REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

Procurement of GOODS

Subscription to Cyber Security Operations Center

Project ID No. **DBM-2024-05**

Sixth Edition
July 2020

Table of Contents

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

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

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

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

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

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

CDA - Cooperative Development Authority.

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

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

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

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

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

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

GFI – Government Financial Institution.

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

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

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

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

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

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

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

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

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

UN – United Nations.

Section I. Invitation to Bid

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

INVITATION TO BID
"Subscription to Cyber Security Operations Center"

1. The Department of Budget and Management (DBM), through the FY 2024 General Appropriations Act, intends to apply the sum of **Fifty-One Million Pesos (P51,000,000.00)** being the Approved Budget for the Contract (ABC) to payments under the contract for the "**Subscription to Cyber Security Operations Center**" (Project ID No. **DBM-2024-05)**. For the purpose of **early procurement** authorized under Section 7.6 of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184, the proposed budget under the FY 2024 National Expenditure Program shall be used as basis. Further, consistent with the requirement in the same Section 7.6, **no award of contract shall be made until the approval and effectivity of the FY 2024 General Appropriations Act**. The period for the performance of the obligations under the Contract shall not go beyond the validity of the appropriation for the Project. Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The DBM now invites bids for the above-entitled Procurement Project. Delivery of the Goods is required as specified in Section VI (Schedule of Requirements) of the Bidding Documents. Bidders should have completed **within the period of November 7, 2020 to November 6, 2023** a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "*pass/fail*" criterion as specified in the 2016 Revised IRR of 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 the DBM-Bids and Awards Committee (BAC) Secretariat through the contact details given below and inspect the Bidding Documents as posted on the websites of the DBM and the Philippine Government Electronic Procurement System (PhilGEPS).

5. A complete set of Bidding Documents may be acquired by interested Bidders on October 17, 2023 from the given address and website below and upon payment of a fee in the amount of Fifty Thousand Pesos (P50,000.00).

   Payment may be made in either mode, as follows:

   a) Online payment through the Landbank Link.Biz Portal. However, this mode of payment may only be done until November 3, 2023 (four [4] calendar days before the Submission of Bids), 11:00 p.m., for crediting and recording purposes. Procedural guidelines for online payment may be accessed via https://dbm.gov.ph/images/Advisory_for_Bidders_Suppliers-LinkBiz.pdf. Bidders shall present its confirmation receipt to the BAC Secretariat in person, by facsimile, or through electronic means, which shall be used as proof of payment for the bidding documents fee.

   b) Payment, in person, to the DBM Administrative Service (AS)-Cash Division, through the BAC Secretariat, DBM AS-Procurement Management Division, Ground Floor, DBM Building III, General Solano St., San Miguel, Manila. The Procuring Entity shall allow the bidder to present its proof of payment for the fees which will be presented in person, by facsimile, or through electronic means.

6. The DBM will hold a Pre-Bid Conference on October 24, 2023, 9:30 a.m., at the BAC Conference Room, Ground Floor, DBM Building III, General Solano St., San Miguel, Manila, and/or **through video conferencing or webcasting**, which shall be open to prospective bidders.

   In case of video conferencing or webcasting, the prospective bidders are advised to first log in the BAC waiting room, **https://meet.google.com/hma-jmco-dbx**, and wait for further advice to join the BAC meeting room, the link of which shall be provided to the prospective bidders before the start of the Pre-Bid Conference.

7. Bids must be duly received by the BAC Secretariat or the DBM AS-Central Records Division through manual submission at the office address indicated below on or before November 7, 2023, 9:30 a.m. Late bids shall not be accepted.

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

9. Bid opening shall be on November 7, 2023, 9:30 a.m., at the given address below and via video conferencing. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity. Authorized attendees, including representatives of bidders, who are physically present at the BAC Conference Room, DBM Building III, General Solano St., San Miguel, Manila shall likewise join the meeting via videoconferencing.

   Bidders are advised to first log in the BAC waiting room, https://meet.google.com/hma-jmco-dbx, and wait for further advice to join the BAC meeting room, the link of which shall be provided to the bidders before the start of bid opening.

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

11. For further information, please refer to:

DBM-BAC Secretariat
DBM-Administrative Service-Procurement Management Division
Ground Floor, DBM Building III, General Solano St., San Miguel, Manila
Telefax No. 8657-3300 local 3115
Email address: procurement@dbm.gov.ph

12. You may visit the following website to download the Bidding Documents:
https://www.dbm.gov.ph/index.php/procurement/invitation-to-bid

October 17, 2023

RAMON VICENTE B. ASUNCION
Vice Chairperson, DBM-BAC

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, Department of Budget and Management, wishes to receive Bids for the "**Subscription to Cyber Security Operations Center**" with Project Identification No. *DBM-2024-05.*

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 **Fifty-One Million Pesos (P51,000,000.00).** The period for the performance of the obligations under the Contract shall not go beyond the validity of the appropriation for the Project.

2.2. The source of funding is the FY 2024 General Appropriations Act. For the purpose of early procurement authorized under Section 7.6 of the 2016 Revised IRR of RA No. 9184, the proposed budget under the FY 2024 National Expenditure Program shall be used as basis.

3. Bidding Requirements

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

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

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

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

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

5. Eligible Bidders

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

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

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

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

b. The bidder must have completed at least two (2) similar contracts:

i. The aggregate amount of which should be equivalent to at least *fifty percent (50%)* of the ABC for this Project; **and**

ii. The largest of these similar contracts must be equivalent to at least half of the percentage of the ABC as required above (i.e., twenty-five percent [25%]).

5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 Revised 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 Bidder may subcontract portions of the Project to the extent allowed by the Procuring Entity as stated herein, but in no case more than twenty percent (20%) of the Project.

The Procuring Entity has prescribed that subcontracting is not allowed.

8. Pre-Bid Conference

The DBM will hold a Pre-Bid Conference for this Project on October 24, 2023, 9:30 a.m., at the BAC Conference Room, Ground Floor, DBM Building III, General Solano St., San Miguel, Manila, **and/or through video conferencing or webcasting**, which shall be open to prospective bidders, as indicated in paragraph 6 of the **IB**.

In case of video conferencing or webcasting, the prospective bidders are advised to first log in the BAC waiting room, **https://meet.google.com/hma-jmco-dbx**, and wait for further advice to join the BAC meeting room, the link of which shall be provided to the prospective bidders before the start of the Pre-Bid Conference.

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 DBM, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

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

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed **within the period of November 7, 2020 to November 6, 2023**.

