must have the following Performance and Connectivity requirements:	
	1.3.13.1 The proposed CS must have up to 780 Gbps in non-blocking bandwidth and up to 580 Mpps for forwarding.	
	1.3.13.2 The proposed CS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.	
	1.3.13.3 The proposed CS must have 24x 1G/10G SFP+ ports (LRM + MACsec), 2x 10G/25G/50G SFP ports, and 2x 10G/25G SFP ports (MACsec).	

	1.3.13.4 The proposed CS must have the following management interface options: 1.3.13.4.1 one (1) x USB-C console port. 1.3.13.4.2 one (1) x RJ Console Port 1.3.13.4.3 one (1) x OOBM port. 1.3.13.4.4 one (1) x USB Type A host port.	
	1.3.13.5 The proposed CS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
	1.3.13.6 The proposed CS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
	1.3.13.7 The proposed CS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.	
	1.3.14 Must have the following Management requirements:	
	1.3.14.1 The proposed CS must have scalable application specific integrated circuit (ASIC)-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	
	1.3.14.2 The proposed CS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.	
	1.3.14.3 The proposed CS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
	1.3.14.4 The proposed CS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
	1.3.14.5 The proposed CS must support Simple Network Management Protocol (SNMP) v2c/v3 which provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.	
	1.3.14.6 The proposed CS must support remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	
	1.3.14.7 The proposed CS must support Trivial File Transfer Protocol (TFTP) and Secure File Transfer Protocol (SFTP) that offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over a Secure Shell (SSH) tunnel to provide additional security.	
	1.3.14.8 The proposed CS must support Network Time Protocol (NTP) that synchronizes timekeeping among distributed	

	time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	
	1.3.14.9 The proposed CS must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
	1.3.14.10 The proposed CS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.	
	1.3.14.11 The proposed CS must be able to assign descriptive names to ports for easy identification.	
	1.3.14.12 The proposed CS multiple configuration files can be stored to a flash image.	
	1.3.14.13 The proposed CS ingress and egress port monitoring must enable more efficient network problem solving.	
	1.3.14.14 The proposed CS must support unidirectional link detection (UDLD) that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
	1.3.14.15 The proposed CS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for Voice over Internet Protocol (VoIP) tests.	
	1.3.14.16 The proposed CS must support precision time protocol that allows precise clock synchronization across distributed network switches as defined in IEEE 1588.	
	1.3.15 Must have the following Layer 2 Switching requirements:	
	1.3.15.1 The proposed CS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).	
	1.3.15.2 The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.	
	1.3.15.3 The proposed CS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.	
	1.3.15.4 The proposed CS must support Rapid Per-VLAN Spanning Tree (RPVST+) that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.	
	1.3.15.5 The proposed CS must support Multiple VLAN Registration Protocol (MVRP) that allows automatic learning and dynamic assignment of VLANs.	
	1.3.15.6 The proposed CS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.	
	1.3.15.7 The proposed CS must support Bridge Protocol Data Unit (BPDU) tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	

	1.3.15.8	The proposed CS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
	1.3.15.9	The proposed CS must have Spanning Tree Protocol (STP) supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).	
	1.3.15.10	The proposed CS must support Internet Group Management Protocol (IGMP) that controls and manages the flooding of multicast packets in a Layer 2 network.	
	1.3.15.11	The proposed CS must have IPv4 Multicast in VXLAN/EVPN overlay support which allows Protocol-Independent Multicast Sparse Mode (PIMSM)/IGMP snooping in the VXLAN overlay.	
	1.3.15.12	The proposed CS must have IPv6 VXLAN/EVPN overlay support which allows IPv6 traffic over the VXLAN overlay.	
	1.3.15.13	The proposed CS must have VXLAN Address Resolution Protocol (ARP)/ Neighbor Discovery (ND) suppression which allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network.	
	1.3.16	Must have the following Layer 3 Services and Routing requirements:	
	1.3.16.1	The proposed CS must have ARP that determines the MAC address of another IP host in the same subnet; supports static ARPs.	
	1.3.16.2	The proposed CS must have a DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
	1.3.16.3	The proposed CS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility.	
	1.3.16.4	The proposed CS must have route maps that provide more control during route redistribution; allow filtering and altering of route metrics.	
	1.3.16.5	The proposed CS must have Border Gateway Protocol 4 (BGP-4) that delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks with graceful restart capability.	
	1.3.16.6	The proposed CS must have Multi-protocol BGP (MP-BGP) that enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6.	
	1.3.16.7	The proposed CS must have open shortest path first (OSPF) that delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports	

		ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery.	
	1.3.16.8	The proposed CS must have Equal-Cost Multipath (ECMP) that enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.	
	1.3.16.9	The proposed CS must have static IP routing that provides manually configured routing; includes ECMP capability.	
	1.3.16.10	The proposed CS must have policy-based routing that uses a classifier to select traffic that can be forwarded based on policy set by the network administrator.	
	1.3.16.11	The proposed CS must have IP performance optimization that provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.	
	1.3.16.12	The proposed CS must have dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.	
	1.3.17	Must have the following Security requirements:	
	1.3.17.1	The proposed CS must have Access Control List (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
	1.3.17.2	The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
	1.3.17.3	The proposed CS must have management access security for both on- and off-box authentication for administrative access. RADIUS or Terminal Access Controller Access Control System (TACACS)+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
	1.3.17.4	The proposed CS must support Control Plane Policing (CoPP) which sets rate limit on control protocols to protect CPU overload from Denial-of-Service (DOS) attacks.	
	1.3.17.5	The proposed CS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
	1.3.17.6	The proposed CS must support MAC-based client authentication.	
	1.3.17.7	The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
	1.3.17.8	The proposed CS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.	

	1.3.17.9 The proposed CS must have Internet Control Message Protocol (ICMP) throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	
	1.3.17.10 The proposed CS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	
	1.3.17.11 The proposed CS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.	
	1.3.17.12 The proposed CS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
	1.3.17.13 The proposed CS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	
	1.3.18 Must have the following Multicast requirements:	
	1.3.18.1 The proposed CS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
	1.3.18.2 The proposed CS must support Multicast Listener Discovery (MLD) that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
	1.3.18.3 The proposed CS must support Protocol Independent Multicast (PIM) that defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM Sparse Mode (SM) and Dense Mode (DM) for both IPv4 and IPv6.	
	1.3.18.4 The proposed CS must support IGMP that utilizes Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
1.4 CENTRAL MANAGEMENT SOLUTION FOR NETWORK EQUIPMENT		
	1.4.1 The bidder must provide one (1) lot cloud-based Central Management Solution for the proposed two (2) units of WAN Switch and two (2) units of Core Switch (CS) with minimum requirements and specifications below.	
	1.4.2 Must be a similar platform with the existing Central Management Solution for the existing network devices of the GCG to ensure seamless integration and single-pane management of the new and existing equipment.	
	1.4.3 Must have three (3) years warranty, support, and subscriptions.	
	1.4.4 Must have unified management of wireless, wired, VPN, and SD-WAN for simplified operations.	
	1.4.5 Must have network fabric orchestration, intent-based policy engine, and access controls for unified policy management, automated network provisioning, and zero-trust security.	
	1.4.6 Must have Artificial Intelligence (AI)-based network insights for faster troubleshooting and continuous network optimization.	

	1.4.7 Must have client insights for inline client profiling and telemetry to close visibility gaps.	
	1.4.8 Must have live chat and an AI-based search engine for an enhanced support experience.	
	1.4.9 Must have APIs and webhooks to augment the value of other leading IT platforms in your environment.	
	1.4.10 Must have powerful monitoring and troubleshooting for remote or home office networks.	
	1.4.11 Must have integration with user experience insight to proactively monitor and improve the end-user experience.	
	1.4.12 Must have SaaS, on-premises, and Virtual Private Cloud managed service options for flexible consumption and financing.	
	1.4.13 Must have the following streamlined network operation requirements:	
	1.4.13.1 Provides a comprehensive single pane of glass dashboard for analyzing and improving wired and wireless LAN, and WAN performance at a global or site-level, eliminating the inefficiencies of using disjointed, domain-specific network management tools.	
	1.4.13.2 Provides a consistent operating model and a unified platform for efficient management of compute, storage, and networking infrastructure, while enhancing cost controls. Users can log in using Single Sign-On (SSO) and are granted role-based access (RBAC) based on permissions. An additional layer of security can also be enabled with Multi-Factor Authentication (MFA).	
	1.4.13.3 Supports setup wizard automatically adds account subscriptions, matches device inventory from orders, and assigns purchased licenses, improving accuracy, and saving time.	
	1.4.13.4 Additional visibility into key values of individual and stacked switches is provided. This includes port status, PoE consumption, VLAN assignment, device and neighbor connections, power status and trends, alerts and events and which troubleshooting actions can be performed.	
	1.4.13.5 Geographic availability, scalability, and resiliency as this platform is hosted across regions in multiple public clusters of AWS, Azure, and GCP, maintaining points of presence worldwide, and enabling GDPR compliance.	
	1.4.13.6 Supports accelerated device onboarding, configuration, and provisioning with flexible options of templates and UI groups for all supported network devices at the device, group and MSP levels.	
	1.4.13.7 Zero Touch Provisioning (ZTP) supports simple, intuitive workflow for setting up devices with no onsite IT involvement. Configuration parameters at a network or site-level can be defined.	
	1.4.13.8 Supports IP-based IoT devices that can be securely onboarded with Device Provisioning Protocol (DPP) via QR code, certified by Wi-Fi Alliance as "Easy Connect,"	

	enabling quick, compliant installations with built-in device validation.	
	1.4.14 Must have the following AI and advanced analytic requirements:	
	1.4.14.1 Supports Network Insights to automatically detect and diagnose network issues using dynamic baselines, with built-in anomaly detection for precise problem identification, root cause, and remediation with close to 95% accuracy.	
	1.4.14.2 Supports AI Search, a GenAI-powered, natural language search engine that provides quick and precise answers, configuration tips, troubleshooting advice and more.	
	1.4.14.3 Supports AI Assist that uses event-driven automation to collect diagnostics for critical failure signatures, for proactive customer support and replacement workflows.	
	1.4.14.4 Supports self-healing workflows can be enabled to automatically update configurations as needed, helping IT fix issues without manual intervention.	
	1.4.14.5 Supports Dynamic power save mode in which APs switch into a dynamic power save mode and automatically wake up at a schedule when connectivity demand arises, reducing power demands and saving money in alignment with the organization's sustainability initiatives.	
	1.4.14.6 Enhance wireless coverage and capacity using air match, built in AI/ML analyzes periodic RF data across the network to adjust AP settings dynamically based on changing conditions.	
	1.4.14.7 Enhance traditional radio and roaming techniques with client match, a patented RF optimization technology that continually enhances client connectivity and eliminates sticky clients.	
	1.4.15 Must have the following monitoring, reporting and troubleshooting capabilities:	
	1.4.15.1 Network and client health and assurance.	
	1.4.15.2 Application Health – Monitor app health, prioritize critical services by enforcing acceptable usage by site, device, or location. UCC analytics provides a unified view of VoIP app performance like Zoom, Slack, and Teams, including MOS scores and insights on RF performance and capacity concerns. Additionally, by using SaaS express the branch gateways dynamically identify the optimal path to reach high-priority SaaS applications.	
	1.4.15.3 AI-based Connectivity Insights – Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more. For wired networks, IT administrators gain visibility on port status, PoE consumption, VLAN assignments, device and neighbor connections, power status, etc.	
	1.4.15.4 Wi-Fi Planning and Monitoring – Enhance Wi-Fi design, implementation, and monitoring with easy-to-use floorplans that depict accurate coverage patterns without employing extra sensors.	

