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 ANNUAL SUBSCRIPTION OF CYBER SECURITY STACK SOLUTION FOR THE GOVERNANCE COMMISSION FOR GOCCS (GCG)

Government of the Republic of the Philippines

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

# Preface

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

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

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

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

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

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

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

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

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

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

# Table of Contents

# *Glossary of Acronyms, Terms, and Abbreviations*

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

**BAC** – Bids and Awards Committee.

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

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

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

**BIR** – Bureau of Internal Revenue.

**BSP** – Bangko Sentral ng Pilipinas.

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

**CDA -** Cooperative Development Authority.

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

**CIF –** Cost Insurance and Freight.

**CIP –** Carriage and Insurance Paid.

**CPI –** Consumer Price Index.

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

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

**EXW** – Ex works.

**FCA** – “Free Carrier” shipping point.

**FOB** – “Free on Board” shipping point.

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

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

**GFI** – Government Financial Institution.

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

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

**GOP** – Government of the Philippines.

**GPPB** – Government Procurement Policy Board.

**INCOTERMS** – International Commercial Terms.

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

**LGUs –** Local Government Units.

**NFCC –** Net Financial Contracting Capacity.

**NGA –** National Government Agency.

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

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

**PSA –** Philippine Statistics Authority.

**SEC –** Securities and Exchange Commission.

**SLCC –** Single Largest Completed Contract.

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

**UN –** United Nations.

# *Section I. Invitation to Bid*

## Notes on the Invitation to Bid

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

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

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

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

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

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

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

# INVITATION TO BID FOR THE ONE (1) LOT ANNUAL SUBSCRIPTION OF CYBER SECURITY STACK SOLUTION FOR THE GOVERNANCE COMMISSION FOR GOCCS (GCG)

1. The Governance Commission for GOCCs (GCG), through the General Appropriations Act of 2024 (GAA 2024) intends to apply the sum of Two Million Six Hundred Fifty Thousand Pesos Only (₱2,650,000.00) being the ABC to payments under the contract for procurement One (1) Lot Annual Subscription of Cyber Security Stack Solution for the Governance Commission for GOCCs (GCG) (P.R. No. 24-0032). Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The GCG now invites bids for the above Procurement Project. The delivery, configuration, and deployment of the proposed cyber security stack solution must be completed within twenty (20) calendar days from the receipt of the Notice to Proceed. The bidder must have completed a similar contract for the supply and implementation of cyber security stack solution 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 27 May 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 ₱5,000.00. 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 05 June 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 24 June 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 24 June 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.

23 May 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 Annual Subscription of Cyber Security Stack Solution for the Governance Commission for GOCCs (GCG), with identification number P.R. No. 24-0032.

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

## 2. Funding Information

2.1. The GOP through the source of funding as indicated below for FY 2024 in the amount of Two Million Six Hundred Fifty Thousand Pesos Only (₱2,650,000.00).

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 00 May 2024 at 9:00 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.

## 15. Sealing and Marking of Bids

Each Bidder shall submit one (1) original and eight (8) 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.

[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.

## 16. Deadline for Submission of Bids

The Bidders shall submit on the specified date and time at 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:<br>a. Cyber Security Stack Solution.<br>b. completed within three (3) years prior to the deadline for the 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:<br>a. The amount of not less than ₱53,000.00 if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or<br>b. The amount of not less than ₱132,500.00 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.<br>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.<br>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 eight (8) 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. 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 –**<br>For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows:<br>For Goods supplied from abroad, the delivery terms applicable to the Contract are DDP delivered Makati City. In accordance with INCOTERMS.<br>For Goods supplied from within the Philippines, the delivery terms applicable to this Contract are delivered 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.<br>Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements).<br>For purposes of this Clause the Procuring Entity's Representative at the Project Site is Director Jaypee O. Abesamis.<br>**Incidental Services –**<br>The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements:<br>Training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.<br>The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.<br>**Transportation –**<br>Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.<br>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.<br>The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination.<br>**Intellectual Property Rights –**<br>The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.<br>**Regular and Recurring Services –**<br>The contract for regular and recurring services shall be subject to a renewal whereby the performance evaluation of the service provider shall be conducted in accordance with Section VII. Technical specifications. |
| 2.2 | The payment shall be made on a one-time basis after the deployment of the required license subscriptions.<br>Provided further that payment shall be made at least twenty (20) working days from receipt of complete documents such as billing statement/statement of account, and other pertinent documents.<br>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 ANNUAL SUBSCRIPTION OF CYBER SECURITY STACK SOLUTION FOR THE GOVERNANCE COMMISSION FOR GOCCS (GCG)

### 1. ENDPOINT AND EMAIL PROTECTION REQUIREMENTS

1.1 The bidder must provide two hundred fifty (250) annual license subscription of cloud-based endpoint and email protection at minimum specifications:

1.1.1 General Requirements:

1.1.1.1 Must have advanced threat protection strategies to eliminate vulnerabilities from user activities and endpoints.

1.1.1.2 Must have automatic detection and respond to a variety of threats including fileless attacks and ransomware.

1.1.1.3 Must have investigation capabilities, fast response for suspicious objects or activities, and centralized visibility of the entire network.

1.1.1.4 Must have machine learning and advanced detection techniques for broad protection against multiple threats (known or unknown).

1.1.1.5 Must have a filter for threats using efficient strategies to minimize attack vectors.

1.1.1.6 Must have noise cancellation techniques such as census and whitelist checking to reduce false positives.

1.1.1.7 Must have ability to clean infected files, perform rollback, and recover lost files.

1.1.1.8 Must have minimal impact to performance using efficient detection technique and low management costs.

1.1.1.9 Must have off-premises compliance and protection which enables the employees to work outside the organization’s network and still be covered by the organization’s security policies.

1.1.1.10 Must be able to co-exist with the existing third-party security solution within the GCG.

1.1.1.11 Must be able to support mass deployment through the network and must also support uninstallation of third-party agents.

1.1.1.12 Must have Extended Detection and Response (XDR) solution for both endpoint and email to facilitate detection and response functionalities, and directly integrate with the cloud-based XDR platform.