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

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 **Section VII (Technical Specifications**).

b. For Goods offered from abroad:

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

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

13. Bid and Payment Currencies

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

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

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration 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 **March 6, 2024.** 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) copy of the first and second components of its Bid.

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

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

16. Deadline for Submission of Bids

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

17. Opening and Preliminary Examination of Bids

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

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

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

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

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

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

19.4. The Project shall be awarded as one (1) Project having several items that shall be awarded as one (1) 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

`

Bid Data Sheet

ITB Clause	
5.3	For this purpose, contracts similar to the Project shall: a. refer to the comprehensive design, implementation, and management of a Security Operation Center (SOC); and If the comprehensive design, implementation, and management of a SOC form part of a bigger contract, only the cost component of the comprehensive design, implementation, and management of a SOC shall be considered for purposes of comparing the value thereof to at least fifty percent (50%) of the ABC; and b. have been completed **within the period of November 7, 2020 to November 6, 2023.**
7	Subcontracting is not allowed.
10.1	Notarization of the required documents shall comply with the 2004 Rules on Notarial Practice which limits competent evidence of identity to the following: (i) identification documents issued by an official agency bearing the photograph and signature of the individual (i.e., passport, driver's license, Unified Multi-Purpose ID, etc.); or (ii) the oath of affirmation of one (1) credible witness not privy to the instrument, document or transaction who is personally known to the notary public and who personally knows the individual and shows to the notary public documentary identification.
12	The price of the Goods shall be quoted DDP Manila or the applicable International Commercial Terms (INCOTERMS) for this Project.
14.1	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: a. The amount of not less than P1,020,000.00, if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or b. The amount of not less than P2,550,000.00, if bid security is in Surety Bond.
15	Bidders shall enclose their eligibility and technical documents described in Section II. Instructions to Bidders (ITB) Clause 10 in one sealed envelope marked "TECHNICAL COMPONENT", and their financial component described in ITB Clause 11 in another sealed envelope marked "FINANCIAL COMPONENT", sealing them all in an outer envelope marked "BID".

`

	Further, all envelopes shall: a) contain the name of the contract to be bid in capital letters; b) bear the name and address of the Bidder in capital letters; c) be addressed to the Procuring Entity's BAC in accordance with Section I. Invitation to Bid Clause 9; d) bear the specific identification of the Project indicated in ITB Clause 1; and e) bear a warning "DO NOT OPEN BEFORE…" the date and time for the opening of bids, in accordance with the aforementioned date and time. Please be reminded that pursuant to Section 25.9 of the 2016 Revised IRR of RA No. 9184, unsealed or unmarked bid envelopes shall be rejected. However, bid envelopes that are not properly sealed and marked, as required in the Bidding Documents, shall be accepted, provided that the bidder or its duly authorized representative shall acknowledge such condition of the bid as submitted. The BAC shall assume no responsibility for the misplacement of the contents of the improperly sealed or marked bid, or for its premature opening.
19.3	The computation of a prospective bidder's NFCC must be at least equal to the ABC to be bid, pursuant to Section 23.4.1.4 of the 2016 Revised IRR of RA No. 9184.
20	The bidder with the Lowest Calculated Bid shall submit **ALL** of the following post-qualification requirements: 1. Photocopy/ies of Contract/s or Purchase Order/s of one of the following: i. A single contract that is similar to the project and whose value must be at least fifty percent (50%) of the ABC to be bid; **OR** ii. At least two (2) similar contracts: (a) the aggregate amount of which should be equivalent to at least fifty percent (50%) of the ABC; **AND** (b) the largest of these similar contracts must be equivalent to at least half of the percentage of the ABC as required above (i.e., twenty-five percent [25%]). 2. The corresponding proof/s of completion, which could either be: i. Certificate/s of Final Acceptance/Completion from the bidder's client/s; or ii. Official Receipt/s or Sales Invoice/s of the bidder covering the full amount of the contract/s. 3. Latest Income and Business Tax Returns, filed and paid through the Electronic Filing and Payment System (EFPS), consisting of the following: i. 2022 Income Tax Return with proof of payment; and

`

	ii. VAT Returns (Form 2550M and 2550Q) or Percentage Tax Returns (2551M) with proof of payment covering the months from April 2023 to September 2023. 4. Certification that the bidder is an authorized reseller of the brand(s) being offered together with a valid certification from the manufacturer(s). 5. At least two (2) of the following certifications and accreditation for Cyber Security Operation Center (SOC): i. The Open Group Architecture Framework (TOGAF); ii. Certified Ethical Hacker (CEH); iii. Certification in Information Technology Infrastructure Library (ITIL) Framework; iv. Certified Information Security Manager (CISM); v. CISCO Certified Network Professional (CCNP) or any equivalent certification from other technology provider; vi. Palo Alto Networks Certified Network Security Administrator (PCNSA) or any equivalent certification from other technology provider; vii. Fortinet Certified Network Security or any equivalent certification from other technology provider; and/or viii. COMPTIA Security + or any equivalent security certification. <u>Additional Conditions:</u> * Failure to submit any of the post-qualification requirements on time, or a finding against the veracity thereof, shall disqualify the bidder for award: Provided, that in the event that a finding against the veracity of any of the documents submitted is made, it shall cause the forfeiture of the Bid Security in accordance with Section 69 of the 2016 Revised IRR of RA No. 9184. ****** In case the notice for the submission of post-qualification documents is sent via the bidder's email, it shall be considered as received by the bidder on the date and time the email was sent, whether or not the bidder acknowledged the said email. It shall be the bidder's responsibility to check its/his/her email for the purpose. ******* In case of a tie and two (2) or more bidders have been post-qualified as Lowest Calculated Responsive Bidders (LCRBs), the tie-breaking measure determined by the procuring entity shall be non-discretionary and nondiscriminatory such that the same is based on sheer luck or chance. As a matter of information to the prospective bidders, the DBM-BAC has determined to use the method of a "raffle," wherein the names of the bidders involved in the tie and declared as LCRBs will be written in separate similar unmarked papers, and will be folded and placed in a container. Thereafter, a DBM-BAC representative will draw the raffle in an order wherein the first drawn bidder shall be considered as the winning LCRB and awarded the contract. The second drawn bidder shall be the second ranked LCRB, and so

`

	on until all LCRBs are drawn and ranked. In case of the failure, refusal or inability of the winning LCRB to submit the documents required under Section 37.1 of the 2016 Revised IRR of RA No. 9184 or to enter into contract and post the required Performance Security, as provided in Section 40 of the same IRR, the BAC shall disqualify the said LCRB, and shall proceed to award the contract to the second ranked LCRB. This procedure shall be repeated until a Notice to Proceed has been issued.

