REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF BUDGET AND MANAGEMENT

GENERAL SOLANO STREET, SAN MIGUEL, MANILA

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 2

This SBB No. 2 dated November 10, 2023 for **Project ID No. DBM-2024-05, "Subscription to Cyber Security Operations Center,"** is issued pursuant to Section 22.5 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184, to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of the Bidding Documents.

<table>
<tr><th>PARTICULARS</th><th>AMENDMENTS/CLARIFICATIONS</th></tr>
<tr><td>Section II. Instructions to Bidders

xxx

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.</td><td>Section II. Instructions to Bidders

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.

<s>The Procuring Entity has prescribed that subcontracting is not allowed.</s></td></tr>
<tr><td>Section III. Bid Data Sheet
<table>
<tr><th>ITB Clause</th><th></th></tr>
<tr><td colspan="2">xxx</td></tr>
<tr><td>7</td><td>Subcontracting is not allowed.</td></tr>
<tr><td colspan="2">xxx</td></tr>
<tr><td>20</td><td>The bidder with the Lowest Calculated Bid shall submit ALL of the following post-qualification requirements:

xxx</td></tr>
</table></td><td>Section III. Bid Data Sheet
<table>
<tr><th>ITB Clause</th><th></th></tr>
<tr><td colspan="2">xxx</td></tr>
<tr><td>7</td><td><s>Subcontracting is not allowed</s>. SUBCONTRACTING WILL BE ALLOWED FOR THE TRAINING COMPONENT OF THIS PROJECT.</td></tr>
<tr><td colspan="2">xxx</td></tr>
<tr><td>20</td><td>The bidder with the Lowest Calculated Bid shall submit ALL of the following post-qualification requirements:

xxx</td></tr>
</table></td></tr>
</table>

	5. At least two (2) of the following certifications and accreditation for Cyber Security Operation Center (SOC): i. The Open Group Architecture Framework (TOGAF); ii. Certified Ethical Hacker (CEH); iii. Certification in Information Technology Infrastructure Library (ITIL) Framework; iv. Certified Information Security Manager (CISM); v. CISCO Certified Network Professional (CCNP) or any equivalent certification from other technology provider; vi. Palo Alto Networks Certified Network Security Administrator (PCNSA) or any equivalent certification from other technology provider; vii. Fortinet Certified Network Security or any equivalent certification from other technology provider; and/or viii. COMPTIA Security + or any equivalent security certification.		5. ~~At least two (2) of the following certifications and accreditation for Cyber Security Operation Center (SOC):~~ **ANY TWO (2) OF THE FOLLOWING CERTIFICATIONS OF THE POOL OF PROFESSIONALS WHO WILL HANDLE THE DBM AND SOC MONITORING INCIDENTS:** i. The Open Group Architecture Framework (TOGAF); ii. Certified Ethical Hacker (CEH); iii. Certification in Information Technology Infrastructure Library (ITIL) Framework; iv. Certified Information Security Manager (CISM); v. CISCO Certified Network Professional (CCNP) or any equivalent certification from other technology provider; vi. Palo Alto Networks Certified Network Security Administrator (PCNSA) or any equivalent certification from other technology provider; vii. Fortinet Certified Network Security or any equivalent certification from other technology provider; and/or viii. COMPTIA Security + or any equivalent security certification.

Section VII. Technical Specifications **Annex "A"** **Detailed Technical Specifications** xxx	**Section VII. Technical Specifications** **Annex "A"** **Detailed Technical Specifications (REVISED)** xxx
4. QUALIFICATIONS OF THE CONTRACTOR	**4. QUALIFICATIONS OF THE CONTRACTOR**
4.3. The contractor must have a pool of Certified Professionals who will handle DBM SOC monitoring and security incidents, these professionals shall have the following certifications: 4.3.1 Certified Information Security Manager (CISM) or any equivalent certification 4.3.2 CISCO Certified Network Professional (CCNP) 4.3.3 Palo Alto Networks Certified Network Security Administrator (PCNSA) 4.3.4 Fortinet Certified Network Security NE7 35 4.3.5 COMPTIA Security + or any equivalent security certification Each of the certification shall belong to a different individual and shall be submitted as post-qualification requirement.	4.3 The contractor must have a pool of Certified Professionals who will handle DBM SOC monitoring and security incidents, these professionals shall have **ANY TWO (2) OF** the following certifications: 4.3.1 ~~Certified Information Security Manager (CISM) or any equivalent certification~~ **THE OPEN GROUP ARCHITECTURE FRAMEWORK (TOGAF)** 4.3.2 ~~CISCO Certified Network Professional (CCNP)~~ **CERTIFIED ETHICAL HACKER (CEH) OR ANY EQUIVALENT CERTIFICATION** 4.3.3 ~~Palo Alto Networks Certified Network Security Administrator (PCNSA)~~ **CERTIFIED IN INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) FRAMEWORK** 4.3.4 ~~Fortinet Certified Network Security NE7 35~~ **CERTIFIED INFORMATION SECURITY MANAGER (CISM)** 4.3.5 ~~COMPTIA Security + or any equivalent security certification~~ **CISCO CERTIFIED NETWORK PROFESSIONAL (CCNP) OR ANY EQUIVALENT CERTIFICATION FROM OTHER TECHNOLOGY PROVIDER** **4.3.6 PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ADMINISTRATOR (PCNSA) OR ANY EQUIVALENT CERTIFICATION FROM OTHER TECHNOLOGY PROVIDER** **4.3.7 FORTINET CERTIFIED NETWORK SECURITY OR ANY EQUIVALENT CERTIFICATION FROM OTHER TECHNOLOGY**