	1.4.15.5	Extend Operations to IoT – Unifies visibility of IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices in the physical environment along with IP based IoT devices.	
	1.4.15.6	Live Events – Issue occurrence time, device name, type, category, description, packet logs, rich command line tools are captured and diagnostic checks such as ping tests, traceroutes and device-level performance tests are performed to troubleshoot issues.	
	1.4.15.7	Comprehensive Reports – Offers an extensive set of reporting capabilities on device connectivity, network and application health, throughput, usage data, device inventory, activity auditing, capacity planning, including the ability to baseline and compare user experience across various sites in the network.	
	1.4.15.8	Live upgrades – Simple GUI-based workflows and rules governing firmware upgrades on deployed network devices are available. These upgrades are scheduled at a site level during non-peak hours, ensuring continuous operations and reduced maintenance windows.	
	1.4.15.9	Extensibility through APIs and Webhooks – Customers developing network automation frameworks can automatically pull data from this solution into third-party solutions enabling IT operators to programmatically trigger actions based on certain events or conditions.	
	1.4.16	Must have the following Automate Security at Scale requirements:	
	1.4.16.1	Network wizard that simplifies the creation of underlays for campus and data-center environments. Manual errors are eliminated as network topology is automatically identified and configured with minimal user inputs.	
	1.4.16.2	Fabric wizard that enables IT administrators to automatically generate logical overlays without complex CLI programming, pushing inherent policies universally across wired, wireless, and WAN infrastructure for campus and data center environments.	
	1.4.16.3	Policy manager that empowers IT to define and maintain global policies at scale with ease, using UI-driven, intuitive workflows that automatically translate security intent into policy design and map user roles for employees, contractors, guests, and devices to their proper access privileges.	
	1.4.16.4	Client insights that dynamically compares devices against crowdsourced fingerprints of known clients and applies MAC range classification for unknown devices. Through deep packet inspection, network devices are automatically categorized, accurate policies are enforced based on context and behavioral information.	
	1.4.16.5	Cloud Auth and cloud-native NAC that streamlines end-user authentication for wired and wireless networks. IT admins have the flexibility to select from various authentication methods such as – uploading approved client MAC addresses or authenticating users through	

		integrations with popular cloud identity stores such as Google Workspace or Azure Active Directory and assigning the appropriate level of network access based on network profile.	
	1.4.16.6	Unique pre-shared passwords or passphrases that can be used to onboard user devices and non-user specific devices such as IP phones, cameras, thermostats etc., without prior device registration with Multi Pre-Shared Key (MPSK).	
	1.4.16.7	Users can leverage captive portal authorization methods for effortless network access.	
	1.4.16.8	Secure wireless segmentation – Multizone provides data separation for multi-tenancy, guest/visitor access, IoT devices, and other use cases. A single AP can connect to multiple gateways and tunnel traffic for isolation without requiring extra access points or managing another wireless network.	
	1.4.16.9	Intrusion detection – Rogue AP Intrusion Detection Service (RAPIDS) detects and resolves rogue AP issues, correlating wired and wireless data to enhance security and incident response, with optional Risk Oriented Traffic Inspection.	
	1.4.16.10	Web content filtering – Rates websites by reputation and risk, empowering IT to block malicious sites, preventing phishing, DDoS, and other attacks.	
	1.4.16.11	The Bill of Materials (BOM) must include 3-year Foundational subscriptions on all proposed devices to enable all primary enterprise features such as monitoring, reporting, and troubleshooting, onboarding, provisioning, orchestration, AI and analytics, content filtering, guest access, UXI integration, and 24x7 TAC software support.	
2. GCG EXTENSION OFFICE - B NETWORK INFRASTRUCTURE REQUIREMENTS			
2.1 EXTERNAL FIREWALL APPLIANCES			
	2.1.1	The bidder must provide two (2) units of Next Generation Firewall (NGFW) appliances with complete accessories and satisfy the minimum requirements and specifications below.	
	2.1.2	Must have at least 3.3 Gbps of firewall throughput.	
	2.1.3	Must have at least 2.1 Gbps of threat prevention throughput.	
	2.1.4	Must have at least 1.7 Gbps of VPN throughput.	
	2.1.5	Must have the capability to support 300,000 maximum sessions and least 48,000 new sessions per second.	
	2.1.6	Must have at least eight (8) 1G RJ45 ports for network traffic.	
	2.1.7	Must support high-availability (HA) setup both Active/Active and Active/Passive modes.	
	2.1.8	Must have at least 128 GB embedded multi-media card (eMMC) storage.	
	2.1.9	Must have the following management interface options:	
	2.1.9.1	one (1) 10/100/1000 out-of-bond management port	

	2.1.9.2 one (1) RJ45 console port	
	2.1.9.3 one (1) USB port	
	2.1.9.4 one (1) Micro USB console port	
	2.1.10 Must have power supply redundancy.	
	2.1.11 Must have three (3) years warranty, support, and subscriptions.	
	2.1.12 Must have a similar operating system (OS) with the existing external firewalls of GCG to enable seamless integration and single-pane management to the existing Central Management Solution of the GCG.	
	2.1.13 Must have the following general and functional requirements:	
	2.1.13.1 The proposed NGWF must have a separate and dedicated CPU, memory, and hard drive for control plane and data plane. This is to avoid service interruption on the data processing plane when the control plane has been restarted or rebooted.	
	2.1.13.2 The proposed NGWF must have visibility into applications regardless of ports or protocols.	
	2.1.13.3 The proposed NGWF must support all the following authentication services: Directory services: Microsoft Active Directory, Microsoft Exchange, openLDAP, Novell eDirectory, RADIUS, Kerberos, TACACS+, Sun ONE Directory Server.	
	2.1.13.4 The proposed NGWF must support the identification of the traversing applications, regardless of port or protocol, even if the traffic is tunneled in GRE, GTP and NULL-IPSec, uses evasive tactics, or is encrypted without the need of additional software / hardware.	
	2.1.13.5 The proposed NGWF must allow the administrator(s) to review any policy impact for new or modified application signatures included in a content release version. This Web GUI feature will enable the administrator(s) to simultaneously update the security policies and install new content and allows for a seamless shift in policy enforcement.	
	2.1.13.6 The proposed NGWF must be able to block source IP addresses performing DoS attacks on the hardware INGRESS level even before consuming any CPU or packet buffer resource without any user configuration.	
	2.1.13.7 The proposed NGWF must have a policy optimizer which is able filter rules who are used or unused in specific time frames such as 30 days, 90 days, etc., with an external management device.	
	2.1.13.8 The proposed NGWF must be able to decrypt, inspect and control both inbound and outbound SSL and SSH connections to prevent unwanted activities or malicious content on the same proposed hardware, also serve as the decryption broker to other security devices.	
	2.1.13.9 The proposed NGWF must have the capability to define a Threshold to indicate the minimum number of hours after an update becomes available before the firewall will download it regardless of the schedule.	

	2.1.13.10 The proposed NGWF must include individual user activity report showing applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period without additional software and hardware modules.	
	2.1.14 Must have the following threat protection capabilities:	
	2.1.14.1 The proposed NGWF must have protection against the most recent and relevant malware with payload signatures, not hash, to block known and future variants of malware, and receive the latest security updates.	
	2.1.14.2 The proposed NGWF must support a protocol decoder-based analysis that stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits.	
	2.1.14.3 The proposed NGWF must have integrated IPS, anti-spyware, anti-malware, and C2 prevention capabilities.	
	2.1.14.4 The proposed NGWF must deliver inline machine learning (ML) at the network level and should block unknown threats in real time instead of waiting for a sandbox- integrated directly on the NGFW.	
	2.1.14.5 The proposed NGWF must support inline cloud analysis that detects command and SQL injection vulnerabilities in real time to protect users against zero-day threats.	
	2.1.14.6 The proposed NGWF must support local deep learning which complements cloud-based inline cloud analysis component of the solution.	
	2.1.15 Must have the following sandboxing capabilities:	
	2.1.15.1 The proposed NGWF must completely eliminate the need for standalone IPS or IDS solutions.	
	2.1.15.2 The proposed NGWF must prevent highly evasive malware via stealthy observation to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.	
	2.1.15.3 The proposed NGWF must support uncovering malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis to prevent malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing.	
	2.1.15.4 The proposed NGWF must support an intelligent runtime memory analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed.	
	2.1.15.5 The proposed NGWF must operate a series of inline cloud ML-based detection engines to analyze PE samples traversing through your network to detect and prevent unknown malware in real-time.	
	2.1.15.6 The proposed NGWF must hold files from downloading (and potentially spreading within your network) while analyzing these suspicious files for malware in the cloud, in a real-time exchange.	