`

Section IV. General Conditions of Contract

1. Scope of Contract

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

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

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

2. Advance Payment and Terms of Payment

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

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

3. Performance Security

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

4. Inspection and Tests

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

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

5. Warranty

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

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

6. Liability of the Supplier

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

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

Section V. Special Conditions of Contract

Special Conditions of Contract

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

	Packaging The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit. The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity. The outer packaging must be clearly marked on at least four (4) sides as follows: Name of the Procuring Entity Name of the Supplier Contract Description Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. **Transportation** Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.
	Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.

	Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	The terms of payment shall be in accordance with item 9.0 of Annex "A" (Detailed Technical Specifications).
4	The inspection and approval as to the acceptability of the Goods vis-à-vis its compliance with the technical specifications will be done with prior written notice to the authorized representative of the Supplier. The inspection will push through as scheduled even in the absence of the Supplier's representative, if the latter was duly notified. In which case, the result of the inspection conducted by the Procuring Entity shall be final and binding upon the Supplier.

Section VI. Schedule of Requirements

Section VI. Schedule of Requirements

The delivery schedule stipulates hereafter the date of delivery to the project site.

Item	Description	Delivery Schedule
1	**Delivery, Integration, and Configuration of the Cyber Security Operations Center (SOC)**, as detailed in item 5.4 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Within sixty (60) calendar days from the receipt of the Notice to Proceed (NTP)
2	**Submission of As-built Documentation of the Cyber SOC**, as detailed in item 5.6 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Within seven (7) calendar days after the completion of the Delivery, Integration, and Configuration of the Cyber SOC
3	**Subscription to Cyber Security Operation**, as detailed in item 3.0 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Twelve (12) months from the completion of the delivery, integration, and configuration phase of the Project
4	**Technical Trainings**, as detailed in item 5.4.11 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	
a	**COMPTIA Security +**	Within two (2) months from the receipt of NTP
b	**Certified Ethical Hacker (CEH) v12**	Within three (3) months from the receipt of the NTP
c	**Certified Penetration Testing Professional (CPENT)**	Within four (4) months from the receipt of the NTP
5	**Submission of SOC Monthly Reports**, as detailed in item 5.7.4 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Within the first week of the succeeding month

* The period for the performance of the obligations under the Contract shall not be beyond the validity of the appropriation for the Project.

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

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

Section VII. Technical Specifications

Section VII. Technical Specifications

Bidders must state here either "Comply" or any equivalent term in the column "Bidder's Statement of Compliance" against each of the individual parameters of each "Specification."

Specifications		Bidder's Statement of Compliance
I.	**Objectives** *(see attached Annex "A" [Detailed Technical Specifications], item 2.0)*	
II.	**Duration of the Subscription** *(see attached Annex "A" [Detailed Technical Specifications], item 3.0)*	
III.	**Qualifications of the Contractor** *(see attached Annex "A" [Detailed Technical Specifications], item 4.0)*	
IV.	**Technical Requirements and Scope of Work** *(see attached Annex "A" [Detailed Technical Specifications], item 5.0)*	
V.	**Service Level Agreement** *(see attached Annex "A" [Detailed Technical Specifications], item 6.0)*	
VI.	**Warranties of the Contractor** *(see attached Annex "A" [Detailed Technical Specifications], item 7.0)*	
VII.	**Confidentiality of Data** *(see attached Annex "A" [Detailed Technical Specifications], item 8.0)*	
VIII.	**Terms of Payment** *(see attached Annex "A" [Detailed Technical Specifications], item 9.0)*	

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

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

Annex "A"

DETAILED TECHNICAL SPECIFICATIONS

1. PROJECT TITLE

Subscription to Cyber Security Operations Center (SOC)

2. OBJECTIVES

The Subscription to Cyber SOC aims to:

2.1 Continuously monitor the DBM's network, systems, applications, and digital assets to detect and identify any suspicious or malicious activities, such as unauthorized access, data breaches, malware infections, and other cyber threats;

2.2 Proactively implement preventive measures to stop potential threats before they can cause harm. This involves implementing advanced security technologies, conducting vulnerability assessments, and applying security best practices to reduce the organization's attack surface; and

2.3 Rapidly respond to security incidents to minimize their impact and prevent their escalation. This involves analyzing incidents, identifying their root causes, containing threats, and implementing effective mitigation strategies.

3. DURATION OF THE SUBSCRIPTION

The subscription period for the Project shall be twelve (12) months from the completion of the **Delivery, Integration, and Configuration** phase of the project.

4. QUALIFICATIONS OF THE CONTRACTOR

4.1 The contractor must have at least five (5) years of experience in IT Security industry based on the Securities and Exchange Commission Registration to be submitted as post-qualification requirement.

4.2 The contractor must have a certification that the bidder is an authorized reseller of the brand(s) being offered together with a valid certification from the manufacturer(s) which shall be submitted as a post-qualification requirement.

4.3 The contractor must have a pool of Certified Professionals who will handle DBM SOC monitoring and security incidents, these professionals shall have the following certifications:

4.3.1 Certified Information Security Manager (CISM) or any equivalent certification

4.3.2 CISCO Certified Network Professional (CCNP)

4.3.3 Palo Alto Networks Certified Network Security Administrator (PCNSA)

4.3.4 Fortinet Certified Network Security NE7

4.3.5 COMPTIA Security + or any equivalent security certification

Each of the certification shall belong to a different individual and shall be submitted as post-qualification requirement.

5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK

5.1. **The contractor shall provide SOC solution with at least the following features, but not limited to:**

5.1.1. **SOC**

5.1.1.1. Cloud-native SOC solution that allows two-way integration with the DBM systems, network, data sources, capture of near real-time log data, and must perform correlation between data sources during the investigation. The cloud-native SOC solution shall also be accessible to the DBM and must be capable of the following:

5.1.1.1.1. Security Information and Event Management (SIEM)
5.1.1.1.2. Security Orchestration, Automation, and Response (SOAR)
5.1.1.1.3. Threat Intelligence
5.1.1.1.4. User and Entity Behavior Analytics (UEBA)

5.1.1.2. The SOC platform shall deliver intelligent security analytics and threat intelligence across the enterprise. With the SIEM+SOAR tool, DBM can get a single solution for attack detection, threat visibility, proactive hunting, and threat response which shall be able to:

5.1.1.2.1. Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
5.1.1.2.2. Detect previously undetected threats and minimize false positives using built-in analytics and threat intelligence.
5.1.1.2.3. Investigate threats with artificial intelligence, and hunt for suspicious activities based on the scale of severity.
5.1.1.2.4. Respond to incidents rapidly using built-in orchestration and automation of common tasks.

