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

Procurement of GOODS

Subscription to Cyber Security Operations Center (SOC)

Project ID No. **DBM-2025-44**

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 (SOC)"

1. The Department of Budget and Management (DBM), through the FY 2025 General Appropriations Act and the Multi-Year Contractual Authority No. MYCA-BMB-C-24-0000094, intends to apply the sum of **One Hundred Fifty-Three Million Pesos (P153,000,000.00)** being the Approved Budget for the Contract (ABC) to payments under the contract for the "**Subscription to Cyber Security Operations Center (SOC)**" (Project ID No. **DBM-2025-44)** covering FYs 2025 to 2028, with the breakdown of ABC as follows:

Year	ABC
FY 2025	Forty-Two Million Eight Hundred Forty Thousand Pesos (P42,840,000.00)
FY 2026	Fifty-One Million Pesos (P51,000,000.00)
FY 2027	Fifty-One Million Pesos (P51,000,000.00)
FY 2028	Eight Million One Hundred Sixty Thousand Pesos (P8,160,000.00)

The period for the performance of the obligations under the Contract shall not go beyond the validity of the corresponding appropriations 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 August 5, 2020 to August 4, 2025** a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

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

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

4. Prospective Bidders may obtain further information from 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 July 15, 2025 from the given address and website below and upon payment of a fee in the amount of Fifty Thousand Pesos (P50,000.00). 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 for this Project on July 22, 2025, 1:30 p.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.

   Prior to this, the DBM-BAC will likewise conduct a preliminary audio-visual presentation on the same day, July 22, 2025, 1:00 p.m., **via video conferencing or webcasting**, which shall be open to all prospective bidders. The presentation will discuss the bidding process, the documentary requirements to be submitted, and other matters relevant to the Project.

   In case of video conferencing or webcasting, the prospective bidders are advised to first log in the BAC waiting room, **https://bit.ly/DBM-BAC-WaitingRoom**, 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 both the preliminary audio-visual presentation and the main Pre-Bid Conference.

7. Bids must be duly received by the BAC Secretariat or the DBM-Administrative Service (AS)-Central Records Division through manual submission at the office address indicated below on or before August 5, 2025, 9:00 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 August 5, 2025, 9:00 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://bit.ly/DBM-BAC-WaitingRoom**, 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
11. 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.

12. For further information, please refer to:

    DBM-BAC Secretariat
    DBM-AS-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

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

July 15, 2025

[redacted]
Digitally signed by
Gerardo E. Maula

GERARDO E. MAULA
Chairperson, DBM-BAC [redacted]

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 (SOC)**" with Project Identification No. *DBM-2025-44.*

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 FYs 2025 to 2028 in the amount of **One Hundred Fifty-Three Million Pesos (P153,000,000.00)** covering FYs 2025 to 2028, with the breakdown of ABC as follows:

Year	ABC
FY 2025	Forty-Two Million Eight Hundred Forty Thousand Pesos (P42,840,000.00)
FY 2026	Fifty-One Million Pesos (P51,000,000.00)
FY 2027	Fifty-One Million Pesos (P51,000,000.00)
FY 2028	Eight Million One Hundred Sixty Thousand Pesos (P8,160,000.00)

The period for the performance of the obligations under the Contract shall not go beyond the validity of the corresponding appropriations for the Project.

2.2. The source of funding is the FY 2025 General Appropriations Act and the Multi-Year Contractual Authority No. MYCA-BMB-C-24-0000094.

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, **or**

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%) (in the case of non-expendable supplies and services) or twenty-five percent (25%) (in the case of expendable supplies) 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 July 22, 2025, 1:30 p.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**.

Prior to this, the DBM-BAC will likewise conduct a preliminary audio-visual presentation on the same day, July 22, 2025, 1:00 p.m., **via video conferencing or webcasting**, which shall be open to all prospective bidders. The presentation will discuss the bidding process, the documentary requirements to be submitted, and other matters relevant to the Project.

In case of video conferencing or webcasting, the prospective bidders are advised to first log in the BAC waiting room, **https://bit.ly/DBM-BAC-WaitingRoom**, 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 both the preliminary audio-visual presentation and 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 August 5, 2020 to August 4, 2025**.

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 **December 3, 2025**. 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 14 shall be submitted for each lot or item separately.

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

19.4. The Project shall be awarded as 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 supply, implementation, and/or services of a cyber/information security operations center which may include deployment of related cyber security tools/technologies such as Security Information and Event Management (SIEM), Firewalls, Security Orchestration, Automation and Response (SOAR), Endpoint Detection and Response (EDR) and/or services such as cyber security monitoring services, threat intelligence, forensics, cyber security incident response/management, cyber security administration. If the supply, implementation, and/or services of a cyber/information security operations center which may include deployment of related cyber security tools/technologies such as SIEM, Firewalls, SOAR, EDR and/or services such as cyber security monitoring services, threat intelligence, forensics, cyber security incident response/management, cyber security administration form part of a bigger contract, only the cost component of the supply, implementation, and/or services of a cyber/information security operations center which may include deployment of related cyber security tools/technologies such as SIEM, Firewalls, SOAR, EDR and/or services such as cyber security monitoring services, threat intelligence, forensics, cyber security incident response/management, cyber security administration 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 August 5, 2020 to August 4, 2025**.
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.

`

	Bidders are advised to provide bid prices with exact values. During the conduct of bid evaluation, only the total calculated bid price shall be rounded off to the nearest hundredths [two (2) decimal places].
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 P3,060,000.00, 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 P7,650,000.00, 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. Latest Income and Business Tax Returns, filed and paid through the Electronic Filing and Payment System (EFPS), consisting of the following:

`

	i. 2024 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 January 2025 to June 2025. 2. In case the Mayor's/Business permit mentioned in the PhilGEPS certificate is recently expired, the renewed permit shall be submitted in accordance with Section 34.2 of the IRR of RA No. 9184. The bidder with the LCB is likewise requested to present the following documents during post-qualification: 1. Photocopy/ies of Contract/s or Purchase Order/s of one of the following: 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%]). 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. The copy of Securities and Exchange Commission Registration showing that the Service Provider must have at least five (5) years of experience in providing IT security services. 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. The Service Provider must have at least an aggregate of ten (10) unique and distinct certifications from the list below, belonging to at least five (5) locally employed certified professionals: i. ISC2 Information Systems Security Engineering Professional (ISSEP) ii. ISC2 Information Systems Security Management Professional (ISSMP) iii. ISC2 Certified Information Systems Security Professional (CISSP) iv. ISC2 Certified Cloud Security Professional (CCSP)

`

	v. ITIL v4 Foundation vi. CompTIA Cybersecurity Analyst+ (CySA+) vii. CompTIA Security+ CE viii. CompTIA Security Analytics Professional (CSAP) ix. Security Blue Team Level 1 (BTL1) x. Security Blue Team Level 2 (BTL2) xi. Certified CyberDefender (CCD) xii. SANS GIAC Cyber Threat Intelligence (GCTI) xiii. SANS GIAC Continuous Monitoring (GMON) xiv. SANS GIAC Certified Security Essentials (GSEC) xv. SANS GIAC Certified Detection Analyst (GCDA) xvi. SANS GIAC Certified Intrusion Analyst (GCIA) xvii. SANS GIAC Certified Incident Handler (GCIH) xviii. SANS GIAC Enterprise Incident Responder (GEIR) xix. SANS GIAC Certified Network Forensics Analyst (GNFA) xx. SANS GIAC Certified Advanced Smartphone Forensics (GASF) xxi. SANS GIAC Certified Forensics Analyst (GCFA) xxii. SANS GIAC Certified Cloud Forensics Responder (GCFR) xxiii. SANS GIAC Cloud Security Automation (GCSA) xxiv. eLearnSecurity Certified Incident Responder (eCIR) xxv. eLearnSecurity Certified Digital Forensic Professional (eCDFP) <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 VII (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

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

5. Warranty

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

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

6. Liability of the Supplier

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

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

Section V. Special Conditions of Contract

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 Functional Group Head of the Information and Communications Technology Group and 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	Milestone payments shall be made in accordance with item 11 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications. Pursuant to the Bureau of Internal Revenue Regulation No. 017-2024, the Supplier shall present their valid and updated Tax Clearance Certificate to the End-user Unit, prior to the final payment of the contract. Failure to present a valid and updated Tax Clearance Certificate shall entitle the DBM to suspend the final payment due to the Supplier.
4	The conduct of annual performance evaluation of the service provider shall be in accordance with item 12 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications. 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.
5	In order to assure that manufacturing defects shall be corrected by the supplier, a warranty security shall be required from the supplier for a minimum period of three (3) months, in case of expendable supplies, or a minimum period of one (1) year, in case of non-expendable supplies, after acceptance of the DBM of the delivered goods. The obligation for the warranty shall be covered by either a retention money in an amount equivalent to one percent (1%) of every progress payment, or a special bank guarantee equivalent to one percent (1%) of the total contract price. The said amount shall be released after the lapse of the warranty period, or, in the case of expendable supplies, after consumption thereof: Provided, however, that the supplies delivered are free from patent and latent defects and all the conditions imposed under the contract have been fully met.