1.1.2 Anti-virus Requirements:

1.1.2.1 Must have pattern-based anti-malware.

1.1.2.2 Must have behavioral analytics against scripts, ransomware, injection, memory, and browser attacks.

1.1.2.3 Must have census check, variant protection, and file and web reputation.

1.1.2.4 Must have exploit protection.

1.1.2.5 Must have command-and-control (C&C) protection.

1.1.2.6 Must have ransomware protection.

1.1.2.7 Must have detection, response, and isolation functionality.

1.1.2.8 Must have device control functionality.

1.1.2.9 Must have threat intelligence sharing capability.

1.1.2.10 Must have cloud-based centralized management console for multiple product deployment that would allow easy management and extended visibility of the environment. The centralized management console must allow integration with the third-party Security Information and Event Management (SIEM) or Security Orchestration, Automation and Response (SOAR).

1.1.2.11 Must have user-based visibility to improve protection, reduce complexity, and eliminate redundant tasks related to security administration.

1.1.2.12 Must have customizable dashboard to allow different administrators to select which summary they would like to view at a glance.

1.1.2.13 Must have a Media Access Control (MAC) security solution to provide more regular anti-malware protection which includes device control and machine learning. The solution does not require a separate management console for MAC clients. Everything should be viewable and managed under a single pane of glass.

1.1.2.14 Must have an option to allow users to configure the security agent settings and an option to uninstall the MAC security solution agent if needed.

1.1.3 Vulnerability Protection Requirements:

1.1.3.1 Must be able to prevent emerging threats that could potentially compromise the GCG security regardless of the platform.

1.1.3.2 Must be able to perform virtual patching for vulnerable operating systems.

1.1.3.3 Must be integrated into a single security agent.

1.1.4 Application Control Requirements:

1.1.4.1 Must be capable of allowing or denying known or unknown applications, executables, and file types.

1.1.4.2 Must have a reliable file reputation source for cross checking of known good files. This source must be constantly kept up to date with the latest known good file listing.

1.1.4.3 Must have integration with other security solutions such as host intrusion prevention, data loss prevention, and mobile protection for better data correlation.

1.1.4.4 Must be able to perform an automated inventory scan which categorizes installed applications depending on its file reputation - known good to potentially dangerous

1.1.4.5 Must have application whitelisting or blacklisting feature.

1.1.5 Data Loss Prevention (DLP) Requirements:

1.1.5.1 Must have visibility and control over sensitive data and prevent data loss via USB flash drives, email, web, and cloud storage.

1.1.5.2 Must have built-in templates that comply with specified guidelines and regulations.

1.1.5.3 Must be able to support DLP enforcement of file encryption in Microsoft Office 365.

1.1.5.4 Must be able to detect and react to improper data usage-based keywords, regular expressions, and file attributes.

1.1.5.5 Must provide education to employees about corporate data usage policies through alerts, blocking or soft-blocking, and reporting.

1.1.5.6 Must have visibility and management over data at rest control points and should include scanning of endpoints, file servers, mail store, Microsoft SharePoint, and cloud storage.

1.1.5.7 Must have visibility and management over data in motion control points.

1.1.5.8 Must have visibility and management over data in use control points.

1.1.5.9 Must include a granular list of international identifiers.

1.1.6 Endpoint Encryption Requirements:

1.1.6.1 Must support both file encryption and full disk encryption.

1.1.6.2 Must have visibility and management of Apple FileVault encryption on keys to manage OSX based computers.

1.1.6.3 Must have visibility and management for Microsoft BitLocker encryption keys.

1.1.6.4 Must have support and leverage flexible hardware and software-based encryption across mixed environments.

1.1.7 Mobile Protection Requirements:

1.1.7.1 Must support smartphones and tablets running iOS or Android.

1.1.7.2 Must allow administrator to track, monitor, and manage mobile devices, applications, and data through a single console.

1.1.7.3 Must be able to protect corporate data with remote lock and wipe, and selective wipe.

1.1.7.4 Must have option for device enrollment through a web link, QR code, or iTunes download.

1.1.7.5 Must provide notification to administrator of jail broken or unencrypted devices.

1.1.7.6 Must allow administrator to manage and block specific types of applications based on categories.

1.1.7.7 Must be able to protect a mobile device from known bad websites that promote phishing, pharming, hacking, and the likes.

1.1.7.8 Must be able to scan mobile malware and allows to quarantine or delete detected files.

1.1.7.9 Must be able to perform remote wipe all data on a mobile device by sending a Short Message Service (SMS) text message.

1.1.7.10 Must have control filters to alert or block specific traffic.

1.1.7.11 Must prevent networking backdoors from attacking the network.

1.1.7.12 Must have application inventory and be able to control it per category.

1.1.8 Mail Protection Requirements:

1.1.8.1 Must have integration with Microsoft Office 365 email service.

1.1.8.2 Must have anti-virus, anti-spam, and anti-relay protection.

1.1.8.3 Must be able to quarantine emails upon virus detection.

1.1.8.4 Must have heuristic anti-spam protection.

1.1.8.5 Must be able to add policies based on custom preferences.

1.1.8.6 Must be able to block or allow customized subjects, based on keywords and the likes in any part of the email message.

1.1.8.7 Must be able to support multiple domains.

1.1.8.8 Must be able to protect against phishing websites.

1.1.8.9 Must be able to block or approve senders list.

1.1.8.10 Must have advanced detection and alert functionalities for early mitigation of emerging threats and targeted attacks.

1.1.8.11 Must detect unknown Uniform Resource Locators (URLs) embedded in email messages.

1.1.8.12 Must support protection against directory harvest attacks (DHA).

1.1.8.13 Must protect from malicious URLs embedded in email messages.

1.1.8.14 Must have anti-spoofing feature.

1.1.8.15 Must provide security for business email compromise (BEC).

1.1.8.16 Must be able to capture and analyze all incoming emails from internet to Microsoft Office 365 mailboxes.

1.1.8.17 Must be able to capture and analyze all outgoing emails from Microsoft Office 365 mailboxes to the internet.

1.1.8.18 Must be able to capture and analyze all Microsoft SharePoint and Microsoft OneDrive for business files.

1.1.8.19 Must be able to capture and analyze all Microsoft Office 365 internal email flows (from Microsoft Office 365 mailbox to Microsoft Office 365 mailbox).