	PROVIDER; AND **4.3.8 COMPTIA SECURITY + OR ANY EQUIVALENT SECURITY CERTIFICATION.** ~~Each of the certification shall belong to a different individual and shall be submitted as post-qualification requirement.~~ **4.4 THE CONTRACTOR MUST HAVE A SOC 2 TYPE II ATTESTATION REPORT AND/OR ISO 27001 CERTIFICATION FOR MANAGED INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICES OR SIMILAR, DONE AT LEAST IN 2021, TO ENSURE CONTROLS RELATED TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY AND PRIVACY ARE IN PLACE. THE SAID REPORT AND/OR CERTIFICATION SHALL BE SUBMITTED AS POST QUALIFICATION REQUIREMENT.**
5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK	**5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK**
xxx	xxx
5.1.1.14 The proposed solution should provide 12-months data retention and unlimited data ingestion.	5.1.1.14 The proposed solution should provide 12 months data retention and ~~unlimited data~~ ingestion **FROM 1500 DEVICES SPECIFIED IN ITEM 5.1.1.15.**
5.1.1.15 The proposed solution should enroll 1300 assets of DBM which includes Desktop, Laptop, Servers, and Network Equipment.	5.1.1.15. The proposed solution should enroll ~~1300~~ **1,500** assets of DBM which includes Desktop, Laptop, Servers, and Network Equipment.
xxx	xxx
	5.1.1.20 SUPPLY CHAIN DEFENSE **5.1.1.20.1. THE SOC MUST BE ABLE TO CONTINUOUSLY MONITOR AND IDENTIFY KEY CYBER RISKS OF THE THIRD PARTIES IDENTIFIED BY DBM.** **5.1.1.20.2. THE SOC MUST BE ABLE TO DIRECTLY COORDINATE AND ASSIST VENDORS IN REMEDIATING THEIR**

	CYBER RISK ON BEHALF OF DBM. **5.1.1.20.3. THE SOC MUST BE ABLE TO ALERT DBM AND ITS THIRD PARTIES WHENEVER THEY MAY BE AFFECTED BY ZERO-DAY VULNERABILITIES BASED ON THE ACTUAL CYBER FINDINGS FROM MONITORING.**
xxx	xxx
5.1.2. Security Information and Event Management (SIEM)	**5.1.2. Security Information and Event Management (SIEM)**
xxx	xxx
5.1.2.2. The SIEM should have the capability to seamlessly integrate with Microsoft 365, utilizing XDR for identity, email, endpoint, and multi-cloud functions. Additionally, it should be able to ingest log sources at no additional cost to DBM.	5.1.2.2. The SIEM should have the capability to seamlessly integrate with **1300** Microsoft 365 **USERS**, utilizing XDR for identity, email, **1500** endpoint **USERS**, and multi-cloud functions. Additionally, it should be able to ingest **MICROSOFT** log sources at no additional cost to DBM.
xxx	xxx
5.1.4.10. The SOC solution shall deliver threat intelligence on the following:	5.1.4.10. The SOC solution shall deliver threat intelligence on the following:
5.1.4.10.1 Brand protection - company names/domain	5.1.4.10.1 Brand protection - company names/domain
5.1.4.10.1 Social Media Pages	~~5.1.4.10.1~~ **5.1.4.10.2** Social Media Pages
5.1.4.10.2 External Internet Protocol (IP) addresses	~~5.1.4.10.2~~ **5.1.4.10.3** External Internet Protocol (IP addresses
5.1.4.10.3 Website and mobile application monitoring	~~5.1.4.10.3~~ **5.1.4.10.4** Website and mobile application monitoring
5.1.4.10.4 VIP e-mails	~~5.1.4.10.4~~ **5.1.4.10.5** VIP e-mails
5.1.4.10.5 Sector monitoring Financial, Government, Insurance, and Healthcare	~~5.1..4.10.5~~ **5.1.4.10.6** Sector monitoring Financial, Government, Insurance, and Healthcare
5.1.4.10.6 GitHub	~~5.1.4.10.6~~ **5.1.4.10.7** GitHub
5.1.4.10.7 Custom queries	~~5.1..4.10.7~~ **5.1.4.10.8** Custom queries
5.1.4.10.8 Malicious sites during the duration of the contract (i.e., phishing, social media sites, and others)	~~5.1.4.10.8~~ **5.1.4.10.9**Malicious sites during the duration of the contract (i.e., phishing, social media sites, and others
5.1.4.10.9 Databases that contain large amounts of data found in the deep and dark web	~~5.1.4.10.9~~ **5.1.4.10. 10** Databases that contain large amounts of data found in the deep and dark web
5.1.4.10.10 Third-party queries	~~5.1.4.10.10~~ **5.1.4.10.11** Third-party queries