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	Conduct of Pre-implementation Meeting/s	Within ten (10) calendar days from receipt of the Notice to Proceed (NTP)
2	Provision of Work Plan of Activities	Within seven (7) calendar days upon successful conclusion of the pre-implementation meeting/s but not more than thirty (30) days from receipt of NTP
3	**Delivery, Integration, and Configuration of the Cyber Security Operations Center (SOC)**, as detailed in Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Within sixty (60) calendar days from receipt of the NTP and approval of the work plan of activities
4	**Submission of As-built Documentation of the Cyber SOC**, as detailed in Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Within seven (7) calendar days from the completion of the delivery, integration, and configuration of the Cyber SOC
5	**Issuance of Proof of Subscription**	Within seven (7) calendar days from the completion of the delivery, set-up, installation, integration, and configuration of the Cyber SOC
6	**Subscription to Cyber Security Operations**, as detailed in item 3 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Thirty-six (36) months from the issuance of Proof of Subscription
7	**Technical Trainings**, as detailed in Attachment 2 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	As detailed in Attachment 2 of Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications

Item	Description	Delivery Schedule
8	**Submission of Cyber SOC Monthly Reports**, as detailed in Annex "A" (Detailed Technical Specifications) of Section VII. Technical Specifications	Within the fifth (5^{th}) working day of the succeeding months

* The period for the performance of the obligations under the Contract shall not be beyond the validity of the corresponding appropriations 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.	**Subscription Period** *(see attached Annex "A" [Detailed Technical Specifications], item 3.0)*	
II.	**Qualifications of the Service Provider** *(see attached Annex "A" [Detailed Technical Specifications], item 4.0)*	
III.	**Technical Requirements for Cyber SOC Solution** *(see attached Annex "A" [Detailed Technical Specifications], item 5.0)*	
IV.	**Scope of Work and Services** *(see attached Annex "A" [Detailed Technical Specifications], item 6.0)*	
V.	**Service Level Agreement** *(see attached Annex "A" [Detailed Technical Specifications], item 7.0)*	
VI.	**Warranties of the Service Provider** *(see attached Annex "A" [Detailed Technical Specifications], item 8.0)*	
VII.	**Confidentiality of Data** *(see attached Annex "A" [Detailed Technical Specifications], item 9.0)*	
VIII.	**Data Sovereignty** *(see attached Annex "A" [Detailed Technical Specifications], item 10.0)*	
IX.	**Terms of Payment** *(see attached Annex "A" [Detailed Technical Specifications], item 11.0)*	
X.	**Performance Review and Assessment** *(see attached Annex "A" [Detailed Technical Specifications], item 12.0)*	

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 Provide a solution to 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, monitoring and analysis of logs, assessment of threat indicators, and applying security best practices to reduce the DBM'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. SUBSCRIPTION PERIOD

The subscription period for the Project shall be thirty-six (36) months from the issuance of Proof of Subscription. The Proof of Subscription shall only be issued by the Service Provider within seven (7) calendar days after the complete set up, installation, and configuration of all licenses for all environments.

The delivery, integration, and configuration of the Cyber Security Operations Center (SOC) must be completed within sixty (60) calendar days from the receipt of the Notice to Proceed (NTP).

4. QUALIFICATIONS OF THE SERVICE PROVIDER

4.1. The Service Provider must have at least five (5) years of experience in providing IT security services.

Note: A copy of the Securities and Exchange Commission Registration is requested to be submitted during post-qualification.

4.2. The Service Provider must have a certification that the bidder is an authorized partner/reseller of the solution/brand(s) being offered together with a valid certification from the manufacturer(s).

Note: The certification that the bidder is an authorized reseller of the brand(s) being offered together with a valid certification from the manufacturer(s) are requested to

be submitted during post-qualification.

4.3. The Service Provider shall undergo a Proof of Concept (PoC) of the proposed submitted solution that includes testing the compliance to the technical requirements and competencies of the Service Provider to deliver the services defined on the scope of work.

4.3.1. An executed Non-Disclosure Agreement (NDA) must be submitted by the service provider at least two (2) working days prior to the commencement of the PoC.

4.3.2. All PoC preparations, including the setup and configuration of the PoC environment must be configured at least two (2) working days before the scheduled start of the live PoC demonstration.

Note: The PoC is requested to be demonstrated during the post-qualification.

4.4. The Service Provider must have a pool of locally employed Certified Professionals who will handle the DBM Cyber SOC monitoring and security incidents, these professionals shall have at least any of the following certifications which are requested to be submitted as part of the post qualification requirement. The Service Provider must have at least an aggregate of ten (10) unique and distinct certifications from the list below belonging to at least five (5) locally employed certified professionals. **Only distinct certifications will be counted toward the total.** (*see examples below in illustration 1*)

4.4.1. ISC2 Information Systems Security Engineering Professional (ISSEP)
4.4.2. ISC2 Information Systems Security Management Professional (ISSMP)
4.4.3. ISC2 Certified Information Systems Security Professional (CISSP)
4.4.4. ISC2 Certified Cloud Security Professional (CCSP)
4.4.5. ITIL v4 Foundation
4.4.6. CompTIA Cybersecurity Analyst+ (CySA+)
4.4.7. CompTIA Security+ CE
4.4.8. CompTIA Security Analytics Professional (CSAP)
4.4.9. Security Blue Team Level 1 (BTL1)
4.4.10. Security Blue Team Level 2 (BTL2)
4.4.11. Certified CyberDefender (CCD)
4.4.12. SANS GIAC Cyber Threat Intelligence (GCTI)
4.4.13. SANS GIAC Continuous Monitoring (GMON)
4.4.14. SANS GIAC Certified Security Essentials (GSEC)
4.4.15. SANS GIAC Certified Detection Analyst (GCDA)
4.4.16. SANS GIAC Certified Intrusion Analyst (GCIA)
4.4.17. SANS GIAC Certified Incident Handler (GCIH)
4.4.18. SANS GIAC Enterprise Incident Responder (GEIR)
4.4.19. SANS GIAC Certified Network Forensics Analyst (GNFA)
4.4.20. SANS GIAC Certified Advanced Smartphone Forensics (GASF)
4.4.21. SANS GIAC Certified Forensics Analyst (GCFA)
4.4.22. SANS GIAC Certified Cloud Forensics Responder (GCFR)
4.4.23. SANS GIAC Cloud Security Automation (GCSA)
4.4.24. eLearnSecurity Certified Incident Responder (eCIR)
4.4.25. eLearnSecurity Certified Digital Forensic Professional (eCDFP)

Example 1	
Person 1	ISC2 Information Systems Security Engineering Professional (ISSEP)
	ISC2 Certified Information Systems Security Professional (CISSP)
	ITIL v4 Foundation
	CompTIA Security+ CE
	Certified CyberDefender (CCD)
	SANS GIAC Continuous Monitoring (GMON)
Person 2	SANS GIAC Cyber Threat Intelligence (GCTI)
Person 3	eLearnSecurity Certified Incident Responder (eCIR)
Person 4	CompTIA Security Analytics Professional (CSAP)
Person 5	ISC2 Certified Cloud Security Professional (CCSP)