1.1.8.20 Must have real-time scans to protect data in motion and manual scan for data at rest.

1.1.8.21 Must not impact or affect user email delivery or file sharing in case of service disruption or unavailability (pass-through).

1.1.8.22 Must be able to prevent the delivery of an identified suspicious or threated email and files.

1.1.8.23 Must be able to detect threats in emails without blocking the delivery to the recipient (pass-through).

1.1.8.24 Must support BEC that includes writing style DNA technology to scan the English email messages of a desired individual to learn their Writing Style and generate a Writing Style mode.

1.1.9 Web Protection Requirements:

1.1.9.1 Must have anti-virus and must be able to scan traffic going in and out the network in real-time.

1.1.9.2 Must have a URL database with multiple categories.

1.1.9.3 Must be able to protect HTTP, FTP, SMTP, POP3 protocols.

1.1.9.4 Must be able to create access policy by category, from URL database, customized list and by keyword.

1.1.9.5 Must block forbidden internet applications through a web browser.

1.1.9.6 Must be able to block access to malicious websites and restricted areas.

1.1.9.7 Must be able to support scan HTTP and HTTPs traffic for spyware and other web threats.

1.1.9.8 Must be able to support blocking of outbound data to known spyware and phishing-related websites.

1.1.9.9 Must be able to validate web-based codes to screen web pages for malicious codes.

1.1.9.10 Must be able to deploy policy based on users and/or groups defined in the active directory.

1.1.9.11 Must be able to generate web security violations per user, hostname, or IP address.

1.1.9.12 Must be able to generate reports on web violations statistics.

## 2. SERVER PROTECTION REQUIREMENTS

2.1 The bidder must provide fifty (50) annual license subscription of cloud-based server protection at minimum specifications:

2.1.1 General Requirements:

2.1.1.1 Must provide a single platform for complete server protection over physical servers, virtual servers, and virtual desktop computers in a single management console.

2.1.1.2 Must have layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications, and operating systems.

2.1.1.3 Must support web reputation for preventing access to malicious websites.

2.1.1.4 Must support Docker hosts and containers running on the Windows and Linux distribution.

2.1.1.5 Must have Extended Detection and Response (XDR) solution for server to facilitate detection and response functionalities, and directly integrate with the cloud-based XDR platform.

2.1.1.6 For unsupported operating systems, the bidder shall provide at least 500mbps of network detection and response capabilities. The GCG will provide the virtual machine requirements.

2.1.2 Management Console Requirements:

2.1.2.1 Must be a web-based management system for administrators.

2.1.2.2 Must have a dashboard for displaying multiple information and must be configurable by administrators to display information which is only required.

2.1.2.3 Must have alerts in the main menu to view administrator notifications concerning system or security events.

2.1.2.4 Must have Firewall Events to view activities on computers with the firewall enabled.

2.1.2.5 Must have Deep Packet Inspection (DPI) Events to view security-related DPI activities. This should display exploits detected, either resulting in dropped traffic or logging of events.

2.1.2.6 Must have System Events to view a summary of security-related events, primarily for the management server and including Agents' system events. All administrative actions should be audited within the System Events.

2.1.3 Anti-malware Requirements:

2.1.3.1 Must have web filtering to protect against malicious websites.

2.1.3.2 Must have prediction machine learning to protect against unknown malware.

2.1.3.3 Must have behavioral monitoring to protect against malicious scripts and applications.

2.1.3.4 Must have Ransomware Protection to backup and restore encrypted documents.

2.1.4 Intrusion Prevention Requirements:

2.1.4.1 Must have Host Intrusion Prevention System (HIPS) or Host Intrusion Detection System (HIDS.

2.1.4.2 Must have a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.

2.1.4.3 Must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.

2.1.4.4 Must provide detailed events with valuable information, including the attacker's information, when the attack occurred, and what are attempted to be exploited.

2.1.4.5 Must provide protection against known and zero-day attacks.

2.1.4.6 Must be able to deploy to multiple servers without a system reboot.

2.1.4.7 Must include out-of-the-box vulnerability protection for applications, including database, web, email, and File Transfer Protocol (FTP) services.

2.1.4.8 Must include rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code.

2.1.4.9 Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits.

2.1.4.10 Must automatically shield newly discovered vulnerabilities within hours, pushing protection to multiple servers without a system reboot.

2.1.4.11 Must have application control on network layer.

2.1.5 Firewall Requirements:

2.1.5.1 Must have enterprise-grade firewall policy with centralized management including pre-defined templates.

2.1.5.2 Must have virtual machine isolation.

2.1.5.3 Must have fine-grain filtering for ports, IP and MAC addresses.

2.1.5.4 Must have coverage on all IP-based protocols and all frame types.

2.1.5.5 Must have prevention for denial of service (DoS) attacks.

2.1.5.6 Must be able to design policies per network interface.

2.1.5.7 Must have detection of reconnaissance scans.

2.1.6 Integrity Monitoring Requirements:

2.1.6.1 Must be able to monitor critical operating system and application files such as directories, registry keys, and values to detect and report malicious and unexpected changes in real-time.

2.1.6.2 Must provide integrity monitoring, extend security and compliance of virtualized systems.

2.1.6.3 Must provide file integrity monitoring which tests and checks operating system, database, and application software if they have been tampered with or corrupted.

2.1.6.4 Must provide recommendation scan or baseline scan.

2.1.7 Virtual Patching Requirements:

2.1.7.1 Must provide virtual patching which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to servers within minutes.

2.1.7.2 Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours.

2.1.7.3 Must provide recommended virtual patching rules to protect applications and operating systems.

2.1.7.4 Must be able to create scheduled tasks for running recommendation scan to discover new rules to apply.

2.1.7.5 Must be able to assign virtual patching rules automatically through the scheduled tasks.

2.1.7.6 Must be able to unassign virtual patching rules after physical patch has been installed.

2.1.8 Application Control Requirements:

2.1.8.1 Must be able to monitor changes made to the server compared to baseline software.

2.1.8.2 Must be able to allow or block the software and optionally lock down the server from unauthorized change.

2.1.8.3 Must be able to set maintenance mode to allow installation of software and changes to operating systems.

2.1.8.4 Must be able to unauthorize scripts and applications should be alerted in the console.

2.1.8.5 Must be able to manually input (Secure Hash Algorithm 1) SHA-1 value to block specific files.

2.1.9 Log Inspection Requirements:

2.1.9.1 Must have the capability to inspect logs and events generated by operating systems and applications.

2.1.9.2 Must be able to recommend and assign relevant log inspection rules to the server automatically based on the operating system and applications installed.