5.1.4.10.11 Investigation 5.1.4.10.12 Threat library	~~5.1.4.10.11~~ **5.1.4.10.12** Investigation ~~5.1.4.10.12~~ **5.1.4.10.13** Threat Library
xxx	xxx
5.4.11 The contractor shall provide Technical Trainings with certifications to be conducted by an Authorized IT Security Training Centers. The Technical Training should be a classroom type based on the following schedule.	5.4.11 The contractor shall provide Technical Trainings with certifications to be conducted by an Authorized IT Security Training Centers. The Technical Training should be a **FACE TO FACE** classroom type **SETUP** based on the following schedule. **ANY CHANGES IN THE METHOD OF INSTRUCTION AND SCHEDULE OF TECHNICAL TRAINING SHALL BE APPROVED BY THE DBM-OCIO**.
xxx	xxx
5.5 During the subscription period, the contractor shall provide/render twenty-four (24) hours a day, seven (7) days a week technical support service. xxx Problems reported/concerns shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report.	5.5 During the subscription period, the contractor shall provide/render twenty-four (24) hours a day, seven (7) days a week technical support service. xxx ~~Problems reported/concerns shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report~~.
xxx	xxx
5.7.2 The contractor shall conduct a monthly vulnerability assessment on all DBM's critical and public facing applications/servers. The contractor shall use Common Vulnerability Scoring System (CVSS) version 3.1 or later for risk ranking and prioritizing security vulnerabilities.	5.7.2 The contractor shall conduct a monthly vulnerability assessment on all DBM's critical and **TWENTY (20)** public facing applications/servers. The contractor shall use Common Vulnerability Scoring System (CVSS) version 3.1 or later for risk ranking and prioritizing security vulnerabilities.
xxx	xxx
5.7.4.3 **Vulnerability Assessment Report:** This report details the results of regular vulnerability assessments and penetration tests conducted on the organization's systems and networks. They identify vulnerabilities that need to be addressed to prevent potential breaches.	5.7.4.3 **Vulnerability Assessment Report:** This report details the results of regular vulnerability assessments ~~and penetration tests~~ conducted on the **DBM'S** ~~organization's~~ systems and networks. They identify vulnerabilities that need to be addressed to prevent potential breaches.
xxx	xxx
	5.9.9.7 THE REPORTED IT INCIDENT SHALL BE RESOLVED TO THE SATISFACTION OF THE DBM

WITHIN FOUR (4) HOURS FROM RECEIPT OF THE REPORT OR ON CASE TO CASE BASIS DEPENDING ON THE SEVERITY & COMPLEXITY OF THE INCIDENT.