	2.1.15.7 The proposed NGWF must operates using a lightweight forwarding mechanism on the firewall to minimize any local performance impact; and to keep up with the latest changes in the threat landscape, cloud inline ML detection models are added and updated seamlessly in the cloud, without requiring content updates or feature release support.	
	2.1.15.8 The proposed NGWF must support analysis of email links by extracting HTTP/HTTPS contained in SMTP and POP3 email messages.	
	2.1.16 Must have the following URL filtering capabilities:	
	2.1.16.1 The proposed NGWF must protect the GCG network and its users against malicious and evasive web-based threats—both known and unknown.	
	2.1.16.2 The proposed NGWF must support inline real time web threat prevention by using cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).	
	2.1.16.3 The proposed NGWF must support phishing image detection with ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.	
	2.1.16.4 The proposed NGWF must support translation site filtering that applies advanced URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.	
	2.1.16.5 The proposed NGWF must inspect for phishing and malicious JavaScript using local inline categorization, a firewall-based analysis solution, which can block unknown malicious web pages in real-time.	
	2.1.17 Must have the following DNS security capabilities:	
	2.1.17.1 The proposed NGFW must stop known and unknown DNS traffic with machine learning and predictive analytics.	
	2.1.17.2 The proposed NGFW must help identify systems that are infected/ compromised by sinkholing DNS request to a C2 server.	
	2.1.17.3 The proposed NGFW must protect against DGA based attacks which generate random domains on the fly for malware to use as a way to call back to a C2 server.	
	2.1.17.4 The proposed NGFW must protect against DNS tunneling based attacks that utilize crafted DNS queries and response to hide malware delivery, command-and control traffic or data exfiltration/extraction.	
	2.1.17.5 The proposed NGFW must protect against ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.	
	2.1.17.6 The proposed NGFW must protect against strategically aged domains using predictive analytics. It must protect	

		users from connecting to domains that were reserved and left dormant for months before use by malicious actors.	
	2.1.17.7	The proposed NGFW must prevent fast flux, technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.	
	2.1.17.8	The proposed NGFW must protect against domains surreptitiously added to hacked DNS zones of reputable domains.	
	2.1.17.9	The proposed NGFW must prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.	
	2.1.17.10	The proposed NGFW must prevent dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.	
	2.1.17.11	The proposed NGFW must support the following DNS security categories: C2, DDNS, malware, newly registered domains, phishing, grayware, parked, and proxy avoidance & anonymizers.	
	2.1.18	Must have the following SDWAN capabilities:	
	2.1.18.1	The proposed NGFW must be integrated into the operating system of the next generation secure-SDWAN.	
	2.1.18.2	The proposed NGFW must support dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss.	
	2.1.18.3	The proposed NGFW must support security features, such as user and application identification/control, to provide complete traffic and security control.	
	2.1.18.4	The proposed NGFW must support link bundling of different ISP.	
	2.1.18.5	The proposed NGFW must support path quality profile for each set of business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage.	
	2.1.18.6	The proposed NGFW must support the following types of WAN connections that terminates as ethernet to the device's interface: ADSL/DSL, cable modem, ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, Wi-Fi, and anything that terminates as ethernet to the device's interface.	
	2.1.18.7	The proposed NGFW must be able to monitor business-critical SaaS application to monitor the latency, jitter, and packet loss and able to swap from available WAN links to ensure application usability.	
	2.1.18.8	The proposed NGFW must support forward error correction.	

	2.1.18.9 The proposed NGFW must support packet duplication.	
	2.1.18.10 The proposed NGFW must have SD-WAN traffic distribution profiles, such as: Best Available Path, Top-Down Priority, and Weighted Session Distribution.	
	2.1.18.11 The proposed NGFW must have DIA SD-WAN.	
	2.1.18.12 The proposed NGFW must support Hub-and-Spoke topology.	
	2.1.18.13 The proposed NGFW must support Full Mesh VPN topology.	
	2.1.18.14 The proposed NGFW must support Full Mesh VPN Cluster with DDNS Service.	
	2.1.18.15 The proposed NGFW must be managed in the central management console.	
	2.1.18.16 The proposed NGFW must have a dashboard for visibility into your SD-WAN links and performance so that the administrator can adjust the path quality thresholds and other aspects of SD-WAN to improve its performance.	
	2.1.18.17 The proposed NGFW must have centralized statistics and reporting including application and link performance statistics, path health measurements and trend analysis, and focused views of application and link issues.	
	2.1.19 Must have the following remote client / user VPN capabilities:	
	2.1.19.1 The proposed NGFW must provide management functions for VPN infrastructure.	
	2.1.19.2 The proposed NGFW must provide security enforcement for traffic from VPN applications.	
	2.1.19.3 The proposed NGFW must provide application software that runs on endpoints and enables access to the GCG network resources through the VPN portals and gateways.	
	2.1.19.4 The proposed NGFW must perform host information profile checking to enforce security posture on endpoints.	
	2.1.19.5 The proposed NGFW must support identification of managed devices using the endpoint serial number on gateways.	
	2.1.19.6 The proposed NGFW must support mobile applications for endpoints running iOS, Android, Chrome OS, and Windows 10.	
	2.1.19.7 The proposed NGFW must support endpoints running Linux aside from Windows and MacOS.	
	2.1.19.8 The proposed NGFW must support split tunneling based on destination domain, client process, and video streaming application.	
	2.1.19.9 The proposed NGFW must support adding a compromised device to the quarantine list.	
	2.1.19.10 The proposed NGFW must provide 200 maximum SSL VPN tunnels.	
	2.1.19.11 The proposed NGFW must provide 1500 maximum tunnels for client VPN (SSL, IPSec, and IKE with XAUTH).	

	2.1.19.12 The proposed NGFW must provide secure remote access or VPN solution via single or multiple internal/external gateways.	
	2.1.19.13 The proposed NGFW must provide authentication via LDAP, SAML, Kerberos, RADIUS or TACACS.	
2.2 WIDE AREA NETWORK (WAN) SWITCH		
	2.2.1 The bidder must provide one (1) unit of WAN Switch (WANS) with complete accessories and satisfy the minimum requirements and specifications below.	
	2.2.2 Must have enterprise-class Layer 2 connectivity with support for ACLs, robust QoS and routing.	
	2.2.3 Must be a 1U rack mountable switch with full density 24 x 10/100/1000Base-T ports and 4 x 1G/10G SFP ports.	
	2.2.4 Must have built-in high speed 1/10GbE uplinks.	
	2.2.5 Must be a software defined ready with REST APIs.	
	2.2.6 Must have simple deployment with zero touch provisioning.	
	2.2.7 Must simplify add, move, and change with colorless ports.	
	2.2.8 Must have three (3) years warranty, support, and subscriptions.	
	2.2.9 Must have intelligent monitoring, visibility, and remediation with analytics engine.	
	2.2.10 Must be manageable via single pane of glass across wired, wireless, and WAN.	
	2.2.11 Must support automated configuration and verification.	
	2.2.12 Must enable secure and simple access for users and Internet of Things (IoT).	
	2.2.13 Must have the following QoS requirements:	
	2.2.13.1 The proposed WANS must support SP queuing.	
	2.2.13.2 The proposed WANS must have traffic prioritization (IEEE 802.1p) for real-time classification.	
	2.2.13.3 The proposed WANS have Class of Service (CoS) that sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and differentiated service.	
	2.2.13.4 The proposed WANS must have rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.	
	2.2.13.5 The proposed WANS must have large buffers for graceful congestion management.	
	2.2.14 Must have the following Resiliency and High Availability requirements:	
	2.2.14.1 The proposed WANS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
	2.2.14.2 The proposed WANS must support IEEE 802.3ad LACP that supports up to 8 LAGs, each with up to 8 links per LAG;	

	and provides support for static or dynamic groups and a user-selectable hashing algorithm.	
	2.2.14.3 The proposed WANS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
	2.2.14.4 The proposed WANS must have smart link that provides easy-to-configure link redundancy of active and standby links.	
	2.2.15 Must have the following Performance and Connectivity requirements:	
	2.2.15.1 The proposed WANS must have up to 128 Gbps in non-blocking bandwidth and up to 95.2 Mpps for forwarding.	
	2.2.15.2 The proposed WANS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.	
	2.2.15.3 The proposed WANS must have 24x ports 10/100/1000Base-T ports and 4x 1G/10G SFP ports.	
	2.2.15.4 The proposed WANS must have the following management interface options: 2.2.15.4.1 one (1) x USB-C console port. 2.2.15.4.2 one (1) x USB Type A host port.	
	2.2.15.5 The proposed WANS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
	2.2.15.6 The proposed WANS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
	2.2.16 Must have the following Management requirements:	
	2.2.16.1 The proposed WANS must have a built-in programmable and easy-to-use REST API interface.	
	2.2.16.2 The proposed WANS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	
	2.2.16.3 The proposed WANS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
	2.2.16.4 The proposed WANS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
	2.2.16.5 The proposed WANS must support SNMP v2c/v3 that provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.	

	2.2.16.6 The proposed WANS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group.	
	2.2.16.7 The proposed WANS must support TFTP and SFTP that offer different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.	
	2.2.16.8 The proposed WANS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	
	2.2.16.9 The proposed WANS must support IEEE 802.1AB LLDP that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
	2.2.16.10 The proposed WANS must support dual flash images that provide independent primary and secondary operating system files for backup while upgrading.	
	2.2.16.11 The proposed WANS must assign descriptive names to ports for easy identification.	
	2.2.16.12 The proposed WANS multiple configuration files can be stored to a flash image.	
	2.2.16.13 The proposed WANS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
	2.2.17 Must have the following Layer 2 Switching requirements:	
	2.2.17.1 The proposed WANS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously.	
	2.2.17.2 The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,220 bytes.	
	2.2.17.3 The proposed WANS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
	2.2.17.4 The proposed WANS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.	
	2.2.17.5 The proposed WANS must support MVRP that allows automatic learning and dynamic assignment of VLANs.	
	2.2.17.6 The proposed WANS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.	
	2.2.17.7 The proposed WANS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.	

	2.2.17.8 The proposed WANS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
	2.2.18 Must have the following Layer 3 Services and Routing requirements:	
	2.2.18.1 The proposed WANS must support ARP determines the MAC address of another IP host in the same subnet; supports static ARPs.	
	2.2.18.2 The proposed WANS must support DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
	2.2.18.3 The proposed WANS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.	
	2.2.18.4 The proposed WANS must support Dynamic Host Configuration Protocol (DHCP) that simplifies the management of large IP networks and supports client; DHCPv4 Relay support enables DHCP operation across subnets.	
	2.2.18.5 The proposed WANS must have static IP routing that provides manually configured routing.	
	2.2.18.6 The proposed WANS must have dual stack static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routing. Dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.	
	2.2.19 Must have the following Security requirements:	
	2.2.19.1 The proposed WANS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
	2.2.19.2 The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
	2.2.19.3 The proposed WANS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
	2.2.19.4 The proposed WANS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.	
	2.2.19.5 The proposed WANS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	

	2.2.19.6 The proposed WANS must support MAC-based client authentication.	
	2.2.19.7 The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
	2.2.19.8 The proposed WANS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.	
	2.2.19.9 The proposed WANS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	
	2.2.19.10 The proposed WANS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	
	2.2.19.11 The proposed WANS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.	
	2.2.19.12 The proposed WANS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
	2.2.19.13 The proposed WANS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	
	2.2.20 Must have the following Multicast requirements:	
	2.2.20.1 The proposed WANS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
	2.2.20.2 The proposed WANS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
	2.2.20.3 The proposed WANS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
2.3 CORE SWITCHES		
	2.3.1 The bidder must provide two (2) units of Core Switch (CS) with complete accessories and satisfy the minimum requirements and specifications below.	
	2.3.2 Must be a stackable Layer 3 switch with BGP, EVPN, VXLAN, VRF, and OSPF with robust security and QoS.	
	2.3.3 Must have at least 448 Gbps system switching capacity, 334 Mpps system throughput, and up to 200 Gbps stacking bandwidth.	
	2.3.4 Must be a 1U rack mountable switch with full density 24 x 10/100/1000Base-T ports and 4 x 1G/10G/25G/50G SFP ports.	
	2.3.5 Must have power-to-port switch bundle with back-to-front air flow, ideal for data center 1GbE top-of-rack (ToR) and out-of-band management (OOBM) deployments.	