2.1.9.3 Must be able to automatically recommend and unassign log inspection rules that are not required.

2.1.9.4 Must have predefined templates for operating systems and enterprise applications to avoid manual creation of rules.

2.1.9.5 Must be able to create customized rules to support custom applications.

2.1.10 Event Tagging Requirements:

2.1.10.1 Must have event tagging so that administrators can add “tag” to events generated.

2.1.10.2 Must be able to add, edit, and delete tags created by the administrators.

2.1.10.3 Must be able to search for events based on the specified tag.

2.1.10.4 Must allow administrators to specify an event that is to be automatically tagged.

2.1.11 Integration Requirements:

2.1.11.1 Must support integration to the third-party SIEM.

2.1.11.2 Must have integration with Microsoft Active Directory.

2.1.11.3 Must have login synchronization in Active Directory when creating new users.

2.1.11.4 Must support selective module on agent installation.

2.1.11.5 Must have an integration to virtual analyzer to send data files for analysis.

## 3. MANAGED EXTENDED DETECTION AND RESPONSE (XDR) PLATFORM

### 3.1 Platform Features:

3.1.1 Must be able to correlate events and integrate different security protection layers such as endpoint, email, and server in a single management console.

3.1.2 Must have a security posture dashboard with customizable view to show alerts, attacks, and reports.

3.1.3 Must have an investigation platform that provides a view of possible procedures used by the attacker.

3.1.4 Must allow integration with third-party solutions through an Application Program Interface (API).

3.1.5 Must have a view for easier response like endpoint isolation, collect files, search endpoint, check execution profile, quarantine the email, or block the email sender.

3.1.6 Must have a preview of the critical users, machines, and email accounts that need prioritization for response.

3.1.7 Must have a platform where the administrator would have the latest view of the security breaches, information, and links to the published articles.

3.1.8 Must have a platform for easier investigation like usual graphical view and timeline of the attack.

3.1.9 Must be able to isolate at-risk endpoints to run an investigation, resolve security issues, and restore the connection promptly when all issues have been resolved.

3.1.10 Must have a built-in graphical triage viewer to ease security operations.

3.1.11 Must allow administrators to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.

3.1.12 Must have risk insight capabilities XDR detection and continuous evaluation of vulnerabilities, cloud application activity, account compromise, and anomaly detections to assess the overall organizational risk, trends over time, and relative comparisons to peer companies in the same industry or region.

### 3.2 Managed Services

3.2.1 Must provide twenty-four by seven (24x7) continuous alert monitoring, correlation and prioritization using automation and analytics, and proactive sweeping of endpoint, email, and server during annual subscription period.

3.2.2 Must provide monitoring and detection.

3.2.3 Must provide analysis and investigation.

3.2.4 Must provide response and reporting.

3.2.5 Must provide security analysts based in the Philippines and be composed of internal employees (no outsourcing) of the manufacturer with expertise and rich experience within areas such as threat research, threat response, and technical support. The analysts shall have global certifications in forensic analysis, threat intelligence and incident handling

3.2.6 Must provide alert severity as part of the initial analysis to filter and reduce the volume of alerts reviewed by the GCG.

3.2.7 Must provide evaluation of the impact of an incident within the GCG.

3.2.8 Must provide interpretation of the root cause chain, determine threat profile, and perform advanced investigation.

3.2.9 Must provide product response, provide remediation recommendations, create clean-up toolkits (if required), and monitor infection for reoccurrence.

3.2.10 Must provide a monthly Executive Summary Report that contains alerts, events, investigations, responses, and recommendations.

## 4. TRAINING REQUIREMENTS

4.1 The bidder shall provide in-depth knowledge on product installation, configuration, and license administration of the proposed Cyber Security Stack Solution for GCG to be conducted by a designated product expert.

## 5. BUDGET REQUIREMENTS

5.1 The budget for One (1) Lot Annual Subscription of Cyber Security Stack Solution for the Governance Commission for GOCCs (GCG) is Two Million Six Hundred Fifty Thousand Pesos Only (₱2,650,000.00).

## 6. BIDDER REQUIREMENTS

6.1 The bidder must have completed a similar contract for the supply and implementation of cyber security stack solution for the past three (3) years from the date of submission and receipt of bids.

6.2 Bidder must have at least five (5) years of continuous existence and engagement in IT security business.

6.3 The bidder must be a Platinum PhilGEPS registered supplier.

6.4 Subcontractors are prohibited.

## 7. POST-QUALIFICATION REQUIREMENTS

7.1 The bidder must provide a demonstration of the proposed cyber security stack solution to further validate and check the compliance with the stated specification and requirements of this Terms of Reference.

7.2 The bidder must provide the following documents during the post-qualification:

7.2.1 a certification issued by the principal or solution provider that the bidder is a certified partner and able to extend direct technical support to end-user for the product being offered; and

7.2.2 a Copy of company’s latest General Information Sheet (GIS), if applicable.

## 8. SERVICE LEVEL AGREEMENT (SLA)

The Winning Bidder (hereafter referred to as simply the “bidder”) must:

8.1 The bidder must provide full-time support and managed services, without additional cost to the GCG, during the twelve (12) months subscription period as specified:

8.1.1 single point of contact for all solution components;

8.1.2 twenty-four by seven (24x7) service desk support via telephone, email, or online chat portal;

8.1.3 at least one (1) hour response time upon receipt of issue escalation and two (2) hours for onsite support, if necessary;

8.1.4 procedures on support and issue escalation; and

8.1.5 service report every after the onsite support.

## 9. TERMS OF PAYMENT

9.1 The payment shall be made on a one-time basis after the deployment of the required license subscriptions.

9.2 Provided further that payment shall be made at least twenty (20) working days from receipt of complete documents such as billing statement/statement of account, and other pertinent documents.

## 10. CONFIDENTIALITY

10.1 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 10.2 or any information it acquires by virtue of the contract which the GCG deems confidential.

10.2 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.