5.1.1.3. The SOC solution is capable for User and Entity Behavior Analytics (UEBA), which:
5.1.1.3.1 collects logs and alerts from all of its connected data sources;
5.1.1.3.2 Analyzes these logs and alerts; and
5.1.1.3.3 Builds baseline behavioral profiles of DBM entities (such as users, hosts, IP addresses, and applications)

across time and peer group horizon, which shall provide the following information:

- **Use cases** - prioritizes relevant attack vectors and scenarios based on security research as aligned with the MITRE ATT&CK framework of tactics, techniques, and sub-techniques that puts various entities as victims, perpetrators, or pivot points in the kill chain.
- **Data Sources** - selects third-party data sources to provide data that matches the threat scenarios.
- **Analytics** - using various machine learning (ML) algorithms, able to identify anomalous activities and present evidence clearly and concisely in the form of *contextual enrichments*.

5.1.1.4. Present artifacts that will help the DBM security team to get a clear understanding of anomalous activities in context, and in comparison, with the user's baseline profile. The actions performed by a user (or a host, or an address) are evaluated contextually, where a "true" outcome indicates an identified anomaly, as follows:

5.1.1.4.1. across geographical locations, devices, and environments;
5.1.1.4.2. across time and frequency horizons (compared to user's own history);
5.1.1.4.3. as compared to peers' behavior; and
5.1.1.4.4. as compared to organization's behavior.

5.1.1.5. The SOC solution must come with connectors for any data sources that are available out-of-the-box and provide real-time integration. This shall also support common event format (CEF), Syslog, or REST-API to connect data sources which allows for easy integration with third-party security tools and services.

5.1.1.6. The SOC solution should have scalable architecture and should be able to collect data at scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds environments.

5.1.1.7. The SOC solution should provide out-of-the-box, built-in templates to help users to create threat detection rules to notify when something suspicious occurs. It should also have the capability to detect advanced multistage attacks and emerging/unknown threats by applying extended ML analysis

and by correlating a broader scope of anomalous signals, while keeping the alert fatigue low.

5.1.1.8. The SOC solution should provide the ability to create custom query rules to detect threats. The rule should allow the analyst to define tactics and techniques of the MITRE ATT&CK framework.

5.1.1.9. The SOC solution should provide a view of the incident including its severity, summary of the number of entities involved, the raw events that triggered this incident, the incident's unique ID, and any mapped MITRE ATT&CK tactics or techniques.

5.1.1.10. The SOC solution should provide out-of-the-box Security operations efficiency overview to monitor DBM SOC operations using the following metrics:

5.1.1.10.1. Incident created over time
5.1.1.10.2. Incidents created by closing classification, severity, owner, and status
5.1.1.10.3. Mean time to triage
5.1.1.10.4. Mean time to closure
5.1.1.10.5. Incidents created by severity, owner, status, product, and tactics over time
5.1.1.10.6. Time to triage percentiles
5.1.1.10.7. Time to closure percentiles
5.1.1.10.8. Mean time to triage per owner
5.1.1.10.9. Recent activities
5.1.1.10.10. Recent closing classifications

5.1.1.11. The contractor shall set up a cluster-level SOC dashboard to have an integrated and high-level overview of the DBM security posture.

5.1.1.12. The SOC, through the SIEM, shall detect and monitor threats, correlate with threat intelligence sources, generate alerts, conduct investigations, and escalate tickets to the DBM on a 24x7 basis, using the SOC platform, inclusive of the security tools to be provisioned for the DBM.

5.1.1.13. There must be a proper onboarding and integration period between the contractor and the DBM prior to full SOC operation to ensure completeness of SOC visibility and familiarization with the DBM's processes and network behavior.

5.1.1.14. The proposed solution should provide 12-months data retention and unlimited data ingestion.

5.1.1.15. The proposed solution should enroll 1300 assets of DBM which includes Desktop, Laptop, Servers, and Network Equipment.

5.1.1.16. The SOC solution shall have its own ticketing tool for incident ticket generation.

5.1.1.17. The SOC solution shall be able to classify security events based on the following priority levels:

5.1.1.17.1. **Critical (Priority 1):** security events with highest level of severity, posing an immediate and significant threat to DBM's IT system, data, and operations.

5.1.1.17.2. **High (Priority 2):** security events that have a substantial impact on IT resources, potentially affecting critical systems, services, or sensitive data.

5.1.1.17.3. **Medium (Priority 3):** security events that have noticeable impact but may not require immediate action.

5.1.1.17.4. **Low (Priority 4):** security events with minimal immediate impact and lower likelihood of causing significant harm.

5.1.1.18. The SOC Solution shall be able to collect data but not limited to the following risk factors:

5.1.1.18.1. Network Security
5.1.1.18.2. DNS Health
5.1.1.18.3. Patching Cadence
5.1.1.18.4. Endpoint Security
5.1.1.18.5. IP Reputation
5.1.1.18.6. Application Security
5.1.1.18.7. Cubit Score
5.1.1.18.8. Hacker Chatter
5.1.1.18.9. Information Leak
5.1.1.18.10. Social Engineering

5.1.1.19. The cloud SOC platform must guarantee 99.9% uptime/ availability per month, with a monthly downtime cap of 43.2 minutes.

5.1.2. Security Information and Event Management (SIEM)

5.1.2.1. The SOC solution shall provide the DBM, with web-based dashboards for accessing DBM's information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time. The DBM must be

able to request customized dashboards and ad-hoc reports from the contractor.

5.1.2.2. The SIEM should have the capability to seamlessly integrate with Microsoft 365, utilizing XDR for identity, email, endpoint, and multi-cloud functions. Additionally, it should be able to ingest log sources at no additional cost to DBM.

5.1.2.3. The SOC solution shall be capable to support the collection of different types of metadata (e.g., logs, security events, network flows, among others) from data sources and shall include log compression and industry-standard encryption- at rest and in transit- to ensure the security of captured data from disclosure to disinterested parties.

5.1.2.4. The data sources ingested by the SOC solution shall include at least the events from perimeter security tools, active directory logs, endpoint protection, and endpoint detection and response tools, including events from sensors that may be deployed by the solutions provider, if needed.

5.1.2.5. The SOC solution shall have content packs that are prebuilt configurations for common security use cases that provide sets of rules, alarms, baselines, views, reports, variables, and watchlists.