	2.3.6 Must have built-in high speed 10GbE/25GbE/50GbE uplinks.	
	2.3.7 Must have three (3) years warranty, support, and subscriptions.	
	2.3.8 Must have intelligent monitoring, visibility, and remediation with analytics engine.	
	2.3.9 Must be manageable via single pane of glass across wired, wireless, and WAN.	
	2.3.10 Must support automated configuration and verification.	
	2.3.11 Must enable secure and simple access for users and Internet of Things (IoT).	
	2.3.12 Must have the following QoS requirements:	
	2.3.12.1 The proposed CS must support SP queuing and DWRR.	
	2.3.12.2 The proposed CS must have traffic prioritization (IEEE 802.1p) for real-time classification into 8 priority levels that are mapped to 8 queues.	
	2.3.12.3 The proposed CS transmission rates of egressing frames can be limited on a per-queue basis using EQS.	
	2.3.13 Must have the following Resiliency and High Availability requirements:	
	2.3.13.1 The proposed CS must have high performance front plane stacking for up to 10 switches.	
	2.3.13.2 The proposed CS must have the flexibility to mix both modular and fixed models within a single stack.	
	2.3.13.3 The proposed CS must have hot swappable power supplies.	
	2.3.13.4 The proposed CS must provide N+1 and N+N redundancy for high reliability in the event of power line or supply failures.	
	2.3.13.5 The proposed CS must support VRRP that allows groups of two routers to dynamically back each other up to create highly available routed environments.	
	2.3.13.6 The proposed CS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
	2.3.13.7 The proposed CS must support IEEE 802.3ad LACP that supports up to 54 LAGs, each with eight links per group with a user-selectable hashing algorithm.	
	2.3.13.8 The proposed CS must support Microsoft NLB for server applications.	
	2.3.13.9 The proposed CS must support ERPS that provides rapid protection and recovery in a ring topology.	
	2.3.13.10 The proposed CS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
	2.3.14 Must have the following Performance and Connectivity requirements:	

	2.3.14.1 The proposed CS must have up to 448 Gbps in non-blocking bandwidth and up to 334 Mpps for forwarding.	
	2.3.14.2 The proposed CS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.	
	2.3.14.3 The proposed CS must have 24x ports 10/100/1000Base-T ports and 4x 1G/10G/25G/50G SFP ports.	
	2.3.14.4 The proposed CS must have the following management interface options: 2.3.14.4.1 one (1) x USB-C console port. 2.3.14.4.2 one (1) x OOBM port. 2.3.14.4.3 one (1) x USB Type A host port.	
	2.3.14.5 The proposed CS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
	2.3.14.6 The proposed CS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
	2.3.14.7 The proposed CS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.	
	2.3.15 Must have the following Management requirements:	
	2.3.15.1 The proposed CS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	
	2.3.15.2 The proposed CS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.	
	2.3.15.3 The proposed CS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
	2.3.15.4 The proposed CS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
	2.3.15.5 The proposed CS must support SNMP v2c/v3 which provides SNMP read and trap support of industry standard MIB, and private extensions.	
	2.3.15.6 The proposed CS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	

	2.3.15.7 The proposed CS must support TFTP and SFTP – offers different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over a Secure Shell (SSH) tunnel to provide additional security.	
	2.3.15.8 The proposed CS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time.	
	2.3.15.9 The proposed CS must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
	2.3.15.10 The proposed CS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.	
	2.3.15.11 The proposed CS must be able to assign descriptive names to ports for easy identification.	
	2.3.15.12 The proposed CS multiple configuration files can be stored to a flash image.	
	2.3.15.13 The proposed CS ingress and egress port monitoring must enable more efficient network problem solving.	
	2.3.15.14 The proposed CS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
	2.3.15.15 The proposed CS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for VoIP tests.	
	2.3.15.16 The proposed CS must support precision time protocol that allows precise clock synchronization across distributed network switches as defined in IEEE 1588.	
	2.3.16 Must have the following Layer 2 Switching requirements:	
	2.3.16.1 The proposed CS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).	
	2.3.16.2 The proposed CS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.	
	2.3.16.3 The proposed CS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.	
	2.3.16.4 The proposed CS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
	2.3.16.5 The proposed CS must support MVRP that allows automatic learning and dynamic assignment of VLANs.	
	2.3.16.6 The proposed CS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.	

	2.3.16.7 The proposed CS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
	2.3.16.8 The proposed CS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
	2.3.16.9 The proposed CS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.	
	2.3.16.10 The proposed CS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.	
	2.3.16.11 The proposed CS must have IPv4 Multicast in VXLAN/EVPN overlay support which allows PIMSM/IGMP snooping in the VXLAN overlay.	
	2.3.16.12 The proposed CS must have IPv6 VXLAN/EVPN overlay support which allows IPv6 traffic over the VXLAN overlay.	
	2.3.16.13 The proposed CS must have VXLAN ARP/ND suppression which allows minimization of ARP and ND traffic flooding within individual VXLAN segments, thus optimizing the VXLAN network.	
	2.3.17 Must have the following Layer 3 Services and Routing requirements:	
	2.3.17.1 The proposed CS must have ARP that determines the MAC address of another IP host in the same subnet; supports static ARPs.	
	2.3.17.2 The proposed CS must have a DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
	2.3.17.3 The proposed CS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per VLAN basis for added flexibility.	
	2.3.17.4 The proposed CS must have route maps that provide more control during route redistribution; allow filtering and altering of route metrics.	
	2.3.17.5 The proposed CS must have BGP-4 that delivers an implementation of the EGP utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks with graceful restart capability.	
	2.3.17.6 The proposed CS must have MP-BGP that enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6.	
	2.3.17.7 The proposed CS must have OSPF that delivers faster convergence; uses link-state routing IGP, which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery.	

	2.3.17.8 The proposed CS must have ECMP that enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.	
	2.3.17.9 The proposed CS must have static IP routing that provides manually configured routing; includes ECMP capability.	
	2.3.17.10 The proposed CS must have policy-based routing that uses a classifier to select traffic that can be forwarded based on policy set by the network administrator.	
	2.3.17.11 The proposed CS must have IP performance optimization that provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.	
	2.3.17.12 The proposed CS must have dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.	
	2.3.18 Must have the following Security requirements:	
	2.3.18.1 The proposed CS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
	2.3.18.2 The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
	2.3.18.3 The proposed CS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
	2.3.18.4 The proposed CS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.	
	2.3.18.5 The proposed CS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
	2.3.18.6 The proposed CS must support MAC-based client authentication.	
	2.3.18.7 The proposed CS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
	2.3.18.8 The proposed CS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.	
	2.3.18.9 The proposed CS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	

	2.3.18.10 The proposed CS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	
	2.3.18.11 The proposed CS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.	
	2.3.18.12 The proposed CS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
	2.3.18.13 The proposed CS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	
	2.3.19 Must have the following Multicast requirements:	
	2.3.19.1 The proposed CS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
	2.3.19.2 The proposed CS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
	2.3.19.3 The proposed CS must support PIM that defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM SM and DM for both IPv4 and IPv6.	
	2.3.19.4 The proposed CS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
2.4 LOCAL AREA NETWORK (LAN) ACCESS SWITCHES		
	2.4.1 The bidder must provide two (2) units of LAN Access Switch (LAS) with complete accessories and satisfy the minimum requirements and specifications below.	
	2.4.2 Must have enterprise-class connectivity with support for ACLs, robust QoS and common protocols such as static and Access OSPF routing.	
	2.4.3 Must have scalability with 8-member switch Virtual Switching Framework (VSF) stacking for up to 384 downlink ports.	
	2.4.4 Must have 36 x 10/100/1000Base-T Class 6 Power over Ethernet (PoE) ports, supporting up to 60W per port.	
	2.4.5 Must have 12 x smart rate 100M/1G/2.5G/5GBase-T Class 6 PoE ports supporting up to 60W per port.	
	2.4.6 Must have 4 x 100M/1G/10G SFP ports (2x LRM; 2x LRM/MACSec 256).	
	2.4.7 Must have supports to PoE Standards IEEE 802.3af, 802.3at, 802.3bt (up to 60W).	
	2.4.8 Must have three (3) years warranty, support, and subscriptions.	
	2.4.9 Must have intelligent monitoring, visibility, and remediation with analytics engine.	

	2.4.10 Must be manageable via single pane of glass across wired, wireless, and WAN.	
	2.4.11 Must support automated configuration and verification.	
	2.4.12 Must enable secure and simple access for users and Internet of Things (IoT).	
	2.4.13 Must have the following QoS requirements:	
	2.4.13.1 The proposed LANS must support SP queuing and DWRR.	
	2.4.13.2 The proposed LANS must have traffic prioritization (IEEE 802.1p) for real-time classification.	
	2.4.13.3 The proposed LANS transmission rates of egressing frames can be limited on a per-queue basis using EQS.	
	2.4.13.4 The proposed LANS must have rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums.	
	2.4.14 Must have the following Resiliency and High Availability requirements:	
	2.4.14.1 The proposed LANS must support UDLD that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.	
	2.4.14.2 The proposed LANS must support IEEE 802.3ad LACP that supports up to 32 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm.	
	2.4.14.3 The proposed LANS must support IEEE 802.1s Multiple Spanning Tree that provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w.	
	2.4.14.4 The proposed LANS must IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking support static and dynamic trunks where each trunk supports up to eight links (ports) per static trunk.	
	2.4.14.5 The proposed LANS must support the VRRP that allows groups of two routers to dynamically back each other up to create highly available routed environments.	
	2.4.14.6 The proposed LANS must have hot-patching support for standalone and VSF stacked switches.	
	2.4.15 Must have the following Performance and Connectivity requirements:	
	2.4.15.1 The proposed LANS must have up to 272 Gbps in non-blocking bandwidth and up to 202 Mpps for forwarding.	
	2.4.15.2 The proposed LANS must have selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications.	
	2.4.15.3 The proposed LANS must have 36 x ports 10/100/1000Base-T Class 6 Power over Ethernet (PoE) ports, supporting up to 60W per port.	