## 11. DELIVERY AND IMPLEMENTATION

11.1 The delivery, configuration, and deployment of the proposed cyber security stack solution must be completed within twenty (20) calendar days from the receipt of the Notice to Proceed.

11.2 The contract for this project shall be subject to renewal whereby the performance evaluation of the bidder shall be conducted in accordance with the requirements of this Terms of Reference.

# 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 ANNUAL SUBSCRIPTION OF CYBER SECURITY STACK SOLUTION FOR THE GOVERNANCE COMMISSION FOR GOCCS (GCG)

| ITEM | SPECIFICATION | STATEMENT OF COMPLIANCE |
|---|---|---|
| 1 | **ENDPOINT AND EMAIL PROTECTION REQUIREMENTS** | |
| | 1.1 The bidder must provide two hundred fifty (250) annual license subscription of cloud-based endpoint and email protection at minimum specifications: | |
| | 1.1.1 General Requirements:<br>1.1.1.1 Must have advanced threat protection strategies to eliminate vulnerabilities from user activities and endpoints. | |
| | 1.1.1.2 Must have automatic detection and respond to a variety of threats including fileless attacks and ransomware. | |
| | 1.1.1.3 Must have investigation capabilities, fast response for suspicious objects or activities, and centralized visibility of the entire network. | |
| | 1.1.1.4 Must have machine learning and advanced detection techniques for broad protection against multiple threats (known or unknown). | |
| | 1.1.1.5 Must have a filter for threats using efficient strategies to minimize attack vectors. | |
| | 1.1.1.6 Must have noise cancellation techniques such as census and whitelist checking to reduce false positives. | |
| | 1.1.1.7 Must have ability to clean infected files, perform rollback, and recover lost files. | |
| | 1.1.1.8 Must have minimal impact to performance using efficient detection technique and low management costs. | |
| | 1.1.1.9 Must have off-premises compliance and protection which enables the employees to work outside the organization's network and still be covered by the organization's security policies. | |
| | 1.1.1.10 Must be able to co-exist with the existing third-party security solution within the GCG. | |
| | 1.1.1.11 Must be able to support mass deployment through the network and must also support uninstallation of third-party agents. | |
| | 1.1.1.12 Must have Extended Detection and Response (XDR) solution for both endpoint and email to facilitate detection and response functionalities, and directly integrate with the cloud-based XDR platform. | |

| | | |
|---|---|---|
| | 1.1.2 Anti-virus Requirements:<br>1.1.2.1 Must have pattern-based anti-malware. | |
| | 1.1.2.2 Must have behavioral analytics against scripts, ransomware, injection, memory, and browser attacks. | |
| | 1.1.2.3 Must have census check, variant protection, and file and web reputation. | |
| | 1.1.2.4 Must have exploit protection. | |
| | 1.1.2.5 Must have command-and-control (C&C) protection. | |
| | 1.1.2.6 Must have ransomware protection. | |
| | 1.1.2.7 Must have detection, response, and isolation functionality. | |
| | 1.1.2.8 Must have device control functionality. | |
| | 1.1.2.9 Must have threat intelligence sharing capability. | |
| | 1.1.2.10 Must have cloud-based centralized management console for multiple product deployment that would allow easy management and extended visibility of the environment. The centralized management console must allow integration with the third-party Security Information and Event Management (SIEM) or Security Orchestration, Automation and Response (SOAR). | |
| | 1.1.2.11 Must have user-based visibility to improve protection, reduce complexity, and eliminate redundant tasks related to security administration. | |
| | 1.1.2.12 Must have customizable dashboard to allow different administrators to select which summary they would like to view at a glance. | |
| | 1.1.2.13 Must have a Media Access Control (MAC) security solution to provide more regular anti-malware protection which includes device control and machine learning. The solution does not require a separate management console for MAC clients. | |
| | 1.1.2.14 Everything should be viewable and managed under a single pane of glass. | |
| | 1.1.2.15 Must have an option to allow users to configure the security agent settings and an option to uninstall the MAC security solution agent if needed. | |
| | 1.1.3 Vulnerability Protection Requirements:<br>1.1.3.1 Must be able to prevent emerging threats that could potentially compromise the GCG security regardless of the platform. | |
| | 1.1.3.2 Must be able to perform virtual patching for vulnerable operating systems. | |
| | 1.1.3.3 Must be integrated into a single security agent. | |

| | | |
|---|---|---|
| | 1.1.4 Application Control Requirements:<br>1.1.4.1 Must be capable of allowing or denying known or unknown applications, executables, and file types. | |
| | 1.1.4.2 Must have a reliable file reputation source for cross checking of known good files. This source must be constantly kept up to date with the latest known good file listing. | |
| | 1.1.4.3 Must have integration with other security solutions such as host intrusion prevention, data loss prevention, and mobile protection for better data correlation. | |
| | 1.1.4.4 Must be able to perform an automated inventory scan which categorizes installed applications depending on its file reputation - known good to potentially dangerous. | |
| | 1.1.4.5 Must have application whitelisting or blacklisting feature. | |
| | 1.1.5 Data Loss Prevention (DLP) Requirements:<br>1.1.5.1 Must have visibility and control over sensitive data and prevent data loss via USB flash drives, email, web, and cloud storage. | |
| | 1.1.5.2 Must have built-in templates that comply with specified guidelines and regulations. | |
| | 1.1.5.3 Must be able to support DLP enforcement of file encryption in Microsoft Office 365. | |
| | 1.1.5.4 Must be able to detect and react to improper data usage-based keywords, regular expressions, and file attributes. | |
| | 1.1.5.5 Must provide education to employees about corporate data usage policies through alerts, blocking or soft-blocking, and reporting. | |
| | 1.1.5.6 Must have visibility and management over data at rest control points and should include scanning of endpoints, file servers, mail store, Microsoft SharePoint, and cloud storage. | |
| | 1.1.5.7 Must have visibility and management over data in motion control points. | |
| | 1.1.5.8 Must have visibility and management over data in use control points. | |
| | 1.1.5.9 Must include a granular list of international identifiers. | |
| | 1.1.6 Endpoint Encryption Requirements:<br>1.1.6.1 Must support both file encryption and full disk encryption. | |
| | 1.1.6.2 Must have visibility and management of Apple FileVault encryption on keys to manage OSX based computers. | |