5.1.2.6. The SOC solution shall provide advanced security capabilities, such as User and Entity Behavioral Analytics (UEBA), natively within its own platform.

5.1.2.7. The SOC solution must have a global threat intelligence subscription service for data enrichment to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.

5.1.2.8. The SOC solution must be able to generate and send actionable items to the automation and orchestration tool as well as generate and send alerts to both contractor and DBM analysts and incident responders.

5.1.2.9. The SOC solution must incorporate vulnerability data from a single centralized platform into the SOC service to provide added visibility and security detection.

5.1.2.10. The SOC solution must include unlimited log collection capabilities at no additional cost, circumventing peak event rates, data volume and number of log sources.

5.1.2.11. The SOC solution must allow DBM staff to access the underlying technology and log data.

5.1.3. **Security Orchestration, Automation and Response (SOAR)**

5.1.3.1. The SOC solution should provide built-in SOAR (Security Orchestration, Automation & Response) capability and ability to create playbooks.

5.1.3.2. Supports "no code" methods to rapidly create playbook which supports easy decision making and branching capabilities, as follows:

5.1.3.2.1. Support prebuilt design templates
5.1.3.2.2. Code based logic like JSON
5.1.3.2.3. Support out-of-the-box connectors to save playbook creation time
5.1.3.2.4. Support export of playbooks and reuse it

5.1.3.3. The SOC solution must be integrated with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass.

5.1.3.4. The SOC solution must have visibility into the security operation provided via dashboards, key performance indicators (KPIs), and customizable report.

5.1.3.5. The SOC solution must be able to support machine-driven and analyst-led responses to remediate threats in a consistent and auditable manner.

5.1.3.6. The SOC solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization.

5.1.3.7. The SOC solution must be an open architecture that allows for easy connectivity and integrations to any existing system, bringing them all together into a single, contextual language.

5.1.3.8. The SOC solution must be able to accelerate security incident processes by automating or semi-automating workflows.

5.1.3.9. The SOC solution must include out-of-the-box or *customizable playbooks of best practices* to scale operations, drive consistency in response, and meet compliance requirements. Playbooks deployed shall include at least the following:

5.1.3.9.1 Phishing enrichment and response
5.1.2.9.2 Malware endpoint response

5.1.2.9.3 Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc.)

5.1.2.9.4 Unusual browsing activity

5.1.2.9.5 Web attack profiling and blacklisting

5.1.3.10 The SOC solution shall provide pre-set and customizable KPI metrics to monitor threat response efficacy and team performance.

5.1.3.11 The SOC solution must allow users to customize and develop their own plugins with no limitations to product and/or vendor basis.

5.1.3.12 The SOC solution must provide a bi-directional API access. API usage should not require additional fees.

5.1.3.13 The SOC solution must include an unlimited number of workflows and unlimited number of user role/account with full access.

5.1.4. **Threat Intelligence (TI)**

5.1.4.1. The SOC solution should be able to import threat intelligence by enabling data connectors to various TI platforms and feeds. Users can view and manage the imported threat intelligence in logs.

5.1.4.2. The SOC solution should detect threats and generate security alerts and incidents using the built-in analytics rule templates based on the imported threat intelligence.

5.1.4.3. The SOC solution should be able to import Threat Intelligence by enabling data connector to various TI platforms and feeds.

5.1.4.4. The SOC solution should be able to view and manage the imported threat intelligence.

5.1.4.5. The SOC solution should be able to detect threats and generate security alerts and incidents using the built-in analytics rule templates based on your imported threat intelligence.

5.1.4.6. The SOC solution should be able allow to create new indicator.

5.1.4.7. The SOC solution should be able add indicator in bulk to SIEM Threat Intelligence from CSV or JSON file.

5.1.4.8. The SIEM of the SOC solution should allow the ICTSS security team to flag entities as malicious, right from within the investigation graph, and add it to threat indicator lists.

5.1.4.9. The SOC solution should be able to enrich all imported threat intelligence indicators with Geolocation and *Whois Data*.

5.1.4.10. The SOC solution shall deliver threat intelligence on the following:

5.1.4.10.1 Brand protection - company names/domain
5.1.4.10.1 Social media pages
5.1.4.10.2 External Internet Protocol (IP) addresses
5.1.4.10.3 Website and mobile application monitoring
5.1.4.10.4 VIP e-mails
5.1.4.10.5 Sector monitoring Financial, Government, Insurance, and Healthcare
5.1.4.10.6 GitHub
5.1.4.10.7 Custom queries
5.1.4.10.8 Malicious sites during the duration of the contract (i.e., phishing, social media sites, and others)
5.1.4.10.9 Databases that contain large amounts of data found in the deep and dark web
5.1.4.10.10 Third-party queries
5.1.4.10.11 Investigation
5.1.4.10.12 Threat library

5.1.4.11 The threat intelligence must harvest data from the following open, technical, and closed sources types:

5.1.4.11.1 Mainstream Media (including news, information security sites, vendor research, blogs, and vulnerability disclosures)
5.1.4.11.2 Social Media
5.1.4.11.3 Forums
5.1.4.11.4 Paste Sites
5.1.4.11.5 Code Repositories
5.1.4.11.6 Threat lists (including spam, malware, and malicious infrastructure)
5.1.4.11.7 Dark Web (including multiple tiers of underground communities and marketplaces)
5.1.4.11.8 Original research from in-house human intelligence analysts

5.2 The contractor shall conduct a pre-implementation meeting with DBM representatives within seven (7) calendar days from the receipt of Notice to Proceed (NTP), so that all the necessary preparations, ideal set-up, contractor's familiarization, and other implementation matters are discussed and finalized.

5.3 The contractor shall provide a work plan of activities for the duration of the project and a Deployment and/or Solution Architecture within seven (7) calendar days from the pre-implementation meeting with DBM representatives. Said work plan shall be validated and subject to approval of ICTSS Director.

5.4 The contractor shall deliver, integrate, and configure the SOC Solution (as detailed in item 5.1) within sixty (60) calendar days from the receipt of the NTP.

5.4.1 The contractor shall ensure the availability of the ingested raw logs for at least twelve (12) months with comprehensive searchability. The retention of the logs shall be within the duration of the contract, after which, the logs will be archived and given to the DBM in an agreed format. The logs, including evidence of security incidents, shall be tamper proof and made available for legal and regulatory purposes, as required.

5.4.2 The contractor shall ensure flexibility and scalability of the DBM SOC platform and shall ingest and process all events sent by the DBM for the SIEM and SOAR requirements.