	2.4.15.4 The proposed LANS must have 12 x ports smart rate 100M/1G/2.5G/5GBase-T Class 6 PoE ports supporting up to 60W per port.	
	2.4.15.5 The proposed LANS must have 4x 100M/1G/10G SFP ports (2x LRM; 2x LRM/MACSec 256).	
	2.4.15.6 The proposed LANS must have supports to PoE Standards IEEE 802.3af, 802.3at, 802.3bt (up to 60W).	
	2.4.15.7 The proposed CS must have the following management interface options: 2.4.15.7.1 one (1) x RJ-45 console port. 2.4.15.7.2 one (1) x USB-C console port. 2.4.15.7.3 one (1) x OOBM port. 2.4.15.7.4 one (1) x USB Type A host port.	
	2.4.15.8 The proposed LANS must have jumbo frames that allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9,198 bytes.	
	2.4.15.9 The proposed LANS must have packet storm protection against broadcast and multicast storms with user-defined thresholds.	
	2.4.15.10 The proposed LANS must have smart link that enables simple, fast converging link redundancy, and load balancing with dual uplinks avoiding Spanning Tree complexities.	
	2.4.16 Must have the following Management requirements:	
	2.4.16.1 The proposed LANS must have built-in programmable and easy-to-use REST API interface.	
	2.4.16.2 The proposed LANS must have simple day zero provisioning.	
	2.4.16.3 The proposed LANS must have scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance; The network administrators can gather a variety of network statistics and information for capacity planning and real time network monitoring purposes.	
	2.4.16.4 The proposed LANS management interface must control, enable, or disable each of the following depending on security preferences, console port, or reset button.	
	2.4.16.5 The proposed LANS must have industry standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments.	
	2.4.16.6 The proposed LANS management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access.	
	2.4.16.7 The proposed LANS must support SNMP (v2c/v3) and a wide range of read, write, and trap capabilities for industry standard Management Information Base (MIB), private extensions, and common use cases, such as system, port, PoE and VLAN management.	

	2.4.16.8 The proposed LANS must support RMON with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, and sampled flow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	
	2.4.16.9 The proposed LANS must support TFTP and SFTP that offer different mechanisms for configuration updates; TFTP allows bidirectional transfers over a TCP/ IP network; SFTP runs over an SSH tunnel to provide additional security.	
	2.4.16.10 The proposed LANS must have debug and sampler utility that supports ping and traceroute for IPv4 and IPv6.	
	2.4.16.11 The proposed LANS must support NTP that synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network.	
	2.4.16.12 The proposed LANS must support IEEE 802.1AB LLDP that advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications.	
	2.4.16.13 The proposed LANS must support dual flash images that provides independent primary and secondary operating system files for backup while upgrading.	
	2.4.16.14 The proposed LANS ingress and egress port monitoring must enable more efficient network problem solving.	
	2.4.16.15 The proposed LANS must support UDLD that monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices.	
	2.4.16.16 The proposed LANS must support IP SLA for Voice that monitors the quality of voice traffic using the UDP jitter and UDP jitter for VoIP tests.	
	2.4.17 Must have the following Layer 2 Switching requirements:	
	2.4.17.1 The proposed LANS must have VLAN support and tagging for IEEE 802.1Q (4,094 VLAN IDs).	
	2.4.17.2 The proposed LANS must have jumbo packet support that improves the performance of large data transfers; supports frame size of up to 9,198 bytes.	
	2.4.17.3 The proposed LANS must support IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs.	
	2.4.17.4 The proposed LANS must support RPVST+ that allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.	
	2.4.17.5 The proposed LANS must support MVRP that allows automatic learning and dynamic assignment of VLANs.	
	2.4.17.6 The proposed LANS must support VXLAN encapsulation protocol for overlay network that enables a more scalable virtual network deployment.	

	2.4.17.7	The proposed LANS must support BPDU tunnelling that transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs.	
	2.4.17.8	The proposed LANS must support port mirroring that duplicates port traffic (ingress and egress) to a monitoring port; supports four (4) mirroring groups.	
	2.4.17.9	The proposed LANS must have STP supports standard IEEE 802.1D STP, IEEE 802.1w RSTP for faster convergence, and IEEE 802.1s MSTP.	
	2.4.17.10	The proposed LANS must support IGMP that controls and manages the flooding of multicast packets in a Layer 2 network.	
	2.4.18	Must have the following Layer 3 Services and Routing requirements:	
	2.4.18.1	The proposed LANS must have a loopback interface address defines an address in OSPF, improving diagnostic capability.	
	2.4.18.2	The proposed LANS must support ARP determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network.	
	2.4.18.3	The proposed LANS must support DNS that provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server.	
	2.4.18.4	The proposed LANS must support internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.	
	2.4.18.5	The proposed LANS must support RIPv2 that provides an easy to configure routing protocol for small networks as while RIPng provides support for small IPv6 networks	
	2.4.18.6	The proposed LANS must support OSPF that delivers faster convergence; uses link-state routing IGP, which supports NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery.	
	2.4.18.7	The proposed LANS must have static IP routing that provides manually configured routing.	
	2.4.18.8	The proposed LANS must have IP performance optimization that provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities.	
	2.4.18.9	The proposed LANS must have dual IP stack that maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.	
	2.4.18.10	The proposed LANS must have Multicast Domain Name System Gateway that enables discovery vof mDNS groups across L3 boundaries	

	2.4.18.11 The proposed LANS must support Equal-Cost Multipath (ECMP) that enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth.	
	2.4.19 Must have the following Security requirements:	
	2.4.19.1 The proposed LANS must have ACL support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header.	
	2.4.19.2 The ACLs must also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis.	
	2.4.19.3 The proposed LANS must have management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services.	
	2.4.19.4 The proposed LANS must support CoPP which sets rate limit on control protocols to protect CPU overload from DOS attacks.	
	2.4.19.5 The proposed LANS must have support for multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards.	
	2.4.19.6 The proposed LANS must support MAC-based client authentication.	
	2.4.19.7 The proposed LANS must have secure management access that delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3.	
	2.4.19.8 The proposed LANS must have switch CPU protection that provides automatic protection against malicious network traffic trying to shut down the switch.	
	2.4.19.9 The proposed LANS must have ICMP throttling that defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.	
	2.4.19.10 The proposed LANS must have port security that allows access only to specified MAC addresses, which can be learned or specified by the network administrator.	
	2.4.19.11 The proposed LANS must have MAC address lockout that prevents configured MAC addresses from connecting to the network.	
	2.4.19.12 The proposed LANS SSL must encrypt all HTTP traffic, allowing secure access to the browser-based management GUI in the switch.	
	2.4.19.13 The proposed LANS must have MAC pinning that allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected.	

	2.4.20 Must have the following Multicast requirements:	
	2.4.20.1 The proposed LANS must support IGMP Snooping that allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.	
	2.4.20.2 The proposed LANS must support MLD that enables discovery of IPv6 multicast listeners; support MLD v1 and v2.	
	2.4.20.3 The proposed LANS must support PIM that defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM SM and DM for both IPv4 and IPv6.	
	2.4.20.4 The proposed LANS must support IGMP that utilizes ASM to manage IPv4 multicast networks; supports IGMPv1, v2, and v3.	
2.5 WIRELESS ACCESS POINTS		
2.5.1 WIRELESS ACCESS POINTS FOR WORKFORCE AREA		
	2.5.1.1 The bidder must provide five (5) units of Wireless Access Point (AP) for the Workforce Area with complete accessories and satisfy the minimum requirements and specifications below.	
	2.5.1.2 Must be an indoor AP type with dual radio, 5GHz 802.11ax 4x4 Multiple Input, Multiple Output (MIMO) and 2.4GHz 802.11ax 2x2 MIMO.	
	2.5.1.3 For 5GHz radio: 2.5.1.3.1 Four (4) spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate to individual 4SS HE160.	
	2.5.1.3.2 802.11ax client devices (max): Two (2) spatial stream Single User (SU) MIMO for up to 1.2Gbps wireless data rate to individual 2SS HE80.	
	2.5.1.3.3 802.11ax client devices (typical): Four (4) spatial stream Multi User (MU) MIMO for up to 4.8Gbps wireless data rate to up to four 1SS or two 2SS HE160 802.11ax DL-MU-MIMO capable client devices simultaneously (max); Four (4) spatial stream MU MIMO for up to 2.4Gbps wireless data rate to up to four 1SS or two 2SS HE80 802.11ax DL-MU-MIMO capable client devices simultaneously (typical).	
	2.5.1.4 For 2.4GHz radio: 2.5.1.4.1 Two (2) spatial stream SU MIMO for up to 574Mbps wireless data rate to 2SS HE40 802.11ax client devices (max).	
	2.5.1.4.2 Two spatial stream Single User (SU) MIMO for up to 287Mbps wireless data rate to 2SS HE20 802.11ax client devices (typical).	
	2.5.1.5 Must have three (3) years warranty, support, and subscriptions.	

	2.5.1.6 Must support at least up to 512 associated client devices per radio, and up to 16 Basic Service Set Identifier (BSSID)s per radio.	
	2.5.1.7 Must support the dynamic frequency selection (DFS) which optimizes the use of available radio frequency (RF) spectrum including Zero-Wait DFS (ZWDFS) to accelerate channel change.	
	2.5.1.8 Must support the following radio technologies: 2.5.1.8.1 802.11b: Direct-sequence spread-spectrum (DSSS).	
	2.5.1.8.2 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM).	
	2.5.1.8.3 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to thirty-seven (37) resource units (for an 80MHz channel).	
	2.5.1.9 Must support the following modulation types: 2.5.1.9.1 802.11b: BPSK, QPSK, CCK.	
	2.5.1.9.2 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.	
	2.5.1.9.3 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.	
	2.5.1.9.4 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.	
	2.5.1.10 Must support 802.11n high-throughput support: HT20/40.	
	2.5.1.11 Must support 802.11ac very high throughput support: VHT20/40/80/160.	
	2.5.1.12 Must support 802.11ax high efficiency support: HE20/40/80/160.	
	2.5.1.13 Must support 802.11n/ac packet aggregation: A-MPDU, A-MSDU.	
	2.5.1.14 Must have transmit power that is configurable in increments of 0.5 dBm.	
	2.5.1.15 Must support the following maximum transmit power: 2.5.1.15.1 2.4 GHz band: +24 dBm (18dBm per chain). 2.5.1.15.2 5 GHz band: +24 dBm (18 dBm per chain).	
	2.5.1.16 Must have four integrated dual-band down tilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 3.5dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The down tilt angle for maximum gain is roughly 30 degrees. Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 1.9dBi in 2.4GHz and 3.5dBi in 5GHz.	
	2.5.1.17 Must have at least two (2) multi-gigabit ports: 2.5.1.17.1 Port 1 2.5.1.17.1.1 Must be smart rate port with maximum negotiated speed of 2.5Gbps. 2.5.1.17.1.2 Must be auto-sensing link speed (100/1000/2500/5000BASE-T) and MDI/MDX.	