| | | |
|---|---|---|
| | 1.1.6.3 Must have visibility and management for Microsoft BitLocker encryption keys. | |
| | 1.1.6.4 Must have support and leverage flexible hardware and software-based encryption across mixed environments. | |
| | 1.1.7 Mobile Protection Requirements:<br>1.1.7.1 Must support smartphones and tablets running iOS or Android. | |
| | 1.1.7.2 Must allow administrator to track, monitor, and manage mobile devices, applications, and data through a single console. | |
| | 1.1.7.3 Must be able to protect corporate data with remote lock and wipe, and selective wipe. | |
| | 1.1.7.4 Must have option for device enrollment through a web link, QR code, or iTunes download. | |
| | 1.1.7.5 Must provide notification to administrator of jail broken or unencrypted devices. | |
| | 1.1.7.6 Must allow administrator to manage and block specific types of applications based on categories. | |
| | 1.1.7.7 Must be able to protect a mobile device from known bad websites that promote phishing, pharming, hacking, and the likes. | |
| | 1.1.7.8 Must be able to scan mobile malware and allows to quarantine or delete detected files. | |
| | 1.1.7.9 Must be able to perform remote wipe all data on a mobile device by sending a Short Message Service (SMS) text message. | |
| | 1.1.7.10 Must have control filters to alert or block specific traffic. | |
| | 1.1.7.11 Must prevent networking backdoors from attacking the network. | |
| | 1.1.7.12 Must have application inventory and be able to control it per category. | |
| | 1.1.8 Mail Protection Requirements:<br>1.1.8.1 Must have integration with Microsoft Office 365 email service. | |
| | 1.1.8.2 Must have anti-virus, anti-spam, and anti-relay protection. | |
| | 1.1.8.3 Must be able to quarantine emails upon virus detection. | |
| | 1.1.8.4 Must have heuristic anti-spam protection. | |
| | 1.1.8.5 Must be able to add policies based on custom preferences. | |
| | 1.1.8.6 Must be able to block or allow customized subjects, based on keywords and the likes in any part of the email message. | |
| | 1.1.8.7 Must be able to support multiple domains. | |

| | | |
|---|---|---|
| | 1.1.8.8 Must be able to protect against phishing websites. | |
| | 1.1.8.9 Must be able to block or approve senders list. | |
| | 1.1.8.10 Must have advanced detection and alert functionalities for early mitigation of emerging threats and targeted attacks. | |
| | 1.1.8.11 Must detect unknown Uniform Resource Locators (URLs) embedded in email messages. | |
| | 1.1.8.12 Must support protection against directory harvest attacks (DHA). | |
| | 1.1.8.13 Must protect from malicious URLs embedded in email messages. | |
| | 1.1.8.14 Must have anti-spoofing feature. | |
| | 1.1.8.15 Must provide security for business email compromise (BEC). | |
| | 1.1.8.16 Must be able to capture and analyze all incoming emails from internet to Microsoft Office 365 mailboxes. | |
| | 1.1.8.17 Must be able to capture and analyze all outgoing emails from Microsoft Office 365 mailboxes to the internet. | |
| | 1.1.8.18 Must be able to capture and analyze all Microsoft SharePoint and Microsoft OneDrive for business files. | |
| | 1.1.8.19 Must be able to capture and analyze all Microsoft Office 365 internal email flows (from Microsoft Office 365 mailbox to Microsoft Office 365 mailbox). | |
| | 1.1.8.20 Must have real-time scans to protect data in motion and manual scan for data at rest. | |
| | 1.1.8.21 Must not impact or affect user email delivery or file sharing in case of service disruption or unavailability (pass-through). | |
| | 1.1.8.22 Must be able to prevent the delivery of an identified suspicious or threated email and files. | |
| | 1.1.8.23 Must be able to detect threats in emails without blocking the delivery to the recipient (pass-through). | |
| | 1.1.8.24 Must support BEC that includes writing style DNA technology to scan the English email messages of a desired individual to learn their Writing Style and generate a Writing Style mode. | |
| | 1.1.9 Web Protection Requirements:<br>1.1.9.1 Must have anti-virus and must be able to scan traffic going in and out the network in real-time. | |
| | 1.1.9.2 Must have a URL database with multiple categories. | |
| | 1.1.9.3 Must be able to protect HTTP, FTP, SMTP, POP3 protocols. | |

| | | |
|---|---|---|
| | 1.1.9.4 Must be able to create access policy by category, from URL database, customized list and by keyword. | |
| | 1.1.9.5 Must block forbidden internet applications through a web browser. | |
| | 1.1.9.6 Must be able to block access to malicious websites and restricted areas. | |
| | 1.1.9.7 Must be able to support scan HTTP and HTTPs traffic for spyware and other web threats. | |
| | 1.1.9.8 Must be able to support blocking of outbound data to known spyware and phishing-related websites. | |
| | 1.1.9.9 Must be able to validate web-based codes to screen web pages for malicious codes. | |
| | 1.1.9.10 Must be able to deploy policy based on users and/or groups defined in the active directory. | |
| | 1.1.9.11 Must be able to generate web security violations per user, hostname, or IP address. | |
| | 1.1.9.12 Must be able to generate reports on web violations statistics. | |
| 2 | **SERVER PROTECTION REQUIREMENTS** | |
| | 2.1 The bidder must provide fifty (50) annual license subscription of cloud-based server protection at minimum specifications: | |
| | 2.1.1 General Requirements:<br>2.1.1.1 Must provide a single platform for complete server protection over physical servers, virtual servers, and virtual desktop computers in a single management console. | |
| | 2.1.1.2 Must have layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications, and operating systems. | |
| | 2.1.1.3 Must support web reputation for preventing access to malicious websites. | |
| | 2.1.1.4 Must support Docker hosts and containers running on the Windows and Linux distribution. | |
| | 2.1.1.5 Must have Extended Detection and Response (XDR) solution for server to facilitate detection and response functionalities, and directly integrate with the cloud-based XDR platform. | |
| | 2.1.1.6 For unsupported operating systems, the bidder shall provide at least 500mbps of network detection and response capabilities. The GCG will provide the virtual machine requirements. | |
| | 2.1.2 Management Console Requirements:<br>2.1.2.1 Must be a web-based management system for administrators. | |