5.4.3 The contractor must include onboarding and advisory services throughout the period of engagement.

5.4.4 The contractor must include strategic and advisory threat intelligence by industry sector.

5.4.5 The contractor shall include continuous monitoring for cybersecurity risk ratings.

5.4.6 The contractor shall provide a cybersecurity risk ratings platform that enables DBM to assess and manage DBM cybersecurity posture. The cybersecurity risk ratings platform shall have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

5.4.7 The contractor shall provide a cybersecurity risk ratings platform that enables DBM to assess and manage third-party vendors / business partners. The cybersecurity risk ratings platform shall have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

5.4.8 The contractor should facilitate a Continual Service Improvement (CSI) workshop to DBM for possible improvement of service through process, people and technology.

5.4.9 The contractor should provide security advisories with the DBM for the cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.

5.4.10 The contractor shall conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on the DBM based on the NIST or CIS Controls.

5.4.11 The contractor shall provide Technical Trainings with certifications to be conducted by an Authorized IT Security Training Centers. The Technical Training should be a classroom type based on the following schedule.

Technical Training	Schedule	No. of Participants	Duration
COMPTIA Security +	Within two (2) month from the receipt of Notice to Proceed	Five (5) ICTSS participants	Forty (40) hours
Certified Ethical Hacker (CEH) v12	Within three (3) month from the receipt of Notice to Proceed.	Five (5) ICTSS participants	Forty (40) hours
Certified Penetration Testing Professional (CPENT)	Within four (4) month from the receipt of Notice to Proceed	Five (5) ICTSS participants	Forty (40) hours

5.4.12 The contractor shall secure appropriate certification from the Authorized IT Security Training Center and issue the same to the DBM-ICTSS participants.

5.5 During the subscription period, the contractor shall provide/render twenty-four (24) hours a day, seven (7) days a week technical support service. Technical support can be delivered in the form of a telephone call, electronic mail, and/or on-site support.

Problems reported/concerns shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report.

5.6 The contractor shall provide *as-built documentation* of the Cyber SOC for the DBM, Infrastructure set-up/ diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the software/IT equipment employed in the project as well as procedures for installation, configuration, integration, usage, backup, and restoration within seven (7) calendar days after the completion of the Delivery, Integration, and Configuration.

5.7 The contractor shall conduct the following on a monthly basis such as but not limited to:

5.7.1 The contractor shall facilitate SOC security briefing at least once a month for the DBM-ICTSS, to present the latest local and international news and updates in Cyber security and latest/new Common Vulnerabilities and Exposure (CVE).

5.7.2 The contractor shall conduct a monthly vulnerability assessment on all DBM's critical and public facing applications/servers. The contractor shall use Common Vulnerability Scoring System (CVSS) version 3.1 or later for risk ranking and prioritizing security vulnerabilities.

5.7.3 The contractor must include regular and special consultation schedule through various communication channels for our staff to reach out to.

5.7.4 The contractor shall submit the following SOC monthly reports within the first week of the succeeding month, subject to ICTSS Security Team approval. These reports should provide insights into the security events, incidents, and trends within the DBM's IT environment. The contractor shall conduct monthly regular review with the ICTSS Security Team, in order to help the DBM-ICTSS make decisions to enhance its security posture and response capabilities.

The SOC monthly report shall include the following:

5.7.4.1 **Incident Report:** This report details out any security incidents, breaches, or unauthorized activities detected and responded to by the SOC team. They include information about the incident's scope, impact, mitigation measures, and lessons learned.

5.7.4.2 **Threat Intelligence Report:** This report provides information about emerging threats, vulnerabilities, malware, and attack trends. They help the DBM stay informed about the current threat landscape and adjust their security measures accordingly.

5.7.4.3 **Vulnerability Assessment Report:** This report details the results of regular vulnerability assessments and penetration tests conducted on the organization's systems and networks. They identify vulnerabilities that need to be addressed to prevent potential breaches.

5.7.4.4 **Log Analysis Report:** This report analyzes logs from various systems, applications, and network devices to identify unusual or suspicious activities. They play a crucial role in detecting and mitigating potential security threats.

5.7.4.5 **User Activity Report:** This report tracks user activity within the organization's network to identify any abnormal or unauthorized behavior. This helps in detecting insider threats and unauthorized access.

5.7.4.6 **Security Incident Response Plans (SIRP) Report:** This report outlines the process followed during the response and recovery phases of security incidents. They include details about incident containment, investigation, communication, and resolution.

5.7.4.7 **Dashboard and Metrics Reports:** This report provides visual representations of key security metrics, such as the number of blocked threats, successful intrusions, incident response times, and trends over time.

5.7.4.8 **Executive Summary Report:** This report provides a high-level overview of the organization's security posture, including notable incidents, risks, and the effectiveness of security measures.

5.7.4.9 **Cyber Security Updates:** This report provides the latest local and international news and updates in Cyber security and new Common Vulnerabilities and Exposure (CVE).

5.8 Threat Hunting and Response

5.8.1 The contractor must provide a 24x7 Threat Hunting Service, supported by experienced and certified analysts or incident responders for the remote response on endpoint incidents/events.

5.8.2 The contractor must have pre-built threat-hunting applications and queries.

5.8.3 The contractor must be able to get context from indicators such as IP's, URL's, domains, or hashes using the tools within the platform, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others).

5.8.4 The SOC solution shall be able to isolate "at-risk" endpoints, including the blocking and the launching of suspicious or malicious applications.

5.8.5 The SOC solution shall allow blacklisting and whitelisting of hashes manually through the solution.

5.8.5.1 The SOC solution shall provide a remote response by administrators, analysts, or incident responders such as *containment, deleting files, and killing process*, among others without the need for additional tools.

5.8.5.2 The SOC solution shall provide root cause analysis of all identified malicious activity.

5.8.5.3 The contractor must be able to:

5.8.5.3.1.1 Detect servers launching phishing attacks and take necessary actions.

5.8.5.3.1.2 Take down fake applications that impersonate legitimate ones.

5.8.5.3.1.3 Take immediate action and provide all the context to execute take-down of malicious servers, websites or social media accounts.

5.9 Incident Response

5.9.1 The contractor shall develop an incident response plan for DBM, outlining roles, responsibilities, communication, and establish an incident response team which would guide the DBM on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines, such as, but not limited to:

5.9.1.1 Escalation process
5.9.1.2 Incident identification process
5.9.1.3 Incident containment process
5.9.1.4 Incident eradication process
5.9.1.5 Incident recovery process
5.9.1.6 Post-incident reporting

5.9.2 The contractor shall map the security playbook and runbooks for applicable security use cases to guide DBM on their incident response.