	2.5.1.17.1.3 Must be 2.5Gbps speeds that comply with NBase-T and 802.3bz specifications. 2.5.1.17.1.4 Must be 48Vdc (nominal) 802.3at/bt POE-PD (class 3 or higher). 2.5.1.17.1.5 Must be 802.3az Energy Efficient Ethernet (EEE).	
	2.5.1.17.2 Port 2 2.5.1.17.2.1 Must be 10/100/1000BASE-T Ethernet network interface (RJ-45). 2.5.1.17.2.2 Must be auto-sensing link speed and MDI/MDX. 2.5.1.17.2.3 Must be 802.3az Energy Efficient Ethernet (EEE).	
	2.5.1.18 Must have LACP support between both network ports for redundancy and increased capacity.	
	2.5.1.19 Must have DC power interface: 12Vdc (nominal, +/- 5%), accepts 2.1mm/5.5mm center-positive circular plug with 9.5mm length.	
	2.5.1.20 Must have USB 2.0 host interface (Type A connector).	
	2.5.1.21 Must support Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio (2.4GHz).	
	2.5.1.22 Must have visual indicators (two multi-color LEDs): for System and Radio status.	
	2.5.1.23 Must have reset button: factory reset, LED mode control (normal/off).	
	2.5.1.24 Must have serial console interface (micro-B USB physical jack).	
	2.5.1.25 Must have Kensington security slot.	
	2.5.1.26 Must have maximum power consumption: DC powered: 16.0W, PoE powered (802.3af, IPM enabled): 13.5W, PoE powered (802.3at/bt): 20.8W, and all numbers above are without an external USB device connected. When sourcing the full 5W power budget to such a device, the incremental power consumption for the AP is up to 5.7W (PoE powered) or 5.5W (DC powered).	
	2.5.1.27 Must have maximum power consumption in idle mode: 12.6W (POE) or 9.7W (DC).	
	2.5.1.28 Must have maximum power consumption in deep-sleep mode: 5.9W (POE) or 1.5W (DC).	
	2.5.1.29 Must have Mean Time Between Failure (MTBF): 560,000hrs (64yrs) at +25C operating temperature.	
	2.5.1.30 Must support up to 2.69 Gbps combined peak data rate.	
	2.5.1.31 Must support WPA3 and Enhanced Open security.	
	2.5.1.32 Must have Built-in Client Match technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices.	
	2.5.1.33 Must be IoT-ready Bluetooth 5 and Zigbee support.	
	2.5.1.34 Must have embedded ranging technology for accurate indoor location measurements.	
	2.5.1.35 Must be designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.	

	2.5.1.36	Must have maximum data rates of 2.4 Gbps in the 5 GHz band and 287 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.69 Gbps).	
	2.5.1.37	Must support Orthogonal Frequency Division Multiple Access (OFDMA), multi-user MIMO (MU-MIMO), and cellular optimization with up to 4 spatial streams (4SS) and 160MHz channel bandwidth (VHT160).	
	2.5.1.38	Must support downlink MU-MIMO (5GHz radio) to maximize the use of its MIMO radio capabilities by simultaneously exchanging data with multiple single or dual stream client devices.	
	2.5.1.39	Must have flexibility to operate as standalone access points or with a gateway for greater scalability, security, and manageability.	
	2.5.1.40	Must support Air Match that allows organizations to automate network optimization using machine learning.	
	2.5.1.41	Must come with built-in Bluetooth Low-Energy (BLE) and Zigbee radio that enables a wide range of IOT use cases, such as asset tracking and mobile engagement.	
	2.5.1.42	Must provide enhanced device assurance with Trusted Platform Module (TPM) for secure credential and key storage, and secure boot.	
	2.5.1.43	Must support Intelligent Power Monitoring (IPM) enabling the AP to continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
	2.5.1.44	Must have Advanced Cellular Coexistence (ACC) to minimize the impact of interference from cellular networks.	
	2.5.1.45	Must support Maximum Ratio Combining (MRC) for improved receiver performance.	
	2.5.1.46	Must support Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance.	
	2.5.1.47	Must support Space-time block coding (STBC) for increased range and improved reception.	
	2.5.1.48	Must support Low-Density Parity Check (LDPC) for high-efficiency error correction and increased throughput.	
	2.5.1.49	Must support Transmit Beam-Forming (TxBF) for increased signal reliability and range.	
	2.5.1.50	Must support 802.11ax Target Wait Time (TWT) to support low-power client devices.	
2.5.2 WIRELESS ACCESS POINTS FOR MEETING ROOMS			
	2.5.2.1	The bidder must provide two (2) units of Wireless Access Point (AP) for Meeting Rooms with complete accessories and satisfy the minimum requirements and specifications below.	
	2.5.2.2	Must be a mid-range dual radio Wi-Fi 6 hospitality AP with 1+2 Ethernet ports.	
	2.5.2.3	For 5GHz radio: two (2) SS SU-MIMO for up to 1.2Gbps wireless data rate (HE80).	

	2.5.2.4 For 2.4GHz radio: two (2) SS SU-MIMO for up to 287Mbps wireless data rate (HE20).	
	2.5.2.5 Must have three (3) years warranty, support, and subscriptions.	
	2.5.2.6 Must support up to 256 associated client devices per radio, and up to 16 BSSIDs per radio.	
	2.5.2.7 Must support the DFS which optimizes the use of available RF spectrum including Zero-Wait DFS (ZWDFS) to accelerate channel change.	
	2.5.2.8 Must support the following radio technologies: 2.5.2.8.1 802.11b: DSSS.	
	2.5.2.8.2 802.11a/g/n/ac: OFDM.	
	2.5.2.8.3 802.11ax: OFDMA with up to eight (8) resource units.	
	2.5.2.9 Must support the following modulation types: 2.5.2.9.1 802.11b: BPSK, QPSK, CCK.	
	2.5.2.9.2 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.	
	2.5.2.9.3 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.	
	2.5.2.9.4 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.	
	2.5.2.10 Must support 802.11n high-throughput support: HT20/40.	
	2.5.2.11 Must support 802.11ac very high throughput support: VHT20/40/80.	
	2.5.2.12 Must support 802.11ax high efficiency support: HE20/40/80.	
	2.5.2.13 Must support 802.11n/ac packet aggregation: A-MPDU, A-MSDU.	
	2.5.2.14 Must have transmit power that is configurable in increments of 0.5 dBm.	
	2.5.2.15 Must support the following maximum transmit power: 2.5.2.15.1 2.4 GHz band: +20 dBm (17 dBm per chain). 2.5.2.15.2 5 GHz band: +21 dBm (18 dBm per chain).	
	2.5.2.16 Two integrated semi-directional antennas for 2x2 MIMO with peak single antenna gain of 5.2dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for vertical wall or desk mounted orientation of the AP. Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 3.3dBi in 2.4GHz and 2.9dBi in 5GHz.	
	2.5.2.17 Must have two (2) multi-gigabit ethernet wired network ports. 2.5.2.17.1 auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDX. 2.5.2.17.2 802.3az Energy Efficient Ethernet (EEE). 2.5.2.17.3 PoE-PSE: 802.3af/at PoE output; dual 802.3af (both ports) or single 802.3at.	

	2.5.2.18	Must have DC power interface: 48Vdc (nominal, +/- 5%), accepts 1.35mm/3.5mm center-positive circular plug with 9.5mm length.	
	2.5.2.19	Must have USB 2.0 host interface (Type A connector).	
	2.5.2.20	Must support Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio (2.4GHz).	
	2.5.2.21	Must have visual indicators (two multi-color LEDs): for System and Radio status.	
	2.5.2.22	Must have reset button: factory reset, LED mode control (normal/off).	
	2.5.2.23	Must have serial console interface (micro-B USB physical jack).	
	2.5.2.24	Must have Kensington security slot.	
	2.5.2.25	Must have maximum power consumption: DC powered: 14W / 50W, PoE powered (802.3bt): 14W / 51W, PoE powered (802.3at): 14W / 25.5W, and PoE powered (802.3af): 13.5W / 13.5.	
	2.5.2.26	Must have maximum power consumption in idle mode (without USB or PSE): 6.2W (PoE).	
	2.5.2.27	Must have MTBF: 780khrs (88yrs) at +25C operating temperature.	
	2.5.2.28	Must have combine wireless and wired access in a single compact form factor.	
	2.5.2.29	Must provide high-performance connectivity for any organization experiencing growing mobile, cloud and IoT requirements with a wireless aggregate data rate of up to 1.5 Gbps and gigabit local wired ports.	
	2.5.2.30	Must support WPA3 and Enhanced Open security.	
	2.5.2.31	Must have Built-in Client Match technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices.	
	2.5.2.32	Must be IoT-ready Bluetooth 5 and Zigbee support.	
	2.5.2.33	Must be designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.	
	2.5.2.34	Must support OFDMA, MU-MIMO, and cellular optimization with up to 2 spatial streams (2SS) and 80MHz channel bandwidth.	
	2.5.2.35	Must have flexibility to operate as standalone access points or with a gateway for greater scalability, security, and manageability.	
	2.5.2.36	Must come with built-in BLE and Zigbee radio that enables a wide range of IOT use cases.	
	2.5.2.37	Must provide enhanced device assurance with TPM for secure credential and key storage, and secure boot.	
	2.5.2.38	Must support IPM enabling the AP to continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on	

		available PoE power – ideal when wired switches have exhausted their power budget.	
	2.5.2.39	Must have ACC to minimize the impact of interference from cellular networks.	
	2.5.2.40	Must support MRC for improved receiver performance.	
	2.5.2.41	Must support CDD/CSD for improved downlink RF performance.	
	2.5.2.42	Must support STBC for increased range and improved reception.	
	2.5.2.43	Must support LDPC for high-efficiency error correction and increased throughput.	
	2.5.2.44	Must support TxBF for increased signal reliability and range.	
	2.5.2.45	Must support 802.11ax TWT to support low-power client devices.	
2.6 CENTRAL MANAGEMENT SOLUTION FOR NETWORK EQUIPMENT			
	2.6.1	The bidder must provide one (1) lot cloud-based Central Management Solution for the proposed one (1) unit of WAN Switch (WANS), two (2) units of Core Switch (CS), two (2) units of LAN Access Switch, five (5) units of Wireless Access Point (AP) for the Workforce Area, and two (2) units of Wireless Access Point (AP) for Meeting Rooms with minimum requirements and specifications below.	
	2.6.2	Must be a similar platform with the existing Central Management Solution for the existing network devices of the GCG to ensure seamless integration and single-pane management of the new and existing equipment.	
	2.6.3	Must have three (3) years warranty, support, and subscriptions.	
	2.6.4	Must have unified management of wireless, wired, VPN, and SD-WAN for simplified operations.	
	2.6.5	Must have network fabric orchestration, intent-based policy engine, and access controls for unified policy management, automated network provisioning, and zero-trust security.	
	2.6.6	Must have Artificial Intelligence (AI)-based network insights for faster troubleshooting and continuous network optimization.	
	2.6.7	Must have client insights for inline client profiling and telemetry to close visibility gaps.	
	2.6.8	Must have live chat and an AI-based search engine for an enhanced support experience.	
	2.6.9	Must have APIs and webhooks to augment the value of other leading IT platforms in your environment.	
	2.6.10	Must have powerful monitoring and troubleshooting for remote or home office networks.	
	2.6.11	Must have integration with user experience insight to proactively monitor and improve the end-user experience.	
	2.6.12	Must have SaaS, on-premises, and Virtual Private Cloud managed service options for flexible consumption and financing.	