| | | |
|---|---|---|
| | 2.1.2.2 Must have a dashboard for displaying multiple information and must be configurable by administrators to display information which is only required. | |
| | 2.1.2.3 Must have alerts in the main menu to view administrator notifications concerning system or security events. | |
| | 2.1.2.4 Must have Firewall Events to view activities on computers with the firewall enabled. | |
| | 2.1.2.5 Must have Deep Packet Inspection (DPI) Events to view security-related DPI activities. This should display exploits detected, either resulting in dropped traffic or logging of events. | |
| | 2.1.2.6 Must have System Events to view a summary of security-related events, primarily for the management server and including Agents' system events. All administrative actions should be audited within the System Events. | |
| | 2.1.3 Anti-malware Requirements:<br>2.1.3.1 Must have web filtering to protect against malicious websites. | |
| | 2.1.3.2 Must have prediction machine learning to protect against unknown malware. | |
| | 2.1.3.3 Must have behavioral monitoring to protect against malicious scripts and applications. | |
| | 2.1.3.4 Must have Ransomware Protection to backup and restore encrypted documents. | |
| | 2.1.4 Intrusion Prevention Requirements:<br>2.1.4.1 Must have Host Intrusion Prevention System (HIPS) or Host Intrusion Detection System (HIDS). | |
| | 2.1.4.2 Must have a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations. | |
| | 2.1.4.3 Must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities. | |
| | 2.1.4.4 Must provide detailed events with valuable information, including the attacker's information, when the attack occurred, and what are attempted to be exploited. | |
| | 2.1.4.5 Must provide protection against known and zero-day attacks. | |
| | 2.1.4.6 Must be able to deploy to multiple servers without a system reboot. | |
| | 2.1.4.7 Must include out-of-the-box vulnerability protection for applications, including database, web, email, and File Transfer Protocol (FTP) services. | |

| | | |
|---|---|---|
| | 2.1.4.8 Must include rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code. | |
| | 2.1.4.9 Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits. | |
| | 2.1.4.10 Must automatically shield newly discovered vulnerabilities within hours, pushing protection to multiple servers without a system reboot. | |
| | 2.1.4.11 Must have application control on network layer. | |
| | 2.1.5 Firewall Requirements:<br>2.1.5.1 Must have enterprise-grade firewall policy with centralized management including pre-defined templates. | |
| | 2.1.5.2 Must have virtual machine isolation. | |
| | 2.1.5.3 Must have fine-grain filtering for ports, IP and MAC addresses. | |
| | 2.1.5.4 Must have coverage on all IP-based protocols and all frame types. | |
| | 2.1.5.5 Must have prevention for denial of service (DoS) attacks. | |
| | 2.1.5.6 Must be able to design policies per network interface. | |
| | 2.1.5.7 Must have detection of reconnaissance scans. | |
| | 2.1.6 Integrity Monitoring Requirements:<br>2.1.6.1 Must be able to monitor critical operating system and application files such as directories, registry keys, and values to detect and report malicious and unexpected changes in real-time. | |
| | 2.1.6.2 Must provide integrity monitoring, extend security and compliance of virtualized systems. | |
| | 2.1.6.3 Must provide file integrity monitoring which tests and checks operating system, database, and application software if they have been tampered with or corrupted. | |
| | 2.1.6.4 Must provide recommendation scan or baseline scan. | |
| | 2.1.7 Virtual Patching Requirements:<br>2.1.7.1 Must provide virtual patching which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to servers within minutes. | |

|  |  |  |
|---|---|---|
|  | 2.1.7.2 Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours. |  |
|  | 2.1.7.3 Must provide recommended virtual patching rules to protect applications and operating systems. |  |
|  | 2.1.7.4 Must be able to create scheduled tasks for running recommendation scan to discover new rules to apply. |  |
|  | 2.1.7.5 Must be able to assign virtual patching rules automatically through the scheduled tasks. |  |
|  | 2.1.7.6 Must be able to unassign virtual patching rules after physical patch has been installed. |  |
|  | 2.1.8 <u>Application Control Requirements:</u><br>2.1.8.1 Must be able to monitor changes made to the server compared to baseline software. |  |
|  | 2.1.8.2 Must be able to allow or block the software and optionally lock down the server from unauthorized change. |  |
|  | 2.1.8.3 Must be able to set maintenance mode to allow installation of software and changes to operating systems. |  |
|  | 2.1.8.4 Must be able to unauthorize scripts and applications should be alerted in the console. |  |
|  | 2.1.8.5 Must be able to manually input (Secure Hash Algorithm 1) SHA-1 value to block specific files. |  |
|  | 2.1.9 <u>Log Inspection Requirements:</u><br>2.1.9.1 Must have the capability to inspect logs and events generated by operating systems and applications. |  |
|  | 2.1.9.2 Must be able to recommend and assign relevant log inspection rules to the server automatically based on the operating system and applications installed. |  |
|  | 2.1.9.3 Must be able to automatically recommend and unassign log inspection rules that are not required. |  |
|  | 2.1.9.4 Must have predefined templates for operating systems and enterprise applications to avoid manual creation of rules. |  |
|  | 2.1.9.5 Must be able to create customized rules to support custom applications. |  |
|  | 2.1.10 <u>Event Tagging Requirements:</u><br>2.1.10.1 Must have event tagging so that administrators can add “tag” to events generated. |  |
|  | 2.1.10.2 Must be able to add, edit, and delete tags created by the administrators. |  |
|  | 2.1.10.3 Must be able to search for events based on the specified tag. |  |