Example 2	
Person 1	ISC2 Information Systems Security Engineering Professional (ISSEP)
	ISC2 Information Systems Security Management Professional (ISSMP)
Person 2	ISC2 Certified Information Systems Security Professional (CISSP)
	ISC2 Certified Cloud Security Professional (CCSP)
Person 3	ITIL v4 Foundation
	CompTIA Cybersecurity Analyst+ (CySA+)
Person 4	SANS GIAC Cyber Threat Intelligence (GCTI)
	SANS GIAC Continuous Monitoring (GMON)
Person 5	Security Blue Team Level 1 (BTL1)
	Security Blue Team Level 2 (BTL2)

Example 3	
Person 1	ISC2 Information Systems Security Engineering Professional (ISSEP)
Person 2	ISC2 Information Systems Security Management Professional (ISSMP)
Person 3	ISC2 Certified Information Systems Security Professional (CISSP)
Person 4	ISC2 Certified Cloud Security Professional (CCSP)
Person 5	ITIL v4 Foundation
Person 6	CompTIA Cybersecurity Analyst+ (CySA+)
Person 7	CompTIA Security+ CE
Person 8	CompTIA Security Analytics Professional (CSAP)
Person 9	Security Blue Team Level 1 (BTL1)
Person 10	Security Blue Team Level 2 (BTL2)

Example 4	
Person 1	ISC2 Information Systems Security Engineering Professional (ISSEP)
	ISC2 Certified Information Systems Security Professional (CISSP)
	ISC2 Certified Cloud Security Professional (CCSP)
Person 2	CompTIA Security+ CE
	Security Blue Team Level 1 (BTL1)
	SANS GIAC Cyber Threat Intelligence (GCTI)
	ISC2 Information Systems Security Engineering Professional (ISSEP)
	ISC2 Certified Information Systems Security Professional (CISSP)
	ISC2 Certified Cloud Security Professional (CCSP)
Person 3	ISC2 Certified Cloud Security Professional (CCSP)
	SANS GIAC Certified Security Essentials (GSEC)
	SANS GIAC Certified Detection Analyst (GCDA)
Person 4	ISC2 Certified Cloud Security Professional (CCSP)
	SANS GIAC Certified Network Forensics Analyst (GNFA)
	SANS GIAC Certified Advanced Smartphone Forensics (GASF)
Person 5	SANS GIAC Cyber Threat Intelligence (GCTI)
	eLearnSecurity Certified Incident Responder (eCIR)

Illustration 1

5. TECHNICAL REQUIREMENTS FOR CYBER SOC SOLUTION

The Service Provider shall provide the Cyber SOC solution with the functionalities as provided below in **Attachment 1** and made an integral part of this DTS document.

6. SCOPE OF WORK AND SERVICES

6.1. The details of the Scope of Work and Services that will be provided by the Service Provider is provided below in **Attachment 2** and made an integral part of this document.

7. SERVICE LEVEL AGREEMENT

The DBM shall maintain a Service Level Agreement with the Service Provider. Below is the liquidated damages for the non-compliance of the Service Provider which shall be charged against any money due, or which may become due to the Service Provider, or collected from any securities or warranties posted by the Service Provider.

Component	Description	Liquidated Damages
Delivery, Integration, and Configuration	Within sixty (60) calendar days from the receipt of Notice to Proceed (NTP), as detailed in **Attachment 1** of this Detailed Technical Specifications (DTS)	One tenth ($1/10^{th}$) of one percent (1%) of the total contract price shall be imposed per day of delay.

As-built documentation of the Cyber SOC	As detailed in **Attachment 2** of this DTS	One tenth ($1/10^{th}$) of one percent (1%) of the monthly payment shall be imposed per day of delay.
Cyber SOC Solution Availability	As detailed in **Attachment 2** of this DTS	One tenth ($1/10^{th}$) of one percent (1%) of the monthly payment shall be imposed per minute of downtime.
Submission of Monthly Cyber SOC Reports	As detailed in **Attachment 2** of this DTS	One tenth ($1/10^{th}$) of one percent (1%) of the monthly payment shall be imposed per day of delay.
Incident Response Time	As detailed in **Attachment 2** of this DTS	One tenth ($1/10^{th}$) of one percent (1%) of the monthly payment shall be imposed per hour of delay.
Technical Training	As detailed in **Attachment 2** of this DTS	One tenth ($1/10^{th}$) of one percent (1%) of the monthly payment shall be imposed per day of delay.

8. WARRANTIES OF THE SERVICE PROVIDER

8.1. The Service Provider warrants that it shall strictly conform to the terms and conditions of this DTS.

8.2. The Service Provider warrants that the technical staff assigned are qualified to provide the deliverables required to the satisfaction of the DBM.

8.3. The Service Provider 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.

8.4. The Service Provider's technical staff assigned to support the 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.

8.5. The Service Provider's technical staff assigned to support the DBM shall coordinate with the Information and Communications Technology Systems Service (ICTSS) and/or the designated lead in the implementation of this project.

8.6. The Service Provider 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.

8.7. The Service Provider shall neither assign, transfer, pledge, nor subcontract any part of or interest on the contract.

8.8. The Service Provider shall identify the certified technical staff who will be given authority to access and operate the specified equipment. The DBM, through the Office of the Chief Information Officer (OCIO) shall be informed within five (5) calendar days, through a formal notice, of any change or replacement of technical staff assigned.

8.9. In order to assure that manufacturing defects shall be corrected by the supplier, a warranty security shall be required from the supplier for a minimum period of three (3) months, in case of expendable supplies, or a minimum period of one (1) year, in case of non-expendable supplies, after acceptance of the DBM of the delivered goods.

The obligation for the warranty shall be covered by either a retention money in an amount equivalent to one percent (1%) of every progress payment, or a special bank guarantee equivalent to one percent (1%) of the total contract price.

The said amount shall be released after the lapse of the warranty period, or, in the case of expendable supplies, after consumption thereof: Provided, however, that the supplies delivered are free from patent and latent defects and all the conditions imposed under the contract have been fully met.

9. CONFIDENTIALITY OF DATA

9.1. All personnel assigned by the Service Provider shall be required to sign a NDA before the implementation of the Project.

9.2. The DBM Enterprise 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.

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

10. DATA SOVEREIGNTY

10.1. The DBM subject to conditions prescribed by the Law of the Republic of the Philippines with regards to data residency and sovereignty laws, retains control and ownership of all data stored or processed during the subscription period.

10.2. All DBM Data stored in the Service Provider's solution shall be the sole property

of the DBM. This data can be retrieved anytime upon request of the DBM and has the sole right and authority to copy, move, delete, or transfer it to other systems/locations.

10.3. Except as otherwise permitted under Philippine law, no data shall be subject to foreign laws, or be accessible to other countries, regardless of the system used, the nationality of the Service Provider, or the data's place of storage, processing, or transmission. No rights appurtenant to such data shall be deemed transferred or assigned by virtue of the storage, processing, or transmission thereof by the Service Provider.

10.4. The Service Provider must agree and ensure that the data stored in the proposed solution will remain within it and will not be transferred without the knowledge and permission of the DBM.

11. TERMS OF PAYMENT

Milestone payments shall be made (Table 1), subject to the submission of the following documentary requirements, and in accordance with budgeting, accounting, and auditing laws, rules, and regulations:

Table 1. Milestone Payments

Year	Milestone	Required Outputs and Supporting Documents	Payment
1	Configuration and Technical Maintenance	• As-built documentation in accordance with **Attachment 2** of the DTS for one time submission; • SOC Monthly Reports, as detailed in **Attachment 2** of the DTS; • SOC Training Certificates and Training Materials in accordance with **Attachment 2** of the DTS submitted upon training completion. • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the Functional Group Head (FGH) of the Information and Communications Technology (ICT) Group and Chief Information	Annual Payment for Year 1 (33.33% of the total contract cost) and shall be payable in four (4) tranches, as follows: **First Tranche** (25% of the contract cost for Year 1) - within the 1st quarter of Year 1 upon submission of the required outputs and supporting documents. **Second Tranche** (25% of the contract cost for Year 1) - within the 2nd quarter of Year 1 upon submission of the required outputs and supporting documents. **Third Tranche** (25% of the contract cost for Year