	2.6.13 Must have the following streamlined network operation requirements:	
	2.6.13.1 Provides a comprehensive single pane of glass dashboard for analyzing and improving wired and wireless LAN, and WAN performance at a global or site-level, eliminating the inefficiencies of using disjointed, domain-specific network management tools.	
	2.6.13.2 Provides a consistent operating model and a unified platform for efficient management of compute, storage, and networking infrastructure, while enhancing cost controls. Users can log in using Single Sign-On (SSO) and are granted role-based access (RBAC) based on permissions. An additional layer of security can also be enabled with Multi-Factor Authentication (MFA).	
	2.6.13.3 Supports setup wizard automatically adds account subscriptions, matches device inventory from orders, and assigns purchased licenses, improving accuracy, and saving time.	
	2.6.13.4 Additional visibility into key values of individual and stacked switches is provided. This includes port status, PoE consumption, VLAN assignment, device and neighbor connections, power status and trends, alerts and events and which troubleshooting actions can be performed.	
	2.6.13.5 Geographic availability, scalability, and resiliency as this platform is hosted across regions in multiple public clusters of AWS, Azure, and GCP, maintaining points of presence worldwide, and enabling GDPR compliance.	
	2.6.13.6 Supports accelerated device onboarding, configuration, and provisioning with flexible options of templates and UI groups for all supported network devices at the device, group and MSP levels.	
	2.6.13.7 Zero Touch Provisioning (ZTP) supports simple, intuitive workflow for setting up devices with no onsite IT involvement. Configuration parameters at a network or site-level can be defined.	
	2.6.13.8 Supports IP-based IoT devices that can be securely onboarded with Device Provisioning Protocol (DPP) via QR code, certified by Wi-Fi Alliance as "Easy Connect," enabling quick, compliant installations with built-in device validation.	
	2.6.14 Must have the following AI and advanced analytic requirements:	
	2.6.14.1 Supports Network Insights to automatically detect and diagnose network issues using dynamic baselines, with built-in anomaly detection for precise problem identification, root cause, and remediation with close to 95% accuracy.	
	2.6.14.2 Supports AI Search, a GenAI-powered, natural language search engine that provides quick and precise answers, configuration tips, troubleshooting advice and more.	
	2.6.14.3 Supports AI Assist that uses event-driven automation to collect diagnostics for critical failure signatures, for proactive customer support and replacement workflows.	

	2.6.14.4	Supports self-healing workflows can be enabled to automatically update configurations as needed, helping IT fix issues without manual intervention.	
	2.6.14.5	Supports Dynamic power save mode in which APs switch into a dynamic power save mode and automatically wake up at a schedule when connectivity demand arises, reducing power demands and saving money in alignment with the organization's sustainability initiatives.	
	2.6.14.6	Enhance wireless coverage and capacity using air match, built in AI/ML analyzes periodic RF data across the network to adjust AP settings dynamically based on changing conditions.	
	2.6.14.7	Enhance traditional radio and roaming techniques with client match, a patented RF optimization technology that continually enhances client connectivity and eliminates sticky clients.	
	2.6.15	Must have the following monitoring, reporting and troubleshooting capabilities:	
	2.6.15.1	Network and client health and assurance.	
	2.6.15.2	Application Health – Monitor app health, prioritize critical services by enforcing acceptable usage by site, device, or location. UCC analytics provides a unified view of VoIP app performance like Zoom, Slack, and Teams, including MOS scores and insights on RF performance and capacity concerns. Additionally, by using SaaS express the branch gateways dynamically identify the optimal path to reach high-priority SaaS applications.	
	2.6.15.3	AI-based Connectivity Insights – Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more. For wired networks, IT administrators gain visibility on port status, PoE consumption, VLAN assignments, device and neighbor connections, power status, etc.	
	2.6.15.4	Wi-Fi Planning and Monitoring – Enhance Wi-Fi design, implementation, and monitoring with easy-to-use floorplans that depict accurate coverage patterns without employing extra sensors.	
	2.6.15.5	Extend Operations to IoT – Unifies visibility of IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices in the physical environment along with IP based IoT devices.	
	2.6.15.6	Live Events – Issue occurrence time, device name, type, category, description, packet logs, rich command line tools are captured and diagnostic checks such as ping tests, traceroutes and device-level performance tests are performed to troubleshoot issues.	
	2.6.15.7	Comprehensive Reports – Offers an extensive set of reporting capabilities on device connectivity, network and application health, throughput, usage data, device inventory, activity auditing, capacity planning, including the ability to baseline and compare user experience across various sites in the network.	

	2.6.15.8	Live upgrades – Simple GUI-based workflows and rules governing firmware upgrades on deployed network devices are available. These upgrades are scheduled at a site level during non-peak hours, ensuring continuous operations and reduced maintenance windows.	
	2.6.15.9	Extensibility through APIs and Webhooks – Customers developing network automation frameworks can automatically pull data from this solution into third-party solutions enabling IT operators to programmatically trigger actions based on certain events or conditions.	
	2.6.16	Must have the following Automate Security at Scale requirements:	
	2.6.16.1	Network wizard that simplifies the creation of underlays for campus and data-center environments. Manual errors are eliminated as network topology is automatically identified and configured with minimal user inputs.	
	2.6.16.2	Fabric wizard that enables IT administrators to automatically generate logical overlays without complex CLI programming, pushing inherent policies universally across wired, wireless, and WAN infrastructure for campus and data center environments.	
	2.6.16.3	Policy manager that empowers IT to define and maintain global policies at scale with ease, using UI-driven, intuitive workflows that automatically translate security intent into policy design and map user roles for employees, contractors, guests, and devices to their proper access privileges.	
	2.6.16.4	Client insights that dynamically compares devices against crowdsourced fingerprints of known clients and applies MAC range classification for unknown devices. Through deep packet inspection, network devices are automatically categorized, accurate policies are enforced based on context and behavioral information.	
	2.6.16.5	Cloud Auth and cloud-native NAC that streamlines end-user authentication for wired and wireless networks. IT admins have the flexibility to select from various authentication methods such as – uploading approved client MAC addresses or authenticating users through integrations with popular cloud identity stores such as Google Workspace or Azure Active Directory and assigning the appropriate level of network access based on network profile.	
	2.6.16.6	Unique pre-shared passwords or passphrases that can be used to onboard user devices and non-user specific devices such as IP phones, cameras, thermostats etc., without prior device registration with Multi Pre-Shared Key (MPSK).	
	2.6.16.7	Users can leverage captive portal authorization methods for effortless network access.	
	2.6.16.8	Secure wireless segmentation – Multizone provides data separation for multi-tenancy, guest/visitor access, IoT devices, and other use cases. A single AP can connect to multiple gateways and tunnel traffic for isolation without	

	requiring extra access points or managing another wireless network.	
	2.6.16.9 Intrusion detection – Rogue AP Intrusion Detection Service (RAPIDS) detects and resolves rogue AP issues, correlating wired and wireless data to enhance security and incident response, with optional Risk Oriented Traffic Inspection.	
	2.6.16.10 Web content filtering – Rates websites by reputation and risk, empowering IT to block malicious sites, preventing phishing, DDoS, and other attacks.	
	2.6.16.11 The Bill of Materials (BOM) must include 3-year Foundational subscriptions on all proposed devices to enable all primary enterprise features such as monitoring, reporting, and troubleshooting, onboarding, provisioning, orchestration, AI and analytics, content filtering, guest access, UXI integration, and 24x7 TAC software support.	
3. BUDGET REQUIREMENTS		
	3.1 The budget for the procurement of One (1) Lot Supply, Delivery, Installation, Configuration, Implementation, Commissioning, and Support Services for the Establishment of Network Infrastructure for GCG Disaster Recovery Site and Extension Office - B is Nineteen Million Nine Hundred Thousand Pesos Only (₱19,900,000.00).	
4. BIDDER REQUIREMENTS		
	4.1 General Requirements 4.1.1 The bidder must provide the following documents during the post-qualification:	
	4.1.1.1 a certification issued by the product manufacturer that they are a certified partner and able to extend direct technical support to end-user for each product brand being offered; and	
	4.1.1.2 copy of company's latest General Information Sheet (GIS).	
	4.1.2 The bidder must have at least five (5) years of continuous existence and engagement in the IT business.	
	4.1.3 The bidder must have completed a similar contract for the supply, delivery, and installation of firewall and network devices for the past three (3) years from the date of submission and receipt of bids.	
	4.1.4 The bidder must be a Platinum PhilGEPS registered supplier.	
	4.1.5 Subcontractors are prohibited.	
	4.2 Manpower Requirements 4.2.1 During post-qualification period, the bidder must provide a list of locally based manpower for the supply, delivery, installation, configuration, and commissioning of the proposed establishment of network infrastructure for GCG Disaster Recovery Site and Extension Office - B, with each personnel being a regular employee of the bidder for at least three (3) years:	