| | | |
|---|---|---|
| | 2.1.10.4 Must allow administrators to specify an event that is to be automatically tagged. | |
| | 2.1.11 Integration Requirements:<br>2.1.11.1 Must support integration to the third-party SIEM. | |
| | 2.1.11.2 Must have integration with Microsoft Active Directory. | |
| | 2.1.11.3 Must have login synchronization in Active Directory when creating new users. | |
| | 2.1.11.4 Must support selective module on agent installation. | |
| | 2.1.11.5 Must have an integration to virtual analyzer to send data files for analysis. | |
| 3 | **MANAGED EXTENDED DETECTION AND RESPONSE (XDR) PLATFORM** | |
| | 3.1 Platform Features:<br>3.1.1 Must be able to correlate events and integrate different security protection layers such as endpoint, email, and server in a single management console. | |
| | 3.1.2 Must have a security posture dashboard with customizable view to show alerts, attacks, and reports. | |
| | 3.1.3 Must have an investigation platform that provides a view of possible procedures used by the attacker. | |
| | 3.1.4 Must allow integration with third-party solutions through an Application Program Interface (API). | |
| | 3.1.5 Must have a view for easier response like endpoint isolation, collect files, search endpoint, check execution profile, quarantine the email, or block the email sender. | |
| | 3.1.6 Must have a preview of the critical users, machines, and email accounts that need prioritization for response. | |
| | 3.1.7 Must have a platform where the administrator would have the latest view of the security breaches, information, and links to the published articles. | |
| | 3.1.8 Must have a platform for easier investigation like usual graphical view and timeline of the attack. | |
| | 3.1.9 Must be able to isolate at-risk endpoints to run an investigation, resolve security issues, and restore the connection promptly when all issues have been resolved. | |
| | 3.1.10 Must have a built-in graphical triage viewer to ease security operations. | |
| | 3.1.11 Must allow administrators to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets. | |

| | | |
|---|---|---|
| | 3.1.12 Must have risk insight capabilities XDR detection and continuous evaluation of vulnerabilities, cloud application activity, account compromise, and anomaly detections to assess the overall organizational risk, trends over time, and relative comparisons to peer companies in the same industry or region. | |
| | 3.2 Managed Services<br>3.2.1 Must provide twenty-four by seven (24x7) continuous alert monitoring, correlation and prioritization using automation and analytics, and proactive sweeping of endpoint, email, and server during annual subscription period. | |
| | 3.2.2 Must provide monitoring and detection. | |
| | 3.2.3 Must provide analysis and investigation. | |
| | 3.2.4 Must provide response and reporting. | |
| | 3.2.5 Must provide security analysts based in the Philippines and be composed of internal employees (no outsourcing) of the manufacturer with expertise and rich experience within areas such as threat research, threat response, and technical support. The analysts shall have global certifications in forensic analysis, threat intelligence and incident handling. | |
| | 3.2.6 Must provide alert severity as part of the initial analysis to filter and reduce the volume of alerts reviewed by the GCG. | |
| | 3.2.7 Must provide evaluation of the impact of an incident within the GCG. | |
| | 3.2.8 Must provide interpretation of the root cause chain, determine threat profile, and perform advanced investigation. | |
| | 3.2.9 Must provide product response, provide remediation recommendations, create clean-up toolkits (if required), and monitor infection for reoccurrence. | |
| | 3.2.10 Must provide a monthly Executive Summary Report that contains alerts, events, investigations, responses, and recommendations. | |
| 4 | **TRAINING REQUIREMENTS**<br>4.1 The bidder shall provide in-depth knowledge on product installation, configuration, and license administration of the proposed Cyber Security Stack Solution for GCG to be conducted by a designated product expert. | |
| 5 | **BUDGET REQUIREMENTS**<br>5.1 The budget for One (1) Lot Annual Subscription of Cyber Security Stack Solution for the Governance Commission for GOCCs (GCG) is Two Million Six Hundred Fifty Thousand Pesos Only (₱2,650,000.00). | |

| | | |
|---|---|---|
| 6 | **BIDDER REQUIREMENTS**<br>6.1 The bidder must have completed a similar contract for the supply and implementation of cyber security stack solution for the past three (3) years from the date of submission and receipt of bids. | |
| | 6.2 Bidder must have at least five (5) years of continuous existence and engagement in IT security business. | |
| | 6.3 The bidder must be a Platinum PhilGEPS registered supplier. | |
| | 6.4 Subcontractors are prohibited. | |
| 7 | **POST-QUALIFICATION REQUIREMENTS**<br>7.1 The bidder must provide a demonstration of the proposed cyber security stack solution to further validate and check the compliance with the stated specification and requirements of this Terms of Reference. | |
| | 7.2 The bidder must provide the following documents during the post-qualification:<br>7.2.1 a certification issued by the principal or solution provider that the bidder is a certified partner and able to extend direct technical support to end-user for the product being offered; and<br>7.2.2 a Copy of company's latest General Information Sheet (GIS), if applicable. | |
| 8 | **SERVICE LEVEL AGREEMENT (SLA)**<br>The Winning Bidder (hereafter referred to as simply the "bidder") must:<br>8.1 The bidder must provide full-time support and managed services, without additional cost to the GCG, during the twelve (12) months subscription period as specified:<br>8.1.1 single point of contact for all solution components;<br>8.1.2 twenty-four by seven (24x7) service desk support via telephone, email, or online chat portal;<br>8.1.3 at least one (1) hour response time upon receipt of issue escalation and two (2) hours for onsite support, if necessary;<br>8.1.4 procedures on support and issue escalation; and<br>8.1.5 service report every after the onsite support. | |
| 9 | **TERMS OF PAYMENT**<br>9.1 The payment shall be made on a one-time basis after the deployment of the required license subscriptions. | |
| | 9.2 Provided further that payment shall be made at least twenty (20) working days from receipt of complete documents such as billing statement/statement of account, and other pertinent documents. | |

|  |  |  |
|---|---|---|
| 10 | **CONFIDENTIALITY**<br>10.1 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 10.2 or any information it acquires by virtue of the contract which the GCG deems confidential. |  |
|  | 10.2 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. |  |
| 11 | **DELIVERY AND IMPLEMENTATION**<br>11.1 The delivery, configuration, and deployment of the proposed cyber security stack solution must be completed within twenty (20) calendar days from the receipt of the Notice to Proceed. |  |
|  | 11.2 The contract for this project shall be subject to renewal whereby the performance evaluation of the bidder shall be conducted in accordance with the requirements of this Terms of Reference. |  |

# *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<br>(col 5+6+7+ 8) | Total Price delivered Final Destination<br>(col 9) x (col 4) |
| | | | | | | | | | |

Name: ____________________________________________________________

Legal Capacity: ______________________________________________________

Signature: __________________________________________________________

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

Republic of the Philippines

gppb

Government Procurement Policy Board