5.9.3 The contractor shall deliver technical assistance to the DBM Security Team during an emergency (successful) breach response.

5.9.4 The contractor shall have a facility to receive the client's reported incident (via an authorized point of contact from the client) for incidents not captured on the monitoring tool.

5.9.5 The contractor shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.

5.9.6 The contractor shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.

5.9.7 The contractor shall identify indicators of compromise and scan the network to search for other related infected systems.

5.9.8 The contractor shall deliver insider threat investigation.

5.9.9 The contractor shall assist in the following:

5.9.9.1 Incident handling preparation and execution

5.9.9.2 Crisis management

5.9.9.3 Breach communication

5.9.9.4 Forensic analysis including preservation of evidence for chain of custody requirements

5.9.9.5 Remediation

5.9.9.6 The contractor shall respond to any IT security incidents from the time it was reported/detected based on the priority level according to the response time as define below. Incident response can be in the form of telephone call, remote assistance, or onsite support.

Priority Code	Description	Incident Response Time
P1	Critical	30 Minutes
P2	High	1 Hour
P3	Medium	2 Hours
P4	Low	4 Hours

6. SERVICE LEVEL AGREEMENT

The DBM shall maintain a Service Level Agreement with the contractor, with provisions for liquidated damages as indicated below for their non-compliance. Liquidated damages shall be charged against any money due or which may become due to the contractor, or collected from any securities or warranties posted by the contractor.

Component	Description	Liquidated Damages
Delivery, Integration, and Configuration	Within sixty (60) days from the receipt of Notice to Proceed (NTP), as detailed in item 5.4 of this Detailed Technical Specifications	1/10th of 1% of the total contract price shall be imposed per day of delay.
As-built documentation of the Cyber SOC	As detailed in item 5.6 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per day of delay.
SOC Platform Availability	As detailed in item 5.1.1.19 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per minute of downtime.
Technical Support	As detailed in item 5.5 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per hour of delay.

Submission of Monthly Cyber SOC Reports	As detailed in item 5.7.4 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per day of delay.
Incident Response Time	As detailed in item 5.9 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per hour of delay.
Technical Training	As detailed in item 5.4.11 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per day of delay.

7. WARRANTIES OF THE CONTRACTOR

7.1. The contractor warrants that it shall strictly conform to the terms and conditions of this Detailed Technical Specifications.

7.2. The contractor warrants that it shall strictly conform to the terms and conditions of this Detailed Technical Specifications.

7.3. The contractor warrants that the technical staff assigned are qualified to provide the deliverables required to the satisfaction of the DBM.

7.4. The contractor shall secure, and maintain at its own expense all registration, licenses, or permits required by national or local laws and shall comply with the rules, regulations, and directives of regulatory authorities and Commissions.

7.5. The contractor's technical staff assigned to support DBM shall take all necessary precautions for the safety of all persons and properties at or near their area of work and shall comply with all the standard and established safety regulations, rules and practices.

7.6. The contractor's technical staff assigned to support DBM shall coordinate with the ICTSS in the implementation of this project.

7.7. The contractor shall be liable for loss, damage, or injury caused directly or indirectly through the fault or negligence of its technical staff assigned. It shall assume full responsibility therefore and the DBM shall be fully released from any liability arising therefrom.

7.8. The contractor shall neither assign, transfer, pledge, nor subcontract any part of or interest on the contract.

7.9. The contractor shall identify the certified technical staff who will be given authority to access and operate the specified equipment. The DBM, through the

ICTSS, shall be informed within five (5) calendar days, through a formal notice, of any change or replacement of technical staff assigned.

8. CONFIDENTIALITY OF DATA

8.1. All technical staff assigned by the contractor shall be required to sign a Non-Disclosure Agreement (NDA) before the implementation of the Project.

8.2. The DBM Enterprise Network System, its component, parts and all products, product samples and specifications, data, ideas, technology, and technical/non-technical materials, all or any which may be derived from any of the foregoing are strictly confidential.

8.3. The contractor agrees to hold all the foregoing information in strict confidence. The contractor further agrees not to reproduce or disclose any confidential information to third parties without the prior written approval of the DBM.

9. TERMS OF PAYMENT

9.1 Monthly payment shall be made, subject to the submission of the following documentary requirements, and in accordance with budgeting, accounting, and auditing laws, rules, and regulations:

- 9.1.1 As-built documentation in accordance to item 5.6 of the Detailed Technical Specifications
- 9.1.2 NDA in accordance to item 8.1 of the Detailed Technical Specification
- 9.1.3 SOC Monthly Report, which shall include the following:
  - Incident Report
  - Threat Intelligence Report
  - Vulnerability Assessment Report
  - Log Analysis Report
  - User Activity Report
  - Security Incident Response Plans (SIRP) Report
  - Dashboard and Metric Report
  - Executive Summary Report
  - Cyber Security Update
- 9.1.4 Sales Invoice / Billing Statement
- 9.1.5 Training Certificates and Training Materials in accordance to the item 5.4.11 of the Detailed Technical Specifications
- 9.1.6 Certificate of Acceptance issued by the DBM- ICTSS to be issued on a Monthly basis

9.2 Payment shall cover the subscription period in accordance with item 3.0 of the Detailed Technical Specifications.

Section VIII. Checklist of Technical and Financial Documents

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

☐ (a) Valid and updated PhilGEPS Registration Certificate (Platinum Membership) (all pages) in accordance with Section 8.5.2. of the 2016 Revised IRR of RA No. 9184;

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 Schedule of Requirements, which may include production/delivery schedule, and/or warranty period requirements, if applicable; **and**

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

☐ (g) 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

☐ (h) 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

☐ (i) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence; **or** duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

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

☐ (j) *[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.

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

II. FINANCIAL COMPONENT ENVELOPE

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

Statement of all Ongoing Government and Private Contracts Including Contracts Awarded but not yet Started

[shall be submitted with the Bid]

Business Name: _____
Business Address:_____

Name of Client/Contact Person/Contact Number/Contact Email Address	**Date of the Contract**	**Title of the Contract / Name of the Project**	**Kinds of Goods**	**Total Amount of Contract**	**Value of Outstanding Contract**	**Date of Delivery**
Government						
Private						

Submitted by : _____
(Printed Name and Signature)
Designation : _____

Date : _____

Instructions:

i. State **ALL** ongoing contracts including those awarded but not yet started (government **[including the DBM]** and private contracts which may be **similar or not similar** to the project being bidded) up to November 6, 2023.