Year	Milestone	Required Outputs and Supporting Documents	Payment
		Officer; • NDA; and • Valid and updated Tax Clearance Certificate.	1) - within the 3rd quarter of Year 1 upon submission of the required outputs and supporting documents. **Fourth Tranche** (25% of the contract cost for Year 1) - within the last month of Year 1, upon submission of the required outputs and supporting documents.
2	Configuration and Technical Maintenance	• SOC Monthly Reports, as detailed in **Attachment 2** of the DTS • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the FGH of the ICT Group and Chief Information Officer; • Valid and updated Tax Clearance Certificate • Submission of Annual Status and Progress Report of the Year 1 subscription; and • Performance Review and Assessment Results Document from End-User Representatives in accordance with Item 8 of the DTS. • Valid and updated Tax Clearance Certificate	Payment for Year 2 (33.33% of the total contract cost) and shall be payable in four (4) tranches, as follows: **First Tranche** (25% of the contract cost for Year 2) - within the 1st quarter of Year 2 upon submission of the required outputs and supporting documents. **Second Tranche** (25% of the contract cost for Year 2) - within the 2nd quarter of Year 2 upon submission of the required outputs and supporting documents. **Third Tranche** (25% of the contract cost for Year 2) - within the 3rd quarter of Year 2 upon submission of the required outputs and supporting documents. **Fourth Tranche** (25% of the contract cost for Year 2) - within the last month

Year	Milestone	Required Outputs and Supporting Documents	Payment
			of Year 2, upon submission of the required outputs and supporting documents.
3	Configuration and Technical Maintenance	• SOC Monthly Reports as detailed in Attachment **2** of the DTS • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the FGH of the ICT Group and Chief Information Officer; • Valid and updated Tax Clearance Certificate • Submission of Annual Status and Progress Report of the Year 2 subscription; • Submission of Completion Report of the Year 3 subscription; and • Performance Review and Assessment Results Document from End-User Representatives in accordance with Item 12 of the DTS. • Valid and updated Tax Clearance Certificate	Payment for Year 3 (33.34% of the total contract cost) and shall be payable in four (4) tranches, as follows: **First Tranche** (25% of the contract cost for Year 3) - within the 1st quarter of Year 3 upon submission of the required outputs and supporting documents. **Second Tranche** (25% of the contract cost for Year 3) - within the 2nd quarter of Year 3 upon submission of the required outputs and supporting documents. **Third Tranche** (25% of the contract cost for Year 3) - within the 3rd quarter of Year 3 upon submission of the required outputs and supporting documents. **Fourth Tranche** (25% of the contract cost for Year 3) - within the last month of Year 3, upon submission of the required outputs and supporting documents.

12. PERFORMANCE REVIEW AND ASSESSMENT

12.1. The Service Provider shall maintain a satisfactory level performance throughout the contract period based on the following set of performance criteria:

ITEM	PERFORMANCE CRITERIA	WEIGHT
I	Conformity to Technical Requirements	25
II	Timeliness in the Delivery of Services	25
III	Behavior of Personnel (Courteous, Professional, and Knowledgeable)	20
IV	Response to Complaints	20
V	Compliance with set office policies for such services	10
TOTAL	**PERFORMANCE RATING** **PASSING RATE: 80 POINTS**	**100**

12.2. The Service Provider must achieve a minimum rating of "Satisfactory" with at least 80 points. Each criterion must meet the minimum weighted score in the performance evaluation.

12.3. The OCIO and ICTSS shall conduct a year-end assessment or evaluation one month before the end of the subscription, based on the above-cited criteria, to ensure compliance of the Service Provider with the DTS, as well as with the other terms and conditions imposed by the DBM during the contract period.

12.4. Based on its assessment, the DBM may pre-terminate the contract for failure of the Service Provider to perform its obligations thereon following the procedures prescribed under the Guidelines on Termination of Contracts issued by the Government Procurement Policy Board under Resolution No. 018-2004 dated December 22, 2004.

12.5. Subject to the provisions of the Implementing Rules and Regulations (IRR) of Republic Act No. 9184, particularly on contract renewal, the engagement of the Service Provider may be renewed for another term, provided that:

- The Service Provider obtains a satisfactory rating (minimum of 80 points) based on the performance evaluation;
- There is a continuing need for the service;
- The renewal is in accordance with the approved Annual Procurement Plan (APP) and budgetary allocation; and
- All applicable procurement and legal requirements are duly complied with

Attachment 1
Details of Technical Requirements of Cyber SOC Solution

The Service Provider shall provide a Cyber SOC solution with the following features and functionalities:

A. Log Ingestion

1. Should have a scalable architecture and should be able to collect data at scale across all users, devices, applications, and infrastructure, both on premises and in multiple cloud environments.
2. Should have the capability to export raw logs in various formats such as syslog, JSON, XML, CSV etc.
3. Should have seamless integration and correlation of logs from multi-cloud environments.
4. Should be scalable to cater the growing data source requirement.
5. Should keep the ingested data along with all the related system, infrastructure, diagnostics address regulatory requirements and other compliance requirements such as SOC2 Type2, ISO27001.
6. Should be able to connect data/log sources for ingestion of logs, majorly through out-of-the-box connectors.
7. Must support both agent and agentless log collection methods e.g. Syslog, Common Event Format (CEF), also support REST APIs.
8. All communications between the various components of the security analytics should be encrypted.
9. Should have capability to ingest data in custom log formats.
10. Should have functional features such as data source health monitoring, view on specific service or data source issues.
11. Must automate internal health checks and notify the user in case of problems.
12. Must have self-monitoring features to track health of all nodes, also monitor capacity requirements in terms of, data consumption, performance, query limits and so on.
13. Provide out-of-the-box, service-to-service support for cloud related services.
14. Should provide options to export stored data for long term retention or archival.
15. Should allow the data to be retained in a low-cost archived state as per the retention policy/configuration.
16. Should be able to parse and correlate multi-line logs.
17. Should have capability to filter undesired, non-security logs at collection, processing and visualization layer.
18. Identify/remember frequently used queries/rules and provide means for optimization of queries/rules.
19. Shall have the ability to perform free text search on events, incidents, rules and other parameters.
20. Shall be sized to meet the data retention requirement, 3 months online and minimum of 11 months for archive.
21. Should be able to collect alerts/logs from several security products including but not limited to, Firewalls, PIM, DLP, IPS, WAF, Anti-APT, HIPS, AV, XDR etc. A baseline list of log/alert sources are listed below in **Attachment 3** and made an

integral part of this document.

22. Should have in-built parser to parse the data.
23. Shall have a robust data ingestion pipeline architecture with health monitoring capabilities.
24. Ability to build a highly robust resilient data/log ingestion pipeline.
25. Solution should be able to browse for content packs which are prebuilt integrations, playbooks, dashboards, fields, and data model rules used to support security automation and analysis.

B. Agent Log Collector

1. Shall incorporate endpoint agent sensor as part of SIEM data collection system.
2. The endpoint agent's sensor can be consolidated to enable endpoint protection capabilities to reduce agent footprint in the future.
3. The endpoint agent able prevent malicious, exploitative and fileless attacks on endpoints.
4. Able to conduct deep forensics investigation without deploying additional agents.
5. Solution must support machine learning-based local analysis and threat prevention.
6. Solution must support behavior-based threat prevention for dynamic analysis of running processes.
7. Solution must provide exploit prevention by exploit technique.
8. Solution must have known threat prevention based on threat intelligence, such as file hashes.
9. Solution must provide Zero-delay signatures to rapidly deliver protection and share threat intelligence.
10. Solution must have network inspection engine to stop network-based attacks.
11. Solution must provide reverse shell protection capability.
12. Solution must have transparent threat detection engine updates.
13. Solution must have security profiles and exceptions.
14. Solution must have capability of providing ad hoc and scheduled scanning of endpoints.
15. Solution must provide protection against malware, ransomware, and fileless attacks.
16. Must be a single lightweight agent for endpoint protection, detection, and response.
17. Solution must be capable of providing the below features:
    a. Host firewall
    b. Disk encryption
    c. USB device control
18. Customizable prevention rules.
19. Compatible with a network security client for endpoints for secure remote access, industry-leading threat prevention, and URL filtering.
20. Collect, Parse, Normalize, Index and Store security logs at very high speeds.
21. Out of the box support for a wide variety of security systems and vendor APIs- both on premises and cloud.
22. Window Agents provide highly scalable and rich event collection including file integrity monitoring, installed software changes, and registry change monitoring.
23. Linux Agents provide file integrity monitoring, syslog monitoring, and custom log file monitoring.