	4.2.1.1 two (2) certified network professionals of the proposed network devices;	
	4.2.1.2 two (2) certified internetworks of the proposed network devices; and	
	4.2.1.3 two (2) certified accredited engineers of the proposed NGFW.	
	4.2.2 The bidder must provide a photocopy of valid certifications, resume, and company ID of the identified local manpower during post-qualification.	
	4.3 Prior to submission of bid, the prospective bidder is required to conduct an ocular inspection of the GCG Main and Extension Office - B. The purpose of this inspection is to allow the bidder to be familiarized with the conditions and requirements for the feasibility of the project.	
	4.3.1 The bidder must send an email request to the GCG at procurement@gcg.gov.ph at least a day prior to their proposed schedule of mandatory ocular inspection. The email must contain the company name and the names of bidder representatives (maximum of 2). This is to secure in advance the required gate pass and permit to enter the office building prior to the scheduled date of ocular inspection.	
	4.3.2 The bidder must obtain a Certificate of Appearance as proof of their attendance at the ocular inspection. The certificate shall be issued by the designated representative of the GCG present during the inspection.	
	4.3.3 The Certificate of Appearance must be included in the bidder's submission along with the bid documents. Bids submitted without the Certificate of Appearance will be considered as non-compliant.	
	4.3.4 The GCG reserves the right to verify the accuracy of the information provided in the Certificate of Appearance. Any falsification of attendance will result in disqualification and other appropriate actions.	
5. SCOPE OF WORK		
The Winning Bidder (hereafter referred to as simply the "bidder") must:		
	5.1 Perform the supply, delivery, installation, configuration, implementation, commission, and support services of the proposed network infrastructure for the GCG Disaster Recovery Site and GCG Extension Office - B at 8th Floor BDO Towers Paseo (formerly Citibank Center) 8741 Paseo de Roxas Makati City.	
	5.2 Cover all cables, structured cabling, civil works, licenses and/or subscriptions needed for the establishment of network infrastructure of the GCG Disaster Recovery Site, including, but not limited to the following:	
	5.2.1 install, configure, and implement the proposed two (2) units of WAN Switches with complete integration to its proposed cloud-based Central Management Solution;	
	5.2.2 install, configure, and implement the proposed two (2) units of Next Generation Firewalls with complete integration to its proposed two (2) units of WAN Switches, to the existing two (2) units of External Firewalls in the GCG Main Office (Palo	

	Alto 3220), and to the existing External Firewall Central Management Solution of the GCG;	
	5.2.3 install, configure, and implement the proposed two (2) units of Core Switches with complete integration to its proposed two (2) units of Next Generation Firewalls and to its proposed cloud-based Central Management Solution; and	
	5.2.4 install, integrate, and implement the existing GCG Hyperconverged Infrastructure System Solution for Disaster Recovery to its proposed Core Switches;	
	5.3 Cover all cables, structured cabling, civil works, licenses and/or subscriptions needed for the establishment of network infrastructure of the GCG Extension Office - B, including, but not limited to the following:	
	5.3.1 install, configure, and implement the proposed one (1) unit of WAN Switch with complete integration to its proposed cloud-based Central Management Solution;	
	5.3.2 install, configure, and implement the proposed two (2) units of Next Generation Firewalls with complete integration to its proposed one (1) unit of WAN Switch, to the existing two (2) units of External Firewalls in the GCG Main Office (Palo Alto 3220), and to the existing External Firewall Central Management Solution of the GCG;	
	5.3.3 install, configure, and implement the proposed two (2) units of Core Switches with complete integration to its proposed two (2) units of Next Generation Firewalls and to its proposed cloud-based Central Management Solution; and	
	5.3.4 install, configure, and implement the proposed two (2) units of LAN Access Switches with complete integration to its proposed two (2) units of Core Switches and to its proposed cloud-based Central Management Solution;	
	5.3.5 install, configure, and implement the proposed five (5) units of Wireless Access Points for the Workforce Area with complete integration to its proposed two (2) units of Core Switches and to its proposed cloud-based Central Management Solution;	
	5.3.6 install, configure, and implement the proposed two (2) units of Wireless Access Points for Meeting Rooms with complete integration to its proposed two (2) units of Core Switches and to its proposed cloud-based Central Management Solution; and	
	5.3.7 install the horizontal cabling distribution needed for the deployment of the new network equipment in the GCG Extension Office - B;	
	5.4 Deliver and pre-configure all equipment for the establishment of GCG Disaster Recovery Site at the GCG Office Main Office until such time that the new datacenter colocation becomes available.	
	5.5 Covers the transfer and re-deployment of the existing GCG Hyperconverged Infrastructure System Solution for Disaster Recovery from its current location (Luzon) to the new datacenter colocation site which will be located anywhere in Luzon.	
	5.6 Conduct Project Management using the below framework:	
	5.6.1 create a project team for the GCG and the bidder;	

	5.6.2 formulate project implementation plan;	
	5.6.3 conduct project kick-off;	
	5.6.4 implement and coordinate project milestones identified in the project implementation plan;	
	5.6.5 provide weekly/monthly/milestone project updates;	
	5.6.6 conduct hands-on technical training on the supplied equipment; and	
	5.6.7 provide and execute user acceptance and test plans.	
	5.7 Submit detailed project documentation in hard and soft copies:	
	5.7.1 Project Implementation Plan;	
	5.7.2 As built drawing;	
	5.7.3 Technical Reports;	
	5.7.4 UAT Test Plan;	
	5.7.5 Service Level Agreement; and	
	5.7.6 Warranty Agreement.	
6. TRAINING REQUIREMENTS		
	6.1 The bidder shall provide in-depth knowledge transfer on product installation, configuration, administration, maintenance, management, and operation of each proposed equipment for the establishment of network infrastructure for GCG Disaster Recovery Site and Extension Office - B to be conducted by a designated product expert.	
7. WARRANTY, MAINTENANCE, AND SUPPORT		
	7.1 The bidder must warrant that the Goods supplied are brand-new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the GCG provides otherwise.	
	7.2 The bidder must further warrant that all Goods supplied shall have no defect, arising from design, materials, or workmanship or from any act or omission of the bidder that may develop under normal use of the supplied Goods.	
	7.3 To ensure that manufacturing defects shall be corrected by the bidder, warranty, support services, and required subscriptions for all equipment and solutions shall be required from the bidder for a minimum period of three (3) years.	
	7.4 The GCG shall promptly notify the bidder in writing of any claims arising under this warranty. Upon receipt of such notice, the bidder shall, within the period specified and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the GCG.	
	7.5 If the bidder, having been notified, fails to remedy the defect(s) within the period specified, the GCG may proceed to take such remedial action as may be necessary, at the bidder's risk and expense and without prejudice to any other rights which the GCG may have against the bidder under the Contract and under the applicable laws.	

	7.6 In the event of any equipment failure, the bidder shall repair or automatically replace the defective products with the same product at no additional cost/charge to GCG.	
	7.7 A functional and workable service unit that is equivalent or higher in specification should be provided in case replacement of hardware would take more than twenty-four (24) hours or if repair requires pull out the equipment from GCG premises.	
	7.8 The bidder must provide a signed after sales service support certificate that the bidder will be supported by their principal in terms of parts and services.	
	7.9 The bidder must provide full-time support and managed services during the warranty period as specified:	
	7.9.1 single point of contact for all hardware and software components;	
	7.9.2 twenty-four hours by seven days (24x7) service desk support via telephone, email, or online chat portal;	
	7.9.3 at least one (1) hour response time upon receipt of issue escalation and four (4) hours for onsite support, if necessary;	
	7.9.4 if the problem was not resolved by service desk support, the bidder must provide an onsite technical support;	
	7.9.5 procedures on support and issue escalation; and	
	7.9.6 service report every after the onsite support.	
8. TERMS OF PAYMENT		
	8.1 Payments shall be made only upon deployment completion of each item and a certification by the Chairperson or Authorized Representative of the GCG to the effect that the goods delivered is in accordance with this Terms of Reference (TOR) and have been duly accepted. Except with the prior approval of the Chairperson of the GCG, no payment shall be made for supplies and materials not yet delivered under this TOR.	
	8.2 Provided further that payment shall be made within twenty (20) working days from the receipt of complete documents, i.e., billing statement / statement of account, and other pertinent documents from the bidder.	
	8.3 All payments made to the bidder will be subjected to a five percent (5%) reduction, to serve as retention money. The said amounts shall only be released after the lapse of the warranty period.	
9. CONFIDENTIALITY		
	9.1 Information or rights acquired and obtained from the GCG, including but not limited to any and all obligations prior to the termination or expiration hereof and provisions on confidentiality and proprietary rights, will remain in effect after termination of the services rendered to the GCG. Hence, the undertaking of the bidder not to disclose and to keep information confidential shall subsist even after the expiration or termination of its obligation to the GCG nor can the bidder, at any time, disclose items mentioned or enumerated in Section 9.2 or any information it acquires by virtue of the contract which the GCG deems confidential.	
	9.2 Records, documents, reports, and relevant data, such as diagrams, plans, designs, estimates, specifications, and other	

	supporting records of materials complied and prepared in the courses of the performance of the services shall be absolute properties of GCG and shall not be used by the bidder for purposes not related to this agreement without prior written approval of GCG. Copies of such documents as required in this TOR shall be turned over to GCG upon completion of the project except that the bidder shall have the right to retain a copy of the same.	
10. DELIVERY AND IMPLEMENTATION SCHEDULE		
	10.1 The delivery of goods, project implementation, documentation, and acceptance must be completed within ninety (90) calendar days from the receipt of the Notice to Proceed.	
	10.2 The bidder shall be subjected to evaluation by the end-user after the implementation of the project.	

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 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

SUBSCRIBED AND SWORN to me before me this _____, in _____, Philippines, with affiant exhibiting me his/her _____ issued on _____ at _____.

NOTARY PUBLIC
Doc No._____
Page No.____
Book No.____
Series of____

Omnibus Sworn Statement (Revised)
[shall be submitted with the Bid]

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

AFFIDAVIT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SUBSCRIBED AND SWORN to me before me this _____, in _____, Philippines, with affiant exhibiting me his/her _____ issued on _____ at _____.

NOTARY PUBLIC
Doc No._____
Page No.____
Book No.____
Series of____

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/deliver/perform] [description of the Goods]* in conformity with the said PBDs for the sum of *[total Bid amount in words and figures]* or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: *[specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties],* which are itemized herein or in the Price Schedules,

If our Bid is accepted, we undertake:

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

b. to provide 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 Amount and Purpose of
of agentCurrencyCommission 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: _____

Price Schedule for Goods Offered from Within the Philippines

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

For Goods Offered from Within the Philippines

Name of Bidder _____ Project ID No._____ Page ___of___

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of origin	Quantity	Unit price EXW per item	Transportation and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)
Establishment of Network Infrastructure for GCG Disaster Recovery Site									
1	External Firewall Appliance		2					3,500,000.00	7,000,000.00
2	WAN Switch		2					500,000.00	1,000,000.00
3	Core Switch		2					2,250,000.00	4,500,000.00
Establishment of Network Infrastructure for GCG Extension Office - B									
4	External Firewall Appliance		2					1,500,000.00	3,000,000.00
5	WAN Switch		1					500,000.00	500,000.00
6	Core Switch		2					1,000,000.00	2,000,000.00
7	LAN Switch		2					600,000.00	1,200,000.00
8	Wireless Access Point		7					100,000.00	700,000.00
								TOTAL	**19,900,000.00**

- **The bid proposal should not exceed the price ceiling for each component indicated under column 9.**

Name: _____

Legal Capacity: _____

Signature: _____

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


Republic of the Philippines
gppb
Government Procurement Policy Board