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

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

iv. Please note that item 6.4 of the Government Procurement Policy Board (GPPB) Circular No. 04-2020 dated September 16, 2020 states that, "[t]he PEs shall check **compliance of the submitted forms with the mandatory provisions stated above**. **Non-submission of the Required Forms or non-inclusion of the mandatory provisions in any of the Required Forms shall be a ground for disqualification**."

Moreover, GPPB Non-Policy Matter Opinion No. 041-2014 dated October 9, 2014 partially states that "**even contracts that include non-disclosure agreements or confidentiality clauses are required to be disclosed**. It is likewise good to clarify that the requirement refers to a "statement" to be made by the bidder relative to all its ongoing and private contracts, and not the actual submission of the physical contracts."

Statement of Single Largest Completed Contract which is Similar in Nature

[shall be submitted with the Bid]

Business Name: _____
Business Address:_____

Name of Client/Contact Person/Contact Number/Contact Email Address	Date of the Contract	Title of the Contract / Name of the Project	Kinds of Goods	Amount of Contract	Date of Acceptance *	End User's Acceptance or Official Receipt(s) Issued for the Contract

Submitted by : _____
(Printed Name and Signature)

Designation : _____

Date : _____

Instructions:

a. 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 following requirements:
   i. a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC; **OR**
   ii. at least two (2) similar contracts:
      (a) the aggregate amount of which should be equivalent to at least fifty percent (50%) of the ABC for this Project; **AND**
      (b) the largest of these similar contracts must be equivalent to at least half of the percentage of the ABC as required above (i.e., twenty-five percent [25%]).
b. The SLCC should have been completed (i.e., accepted) within the period of **November 7, 2020 to November 6, 2023.**
c. The similar contract for this Project shall refer to the comprehensive design, implementation, and management of a Security Operation Center (SOC). If the comprehensive design, implementation, and management of a SOC form part of a bigger contract, only the cost component of the comprehensive design, implementation, and management of a SOC shall be considered for purposes of comparing the value thereof to at least fifty percent (50%) of the ABC.

d. Please note that item 6.4 of the Government Procurement Policy Board (GPPB) Circular No. 04-2020 dated September 16, 2020 states that, "[t]he PEs shall check **compliance of the submitted forms with the mandatory provisions stated above**. **Non-submission of the Required Forms or non-inclusion of the mandatory provisions in any of the Required Forms shall be a ground for disqualification**."

   Moreover, GPPB Non-Policy Matter Opinion No. 041-2014 dated October 9, 2014 partially states that "**even contracts that include non-disclosure agreements or confidentiality clauses are required to be disclosed**. It is likewise good to clarify that the requirement refers to a "statement" to be made by the bidder relative to all its ongoing and private contracts, and not the actual submission of the physical contracts."

* Date of Acceptance shall mean the date when the items delivered have **satisfactorily met** the requirements of the procuring entity, as evidenced by either a Certificate of Final Acceptance/Completion from the bidder's client, or an Official Receipt or a Sales Invoice (to be submitted during post-qualification).

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.: ***DBM-2024-05***

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 before me in [place of execution], Philippines on this [date of notarization], affiant exhibiting before me his competent evidence of identity [valid identification issued by the government].

NOTARY PUBLIC

Doc. No. _____;
Page No. _____;
Book No. _____;
Series of _____.

Omnibus Sworn Statement

[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, procurement agent if engaged, 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, procurement agent if engaged, 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, procurement agent if engaged, 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 before me in [place of execution], Philippines on this [date of notarization], affiant exhibiting before me his competent evidence of identity [valid identification issued by the government].

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. : **DBM-2024-05**

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 **Subscription to Cyber Security Operations Center** 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 details provided herein and made part of this Bid. The total bid price includes the cost of all taxes.

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.

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, 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: _____

CONTRACT No. 2024-___
NAME OF PROJECT

CONTRACT AGREEMENT

THIS AGREEMENT made this _____ day of _____ 20_____ between the **DEPARTMENT OF BUDGET AND MANAGEMENT** of the Philippines (hereinafter called "the Entity") of the one part and _____ of _____ City, Philippines (hereinafter called "the Supplier") of the other part;

WHEREAS, the Entity invited Bids for certain goods and ancillary services, particularly _____, and has accepted a Bid by the Supplier for the supply of those goods and services in the sum of _____ Pesos (P_____) (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

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

2. The following documents as required by the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of this Agreement, *viz.*:

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

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

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

   iii. Performance Security;

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

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

3. In consideration for the sum of _____ (P_____) or such other sums as may be ascertained, _____ agrees to deliver the _____ in accordance with his/her/its Bid.

4. The **DEPARTMENT OF BUDGET AND MANAGEMENT** agrees to pay the above-mentioned sum in accordance with the terms of the Bidding.

5. The period for the performance of the obligations under this Contract shall not go beyond the validity of the appropriation for this Project.

6. In compliance with item 4.3 of Appendix 33 of the 2016 Revised IRR of RA No. 9184 and consistent with Administrative Order No. 34, s. 2020 (Directing Strict Compliance By All Agencies and Instrumentalities of the Executive Department with Transparency, Accountability and Good Governance Policies and Measures in the Procurement Process), the DBM shall publish in its official website and social media platform the following post-award information:

   (a) Project name;
   (b) Approved budget for the contract;
   (c) Contract period;
   (d) Name of the winning bidder and its official business address;
   (e) Amount of contract awarded;
   (f) Date of award and acceptance; and
   (g) Implementing office/unit/division/bureau of the concerned agency or instrumentality.

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

_____	_____
Secretary	*Authorized Representative*
	for:
for:	_____
DEPARTMENT OF BUDGET AND MANAGEMENT	

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
CITY OF MANILA) *S.S.*

BEFORE ME, a Notary Public for and in the City of _____, Philippines on this _____ day of _____, 2024 personally appeared the following:

NAME	**VALID ID**	**VALID UNTIL**
_____	DBM ID No. ___	
_____		

known to me to be the same persons who executed the foregoing Contract and who acknowledged to me that the same is their free and voluntary act and deed and of the entities they respectively represent.

This CONTRACT for the _____ was signed by the parties on each and every page thereof.

WITNESS MY HAND AND SEAL this ____ day of _____, 2024.

Doc. No _____;
Page No _____;
Book No _____;
Series of 2024.


Republic of the Philippines
gppb
Government Procurement Policy Board