24. Can modify parsers from within the GUI and redeploy on a running system without downtime and event loss.
25. Create new parsers (XML templates) via integrated parser development environment.

C. Visibility and Analytics

1. Behavioral analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, and user events over time.
2. Identity analytics to detect user-based threats such as lateral movement.
3. Supervised and unsupervised machine learning capabilities.
4. Predefined and customizable behavior-based detection rules.
5. Custom correlation rules that can retroactively detect attacks.
6. Granular alert exclusions for optional tuning of endpoint, network, cloud, or third-party alerts.
7. Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services.
8. Ability to consume threat intelligence feeds from third party sources in JSON and CSV formats.
9. Detection of attack techniques across the attack lifecycle including discovery, lateral movement, command and control, and exfiltration.
10. Demonstrated ability to detect attacker tactics and techniques through MITRE ATT&CK Evaluations.
11. Tagging of MITRE ATT&CK tactics and techniques in alerts, detection rules, and incidents.
12. Asset management with rogue device discovery.
13. Host inventory with detailed user, system, and application information.
14. Forensics data collection before or after an incident occurs.
15. Forensics data collection from offline and air-gapped devices.
16. Should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules/policies and parsers.
17. Should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics based, Behavioral based, etc., across different devices and applications.
18. Should provide investigation capability to investigate incidents.
19. Should have capability to build customized ML models.
20. Should support logical operation and nested rules for creation of complex rules.
21. Should have the ability to correlate all the fields present in a log/flow data.
22. Should have rules/policies to detect any compromises by generating alerts collected over a period of time.
23. Should provide out-of-the-box rules and built-in templates to help create threat detection rules to notify suspicious events.
24. Should have capabilities to correlate alerts between different source & destination IPs to find similar or colluding threat events.

25. Should have capability to detect advanced multistage attacks mapped to MITRE ATT&CK Framework.
26. Should have a knowledge base on methods used by attackers in various past breaches globally to create models to detect such attacks.
27. Detect suspicious events and generate incidents/offenses on minimum basic use cases given below but limited to:
    a. Failed login attempts
    b. Login attempts from suspicious locations
    c. Vendor logins from unauthorized subnets
    d. Vertical & Horizontal port scans
    e. Traffic from blacklisted Ips
    f. Login attempts at unusual timings
28. Should provide use cases given below but not limited to the list:
    a. Credential harvesting
    b. Credential Access
    c. Unauthorized RDP connections
    d. Unauthorized usage of PowerShell
    e. Crypto mining
    f. Data destruction
    g. Resource abuse
    h. Data Exfiltration (Mass file download, file share, mailbox exfiltration)
    i. Denial of service
    j. Lateral movement
    k. Malware command and control
    l. Ransomware executions
    m. Resource hijacking
29. Detect emerging and unknown threats in your environment by applying extended ML analysis and by correlating a broader scope of anomalous signals, while keeping the alert fatigue low.
30. Should allow alert enrichment features while creating custom query rules using entity (resource) mapping.
31. Should allow to add exceptions to analytic rules to reduce false positives.
32. UEBA feature of SIEM should help build baseline behavioral profiles of organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon.
33. Should provide entity insights based on following data sources:
    a. Syslog (Linux)
    b. Security Events (Windows)
    c. Audit & Sign-in logs (from AD and other cloud platforms) 5.1.3.34.4. Office Activity (Office 365)
    d. Behavior Analytics
    e. Threat Intelligence Indicators
34. Sync user entities from Active Directory/LDAP to SIEM
35. Built-in watchlist of templates for creating custom use cases such as but not limited to track:
    a. Privileged Users
    b. Terminated Employees
    c. Service Accounts/users

d. Identity Correlation
e. High Value assets
f. Network Mapping

36. Must align rules/use cases with MITRE ATT&CK framework.
37. Has native external asset visibility that is part of the SOC solution to determine attack surface.

D. Investigation

1. Automated root cause analysis of any alert, including network alerts, if endpoint data is available.
2. Visualization of the chains of execution leading up to an alert.
3. Timeline analysis view to see all actions and alerts on a timeline.
4. A 360-degree user view with user risk scores.
5. A cloud investigation view with cloud-specific events and artifacts.
6. Querying for Indicators of Compromise (IOCs) and endpoint behaviors.
7. Querying for online and offline hosts.
8. Querying of log data from any source, including network, cloud, endpoint, identity & forensics data.
9. Advanced querying language with support for wildcards, regular expressions, JSON, data aggregating, field and value manipulation, merging of data from disparate sources, and visualization of data.
10. Ability for a security analyst to easily pivot between views.
11. Granular filtering and sorting of query results.
12. In-context wizard that lets you search for information, perform common investigation tasks, or initiate response actions from anywhere in the management console.
13. Automatic aggregation of relevant IP or hash information, including threat intelligence, events, and related incidents in a single view to simplify investigations.
14. Identification of whether an event was blocked by an endpoint agent, firewall, or another prevention technology.
15. Automated stitching of endpoint, network, cloud and identity data, including security alerts & events.
16. Noise cancellation; removal of non-significant binaries and DLLs from chain.
17. SOC analyst context of TTPs to utilize knowledge gained to help in future investigations.

E. Incident Management

1. Automated grouping of related alerts from various sources into a single incident.
2. Intuitive incident view with an incident overview and MITRE tactics and key incident information.
3. Customizable incident scoring.
4. Listing of notable artifacts from alerts and their threat intelligence information.
5. Listing of user and hosts involved in incidents to quickly determine the scope of an incident.
6. Ability to assign incidents to team members.

7. Automated notifications on incident assignment.
8. Ability to add comments to incidents.
9. End-to-end management of the incident lifecycle (new, investigation, closed, handled, etc.).
10. Optional merging of incidents.
11. Ability to send incident data to third-party case management.
12. Ability to trigger a remediation script when a specified incident occurs.
13. API-based integration to external ticketing systems such as ServiceNow, ConnectWise, and Remedy to name a few.
14. Support Built-in Case Management system.
15. Incident reports can be structured to provide the highest priority to critical business services and applications.
16. Trigger on complex event patterns in real time.
17. Incident Explorer — dynamically linking incidents to hosts, IPs and user to understand all related incidents quickly.

F. Threat Intelligence

1. Ability to alert on known malicious objects on endpoints with IOC rules.
2. Ability to automatically scan historic data for IOCs as they are added to the solution and raise alerts.
3. Out-of-the box integration with one or more threat intelligence services for threat intelligence tags and additional context on key artifacts.
4. Ingestion of threat intelligence feeds from third-party sources in JSON and CSV formats.
5. IOC creation using APIs.
6. IOC creation from the management console.
7. Ability to import multiple IOCs using APIs.
8. Ability to import multiple IOCs from a CSV file using the management console.
9. Configurable severity level of an IOC.
10. Threat Intelligence should deliver a comprehensive range of timely adversary and technical threat intelligence through a customizable portal or Dashboard.
11. Threat Intelligence should provide data feeds and APIs for automated consumption by the SIEM solution.
12. Should be able to import threat intelligence by enabling data connectors to various threat intelligence platforms and feeds.
13. View and manage the imported threat intelligence along with features to create new indicators.
14. Threat Intelligence provided must be relevant, context-rich, timely and accurate.
15. Add indicators in bulk to SIEM threat intelligence from a CSV or JSON file and support other formats such as STIX/TAXII, XML, txt, pdf, doc, email etc.
16. Curation, normalization, enrichment, and risk scoring of data.
17. The solution should be able to enrich all imported threat intelligence indicators with Geolocation and WhoIs data.
18. Threat intelligence feeds should enable efficient security operations and reduce the time for investigation.
19. The Threat Intelligence Portal/Dashboard should provide End-to-End picture of

threats.

20. Built-in threat hunting capabilities to detect threat before, during, and after a compromise.
21. Should have a threat hunting dashboard to run all analyst queries.

G. Response and Automation

1. Remote terminal capability.
2. Full CMD, PowerShell, or Python commands and scripts on Windows 7, 8, 10, and 11.
3. Full Bash or Python commands on macOS and Linux.
4. Ability to execute PowerShell, Python, BASH, and ZSH scripts across multiple endpoints simultaneously on Windows, macOS, and Linux.
5. Pre-defined scripts to allow analysts of all experience levels to easily collect data and investigate and respond to threats.
6. Status window that displays script results, confirming whether scripts executed successfully.
7. Remote isolation of a single endpoint or multiple endpoints.
8. Remote file deletion of a single endpoint or multiple endpoints.
9. Automatic and manual collection or retrieval of quarantined files and objects.
10. Ability to view, suspend, or terminate running processes or download binaries with a graphical task manager for Windows, macOS, and Linux.
11. Graphical file manager with ability to view, download, rename, or move files for Windows, macOS, and Linux.
12. Remediation suggestions to restore hosts to their original state.
13. Search and destroy to swiftly sweep across endpoint and eradicate threats.
14. Integration with firewalls to block access to malicious IP addresses or domains.
15. Built-in native security orchestration, automation, and response (SOAR) solution for incident analysis.
16. Native automation playbook development capabilities with the proposed solution.
17. Resolve incidents or automate parts of the incident investigation and resolution workflow.

H. Data Collection, Data Integration, and Forensics

1. Data Collection, ability to ingest logs from virtually any data source, including network, endpoint, cloud, identity, application, HR, and any other data source for threat hunting, correlation and detection.
2. User information for analytics
    a. Domain and distinguished name
    b. Email address
    c. Organizational unit
    d. Phone number
    e. Logged-in user
    f. Typical user of a machine
    g. User creating the process that initiated communication
    h. User group and organizational unit from directory services
    i. User data from a variety of sources including network traffic logs, Windows event logs, Okta logs, PingOne and PingFederate logs, Azure Active Directory

logs and other user identity directory systems/products.

3. Device information for analytics
    a. MAC address
    b. Hostname of device
    c. Domain name
    d. Distinguished name of host
    e. Organizational unit
    f. Operating system and version
    g. Name of firewall, if applicable
    h. Other names used by firewall configuration, if applicable
4. Process information for analytics
    a. Process timestamp
    b. Path and name
    c. Process ID
    d. Loaded modules
    e. Hash values, such as MD5 and SHA-256
    f. Command line arguments
    g. RPC requests and code injection data, if applicable
    h. Signature state
5. File information for file create, write, access, open, rename, or delete for analytics
    a. Timestamp
    b. Path and name
    c. Previous file name and path for file rename events
    d. Hash values, such as MD5 and SHA-256
    e. Username
6. Network activity, including outgoing, incoming, and failed connections for analytics
    a. Timestamp
    b. Source IP address, destination IP address, source port, and destination port
    c. Bytes sent and received
    d. Protocol
    e. Geolocation data
    f. Proxy information
    g. Integration with next-generation firewalls for complete Layer 7 visibility, including application name
    h. Connection duration
    i. Transaction-level data and enhanced information about key protocols, such as DNS, HTTP, DHCP, RPC, ARP, and ICMP
7. Registry activities, such as create, modify, delete and rename key for analytics
    a. Timestamp
    b. Key name
    c. Value and type
    d. Previous key name for rename events
8. System events for analytics
    a. User status change event, such as login and logout
    b. Host status change event
    c. Agent status change event
9. Security alerts for analytics

a. URL filtering logs
b. Firewall threat logs
c. Endpoint threat logs

I. Active Attack Surface Management

1. Internet Indexing & Data Collection
    a. Should have frequent, high-quality internet indexing that is proprietary to the organization and have a means to ensure confidence in the results.
    b. Solution generates its own scan data and does not rely on outside, third-party providers.
    c. Should have a 5+ year history of scanning the internet
    d. Should rescan daily or faster.
    e. Should cover +2500 ports for broad detection.
    f. Should conduct full protocol handshakes, not just open port checks which are noisy and often inaccurate.
    g. Should support IPv4
    h. Should support IPv6
2. Asset Identification: should be able to identify a range of assets that are exposed to the global internet including the following:
    a. Should discover IP ranges
    b. Should discover Certificates. Note that a specific inventory view for certificates is required.
    c. Should discover paid level domains
    d. Should discover subdomains
    e. Should discover websites
    f. Should report all relevant context of each asset type, including the registration information.
    g. Should utilize machine learning to automatically map assets back to the organization and utilize human analyst expertise for additional tuning to achieve higher mapping accuracy.
3. Data should be enriched to provide larger context
    a. Should report the date/time of scan results
    b. Should include GeoIP for additional context
    c. Should include CVE data
4. Cloud Discovery and Analysis: Not only identify, but help manage cloud assets
    a. Should discover assets across all cloud providers
    b. Should treat dynamic assets in a simple manner, so that results can be deduplicated when a single identifier is seen hosted many times across large CDNs.
    c. Should distinguish between directly attributable assets and co located services.
    d. Should allow for the configuration of approved and unapproved cloud providers, and corresponding alerts.
5. Tooling to streamline the management of assets
    a. Should have a defined and scoped process for validating that assets do in fact belong to the DBM.
    b. Should describe why an asset is attributed.
    c. Should provide visibility into asset sprawl across certificate issuers, domain registrars, and cloud providers.

d. The ability to apply tags to enable advanced data filtering, customized data, and to restrict or permit access to data.

6. Risk scores and prioritization
   a. Should identify risks across your assets, categorize the risk, and prioritize incidents for remediation.
   b. Risk score should be based on accepted industry metrics and allow for customization.
   c. Should offer remediation guidance for risks.
   d. Should group alerts impacting the same service together automatically.
7. Capable of fixing things
   a. Should have the ability to automatically remediate exposures. This should include full resolution of the incident by reaching back via API and blocking the service at the port level.
   b. Allow customizability to the remediation path
   c. In solution, instructions on how to set up integrations and use Automated Remediation.
8. Comprehensive score on your overall security posture
   a. Should have the ability to allow users to customize the weight of incidents in their overall risk score based on the DBM needs.
   b. Ability to create or remove risk scoring rules.
   c. Ability to override the default system score and enter a score.
   d. Risk scoring is a combination of CVSS and EPSS data.
9. Should have a method of explaining why an asset was attributed to the DBM.
   a. Should describe why the asset was attributed & provide evidence.
   b. Should be explicit on how confident the solution is on the attribution.
10. Provide compliance dashboards that map identified issues to compliance frameworks to help the DBM understand their overall compliance with regulatory and organizational policies. These dashboards need to provide executive visibility, prioritize high-risk cybersecurity areas, and measure the progress of the DBM's cyber security maturity.
11. Managing assets and identifying risk through policies.
    a. Provide accurate context & classification to enable automated policy development and mitigate security exposures identified.
    b. Identify all VPNs, certificates about to expire, domains about to expire, etc.
    c. A flexible policy engine that allows rapid building of new fingerprints and detect devices against critical CVEs.
    d. Offer descriptions of common CVEs and the best practices around securing the DBM's assets from them.
12. Built-in security policies and settings
    a. Enables to define the approved domains and approved IP ranges through which access the solution.
    b. Enables to specify one or more domain names that can be used in the DBM's distribution lists.

J. Endpoint Agent Solution Support and Resource Requirements

1. Support for all recent Windows versions, including Windows Server systems.
2. Support for all recent macOS and Mac OS X versions.
3. Support for all major Linux distributions

4. Full auditing for all actions in the system
5. Average CPU usage of less than 3% with all services enabled
6. Agent installation size less than 50 MB
7. Ability to push agent updates from the management console.
8. Optional automated agent upgrades.
9. Granular control of agent controls and notifications, including tray icon visibility, custom end user notifications, and the option to restrict response options such as remote terminal access.
10. Support for non-persistent VDI.
11. Ability to support temporary sessions for machines that repeatedly revert to a snapshot (or image) on which the agent is not installed.
12. Optional dissolvable agent for hosts that cannot support a persistent agent to collect endpoint information.

K. Deployment, Management, and Reporting

1. Scalable, cloud-based management and agent deployment.
2. Single, web-based management console for endpoint security as well as extended detection and response.
3. Role-based access control (RBAC) for granular permissions.
4. Multi-factor authentication (MFA) for management.
5. Customizable dashboard for high-level status of security and operational information.
6. Kubernetes integration for deployment and management in a container environment.
7. Optional on-premises broker service to aggregate and manage communications between endpoints and a cloud-based management console.
8. Standards-based APIs to allow third-party management tools to integrate and perform administrative actions.
9. Best practices to ensure the entire solution and its infrastructure are secure, including hardening, encryption for data at rest and data in motion, network security, physical security, and regular assessment tests.
10. Provides default reports and dashboards.
11. Reports can be built with predefined widgets or with custom widgets.
12. Dashboards offer dynamic filters and drill downs to allow users to easily pivot between data points.
13. Reports can be scheduled and saved with raw data attached as a CSV.

L. Data Retention

1. Data retention of at least three (3) months online (hot storage), and nine (9) months archive (cold storage).
2. Minimum of one (1) year of retention for audit logs of administrative and investigative activity.

M. DBM Cyber Security Operation Center Monitoring Video Wall System

1. Minimum of four (4) units of brand-new commercial grade display monitors with the following minimum specifications:
   a. Fifty-Five (55) inches viewable screen size

b. 1,920 x 1,080 (FHD) native resolution
c. 0.44mm bezel width, 0.88mm bezel to bezel
d. 178x178 degrees viewing angle both horizontally and vertically
e. 500 nits' brightness.
f. 1,000:1 contrast ratio.
g. 60Hz refresh rate.
h. 8ms response time.
i. 10bit, 1.07 billion colors, Color Depth.
j. In-plane Switching (IPS) panel technology.
k. Input connectivity: HDMI, DP, DVI-D, USB 2.0, AUDIO IN, RJ 45 LAN.
l. Output connectivity: DP, RJ 45 LAN, AUDIO OUT, RS-232C out.
m. Supports various display orientation (landscape and portrait) to accommodate video wall layout needs.
n. VESA Standard Mount Interface (600x400).

2. One (1) unit of branded and brand-new Video Wall Controller with the following minimum specifications such as but not limited to:
   a. Video Matrix, eight (8) input and ten (10) output.
   b. Input type: VGA, HDMI, DP, IP-Video.
   c. Input channel: 1080P up to 320 channels,4K up to 160 channels.
   d. Input resolution: Single channel 4K: dual link HDMI/DP.
   e. Output type: VGA, DVI, HDMI, CVBS.
   f. Output channel: 1080P up to 320 channels, 4K up to 160 channels.
   g. Pure-hardware FPGA Array, modular design, 25GBps base exchange processing speed.
   h. Support 4K DP/HDMI/Dual-link DVI input and 4K HDMI output.
   i. Support VGA/DVI/HDMI sources self-adaption on single input card.
   j. Support HDCP2.0 for HDMI input and output.
   k. Support opening at least 8 windows on each two screens.
   l. Support up to 16 video wall groups control on single controller and work with variety of display terminals such as LCD, LED, projector.
   m. Support scene management, up to setup and display 100 scenes.
3. One (1) unit of universal mobile videowall stand for 2x2 videowalls with the following minimum specifications:
   a. Four (4) pop-out brackets that can handle 39"-60" videowall monitor screen size.
   b. Compatible with VESA mount interface up to 900mm.
   c. Universal design suitable for all video wall screens.
   d. Tool-less micro-adjustments for seamless screen alignment.
   e. Integrated cable management.
   f. Includes adjustable levelling feet.
   g. Includes non-marking 4" locking/braked casters.
   h. Safety screws help prevent unauthorized removal of screens.
   i. All required mounting hardware components.
4. One (1) set of branded and brand-new Workstation that are capable to operate 24/7 with the following minimum specifications:
   a. 12th generation Intel Core i7 12 Core.
   b. 16GB DDR4 memory.
   c. 1 TB Solid State Drive.
   d. PCIe Quad Monitor Video Card 8GB dedicated memory.

e. 24” LED Monitor.
f. USB Keyboard and Mouse.
g. 10/100/1000 Gigabit Ethernet.
h. Wireless LAN.
i. Bluetooth.
j. USB Type-C Ports.
k. USB 2.0 Ports.
l. Windows 11 Professional 64 bit.
m. Videowall Management Software

5. Delivery, Installation, Commissioning, and Turnover of Videowall System:
   a. The videowall system shall be delivered, installed, configured, and fully commissioned at the DBM within ninety (90) calendar days from the issuance of the Notice to Proceed (NTP).
   b. Commissioning shall include functional testing, calibration of display units, configuration of display layouts, software validation, and user orientation to ensure optimal performance in the actual operating environment.
   c. Upon completion of the subscription period, full ownership, operational control, and custody of the videowall system—including all associated hardware, software, and documentation—shall be formally turned over to the Department of Budget and Management (DBM).
   d. The Service Provider shall coordinate the proper turnover process with DBM, including documentation and submission of as-built and configuration records.

Attachment 2
Scope of Work and Services

The Service Provider shall provide Cyber SOC solution with the following scope of work and services:

A. The Service Provider shall conduct a pre-implementation meeting/s with ICTSS representatives within ten (10) calendar days from the receipt of NTP, so that all the necessary preparations, ideal set up, Service Provider's familiarization, and other implementation matters are discussed and finalized.

B. The Service Provider 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 upon successful conclusion of the pre-implementation meeting/s with ICTSS representatives but not more than thirty (30) days from receipt of NTP. Said work plan shall be validated and subject to approval of the ICTSS Director.

C. The Service Provider shall deliver, integrate, and configure all the necessary components which includes devices listed below in **Attachment 3** in coordination with ICTSS and/or the designated DBM project lead the Cyber SOC Solution within sixty (60) calendar days from the receipt of the NTP and approval of the work plan of activities.
   1. The Service Provider shall configure and install the Monitoring Video Wall System (as specified in **Attachment 1-M**) at the DBM designated location to be provided by ICTSS.
   2. The Service Provider shall ensure the availability of the ingested raw logs with comprehensive searchability. The retention of the logs shall be within the duration of the contract, after which, the logs will be extracted and 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.
   3. The Service Provider shall ensure flexibility and scalability of the DBM Cyber SOC solution and shall ingest and process all events sent by the DBM for the SIEM and SOAR requirements.
   4. The Service Provider must include onboarding and advisory services throughout the period of engagement.
   5. The Service Provider must include strategic and advisory threat intelligence by industry sector.
   6. The Service Provider shall provide a cybersecurity risk ratings solution that enables the DBM to assess and manage its cybersecurity posture. The cybersecurity risk ratings solution shall have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

D. The Service Provider shall provide 24x7 monitoring services for the DBM SOC, ensuring continuous monitoring, surveillance, threat detection, and incident response:
   1. Visibility into lateral movement across the network and other parts of the infrastructure.
   2. Continuous monitoring for cybersecurity risks.
   3. Detection and response for threats involving managed and unmanaged endpoints.
   4. Detection and response for threats involving remote users.
   5. Detection and response for threats involving cloud servers/resources.

6. Ensure continuous collection and centralized storage of all security data for behavioral analytics.
7. Threat hunting or incident responders for the remote response on endpoint incidents/events.
8. Get context from indicators such as IP's, URL's, domains, or hashes using the tools within the solution, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification.
9. Provide root cause analysis of all identified security incidents and malicious activity.
10. Coordinate "Take down" services for malicious servers, websites, and/or social media accounts that impersonate legitimate ones.
11. Provide all the necessary information and/or context for the DBM to execute take-down of malicious servers, websites or social media accounts.
12. Report security events/incidents as soon as validated and within the agreed escalation SLAs through Microsoft Teams and email.
13. Create and tune detection rules. Service Provider, with the participation of the DBM to ensure applicability and proper contextualization, shall be responsible for the definition of detection use cases in the SOC solution. Furthermore, Service Provider shall continuously update and fine-tune the parameters of the use cases to ensure that only relevant threat alerts are generated.
14. Perform continuous baselining of the DBM's infrastructure behavior based on the data sources within the Service Provider's scope of visibility. This is vital to establish what is "normal" in the context of everyday network traffic, host processes, application behavior and observed security artifacts.
15. Continuously incorporate external and internal threat intelligence into its threat detection and analysis activities. This includes regularly updating the IOCs used by the SOC analysts based on acquired information.

E. The Service Provider shall designate a dedicated Technical Account Manager (TAM) to the DBM. The TAM shall be responsible for the close coordination between Service Provider and the DBM's ICTSS and/or designated team/s to ensure that actions pertaining to the remediation of escalated cases and requests are clearly communicated and known to the responsible parties.

F. The Service Provider shall ensure that the Cyber SOC solution maintains a service level agreement (SLA) of 99.9% availability.

G. The Service Provider should facilitate at least quarterly Continual Service Improvement (CSI) workshops to the DBM for possible improvement of service through process, people and technology.

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

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

J. The Service Provider shall provide Technical Trainings with certifications to be

conducted by an Authorized Training Centers. The Technical Training should be a face-to-face classroom type based on the following schedule:

Technical Training	**Schedule**	**No. of Participants**	**Duration**
COMPTIA PenTest +	Within two (2) months from the receipt of Notice to Proceed	Four (4) Participants	Forty (40) hours
	Within three (3) months from the receipt of Notice to Proceed	Four (4) Participants	Forty (40) hours
COMPTIA Cloud +	Within four (4) months from the receipt of Notice to Proceed.	Four (4) Participants	Forty (40) hours
	Within five (5) months from the receipt of Notice to Proceed	Four (4) Participants	Forty (40) hours
CCNA Security	Within six (6) months from the receipt of Notice to Proceed	Four (4) Participants	Forty (40) hours
	Within seven (7) months from the receipt of Notice to Proceed	Four (4) Participants	Forty (40) hours

The Service Provider shall secure appropriate certification from the Authorized Security Training Center and issue the same to the DBM nominated participants.

K. The Service Provider shall provide As-built documentation of the Cyber SOC solution for the DBM, infrastructure set-up/ diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the hardware/software 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 of the Cyber SOC.

L. The Service Provider shall conduct the following monthly activities, such as but not limited to:
   1. Facilitate SOC security briefing at least once a month for the DBM, to present the latest local and international news and updates in Cyber security and latest/new Common Vulnerabilities and Exposure (CVE).
   2. Conduct monthly regular review with the DBM ICTSS and/or designated team/s, to help the DBM make decisions to enhance its security posture and response capabilities.
   3. Submit the following Cyber SOC monthly reports within the 5th working day of the succeeding month, subject to ICTSS Director approval. These reports should provide insights into the security events, incidents, and trends within the DBM's

IT environment. Said **reports** shall include the following:

a. **Incident Report:** This report details out, if any, 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.
b. **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.
c. **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.
d. **Tactics, Techniques, and Procedures (TPPs) Report:** This report tracks TTPs within the DBM's network to identify any abnormal or unauthorized behavior which may include user activity. This helps in detecting insider threats and unauthorized access.
e. **Security Incident Response Plans (SIRP) Report:** This report outlines the process followed during the response and recovery phases of security incidents. They include details, if any, about incident containment, investigation, communication, and resolution.
f. **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.
g. **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.
h. **Cyber Security Updates:** This report provides the latest local and international news and updates in Cyber security and new Common Vulnerabilities and Exposure (CVE).

M. Incident Response

1. The Service Provider shall develop an incident response plan for the 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:
   a. Escalation process
   b. Incident identification process
   c. Incident containment process
   d. Incident eradication process
   e. Incident recovery process
   f. Post-incident reporting
2. The Service Provider shall map the security playbook and runbooks for applicable security use cases to guide the DBM on their incident response.
3. The Service Provider shall deliver technical assistance to the DBM IT Security Team during an emergency (successful) breach response.
4. The Service Provider shall have a facility to receive the DBM’s reported incident (via an authorized point of contact from the DBM) for incidents not captured on the monitoring tool.

5. The Service Provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.
6. The Service Provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.
7. The Service Provider shall identify indicators of compromise and scan the network to search for other related infected systems.
8. The Service Provider shall deliver insider threat investigation.
9. The Service Provider shall assist in the following:
    a. Incident handling preparation and execution
    b. Crisis management
    c. Breach communication
    d. Forensic analysis including preservation of evidence for chain of custody requirements.
    e. Remediation
10. The Service Provider shall respond to any IT security incidents from the time it was reported/detected based on agreed upon Service Level Agreement. Incident response can be in the form of telephone call, remote assistance, or onsite support.

N. The Service Provider shall conduct an annual IT Security Awareness seminar for DBM's employees that covers security best practices at home and at work.

O. The Service Provider shall conduct a one-time lecture on Incident Response Overview for First Responders, for the DBM's information security personnel responsible for responding to security incidents. This shall cover the following topics:
    1. Overview of Incident Response Process
    2. Responsibilities of First Responders
    3. General Guidelines for Data Preservation
    4. Preservation of Key Artifacts and Evidence
    5. Ensuring Chain of Custody and Safe Transfer of Evidence

ATTACHMENT 3
LIST OF ALERT/LOG SOURCES

Log Source	Units	Location	Events Per Second (EPS) Estimated
Palo Alto NGFW	2	On-Premise	867
Fortinet Fortigate (CO)	2	On-Premise	560
Fortinet Fortigate (RO)	16	On-Premise	146
F5 BigIP	2	On-Premise	11
F5 Distributed Cloud Services (XC) DDoS and Web Application Firewall		Cloud	
Cisco Routers	19	On-Premise	
Cisco Switches	120	On-Premise	
Cisco Wireless Controllers	4	On-Premise	
Cisco Access Points	140	On-Premise	
Windows 11	1200	On-Premise	
Windows Server	63	On-Premise	
Linux	97	On-Premise	
External DNS (Linux)	2	On-Premise	
Internal DNS (Windows)	2	On-Premise	480
Active Directory (Windows)	2	On-Premise	20
DHCP Server (Linux)	2	On-Premise	
Oracle Cloud	1	Cloud	
Amazon Web Services (AWS)	1	Cloud	
Google Cloud	1	Cloud	
Microsoft Azure	1	Cloud	
Appian Cloud	1	Cloud	
OutSystems Cloud	1	Cloud	

Note: As the number of devices and log sources are still undetermined due to some are in progress, the solution should be able to handle at least 2,000 devices and a minimum aggregate of 5000 events per second (EPS) capacity.

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;

In cases wherein the Mayor's/Business permit is recently expired, please be reminded that the recently expired Mayor's/Business Permit, together with the official receipt as proof that the prospective bidder has applied for renewal within the period prescribed by the concerned local government unit, shall be accepted by the PhilGEPS for the purpose of updating the PhilGEPS Certificate of Registration and Membership 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 August 4, 2025.

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 **August 5, 2020 to August 4, 2025.**

c. The similar contract for this Project shall refer to the supply, implementation, and/or services of a cyber/information security operations center which may include deployment of related cyber security tools/technologies such as Security Information and Event Management (SIEM), Firewalls, Security Orchestration, Automation and Response (SOAR), Endpoint Detection and Response (EDR) and/or services such as cyber security monitoring services, threat intelligence, forensics, cyber security incident response/management, cyber security administration. If the supply, implementation, and/or services of a cyber/information security operations center form part of a bigger contract, only the cost component of the supply, implementation, and/or services of a cyber/information security operations center which may include deployment of related

cyber security tools/technologies such as SIEM, Firewalls, SOAR, EDR and/or services such as cyber security monitoring services, threat intelligence, forensics, cyber security incident response/management, cyber security administration 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-2025-44*

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 this __ day of *[month] [year]* at *[place of execution]*, Philippines.

[Select one of the two following paragraphs and delete the other]

Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC).

Affiant/s exhibited to me his/her *[insert type of government identification card used]* with no. _____ issued on _____ at _____.

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

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

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

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 this __ day of *[month] [year]* at *[place of execution]*, Philippines.

[Select one of the two following paragraphs and delete the other]

Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC).

Affiant/s exhibited to me his/her *[insert type of government identification card used]* with no. _____ issued on _____ at _____.

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

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

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

Bid Form for the Procurement of Goods
[shall be submitted with the Bid]

BID FORM

Date : _____
Project Identification No. : **DBM-2025-44**

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 (SOC)** 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.

Year	**Annual Price (Inclusive of VAT)**
2025	
2026	
2027	
2028	
Grand Total	

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]*.

Signature of Authorized Signatory: _____

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. 2025-___

SUBSCRIPTION TO CYBER SECURITY OPERATIONS CENTER (SOC)

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 corresponding appropriations 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	_____

A C K N O W L E D G M E N T

REPUBLIC OF THE PHILIPPINES)
C I T Y O F M A N I L A) *S.S.*

BEFORE ME, a Notary Public for and in the City of _____, Philippines on this _____ day of _____, 2025 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 _____, 2025.

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


Republic of the Philippines
gppb
Government Procurement Policy Board