xxx

Priority Code	Description	Incident Response Time*
xxx		

*** INCIDENT RESPONSE TIME REFERS TO THE NOTIFICATION TIME OR HOW LONG THE SERVICE PROVIDER NOTIFIES DBM OF AN INCIDENT.**

xxx

BID FORM

xxx

xxx

BID FORM
(Revised)

xxx

Particulars	Total Price
Subscription to the Cyber Security Operations Center (exclusive of VAT)	
Conduct of Training (exclusive of VAT)	
TOTAL (exclusive of VAT)	P
Add: 12% VAT	
TOTAL (inclusive of VAT)	P

xxx

	Note: **<u>Attached are the following documents which should be used as part of the Bidding Documents to be submitted by the bidders</u>:** **1. Annex "A" (Detailed Technical Specifications) (Revised)** **2. Bid Form (Revised)**
Queries: **<u>Training</u>** 1. Can the training sessions be done online/virtually? 2. Can the CompTIA+, CEH v12, CPENT training be conducted by a third party training provider and cost of which will be included in the bid proposal? **<u>Ownership of the License</u>** 3. Who owns the licenses pertaining to item 7.4 of the Warranties of the Contractor? **<u>Devices</u>** 4. Will the DBM provide the models/operating systems of assets identified in item 5.1.1.15? 5. Please provide the total number of workstation and servers and their operating system (OS) 6. Can you please provide the breakdown of the 1,300 assets (OS, Data Source Type, Location (HO/DR), Deployment Type (On-prem, VM, Cloud), and its quantity)	**Clarifications:** 1. The training session shall be done on a face to face classroom type training setup consistent with item 5.4.11 of the Revised Detailed Technical Specifications. 2. Yes. This can be provided by a third party provider which should qualify as authorized training center/s consistent with item 5.4.11 of the Revised Detailed Technical Specifications. Cost of these trainings should be included in the total bid amount. 3. The licenses being referred to under item 7.4 of the Revised Detailed Technical Specifications are pertinent business licenses issued to the bidder by pertinent authorities. Consistent with item 7.4 on the warranties of the contractor, the service provider **shall secure** registration, licenses, or permits required by national or local laws and shall comply with the rules, regulations, and directives of regulatory authorities and Commissions. 4. Yes. The *models/operating systems of assets identified* will be provided by the DBM during the pre-implementation meeting as indicated in item 5.2 of the Revised Detailed Technical Specifications. 5. The details on the workstation , servers, and their OS will be provided during the implementation after the contractor has signed the NDA consistent with items 5.2 and 8.1 of the Detailed Technical Specifications. 6. The breakdown of the assets will be provided during the pre-implementation meeting after the contractor has signed the NDA consistent with items 5.2 and 8.1 of the Revised Detailed Technical Specifications. For this project, the contractor shall integrate the existing end points

	for 1500 devices, instead of 1300, consistent with item 5.1.1.15 of the Revised Detailed Technical Specifications.
Coverage of Logs and Storage 7. What is the coverage of logs, when are the logs provided to DBM, and will the DBM provide storage as stated in item 5.4.1?	7. Item 5.4.1 of the Revised Detailed Technical Specifications provides that the contractor shall ensure the availability of the **ingested raw logs for at least twelve (12) months with comprehensive searchability.** The retention of the logs shall be within the duration of the contract, after which, the logs will be archived and given to the DBM in an agreed format. The logs, including evidence of security incidents, shall be tamper proof and made available for legal and regulatory purposes, as required.
8. Kindly confirm if the storage that DBM will provide will be in cloud or on-premises as this needs to be considered in the proposal to align on the requirement of cloud base SOC Platform.	8. During the implementation, the requirement for the storage of the raw logs will depend on the SOC solution to be deployed by the Contractor. At the end of the contract, the DBM will provide storage for the archived logs in the agreed format consistent with item 5.4.1 of the Revised Detailed Technical Specifications.
9. Are the 1300 assets all enrolled in the existing MS Defender? Will there be any on-prem log sources and log sources that do not have EDR? Such may require an on-prem log forwarder server.	9. Not all of the assets are enrolled in the existing MS Defender. It should be noted that the contractor shall provide licenses for the log collection as stipulated in item 5.1.1.15 of the Revised Detailed Technical Specifications.
10. Can you please share the breakup of 1300 log sources mentioned (Number of servers, firewall, Database, Applications, proxy etc.) ? Also share EPS/Log ingestion if handy	10. The details of the 1500 devices including the information on EPS/Log ingestion will be provided during the pre-implementation meeting, after the contractor has signed the NDA consistent with Items 5.1.1.15 and 8.1 of the Revised Detailed Technical Specifications.
11. During the pre-bid it was mentioned that there are 5-10 thousand endpoints but the TOR specifies only 1300. Please help clarify the number of endpoints.	11. Under item 5.1.1.15 of the Revised Detailed Technical Specifications, the number of devices has been revised to 1500 devices.
12. Is it okay to adjust the period of data retention to reflect - with 3 months online and 9 months archive data retention?	12. The DBM shall retain the terms under item 5.4.1 of the Revised Detailed Technical Specifications which provides that the contractor shall ensure the availability of the ingested raw logs for at least twelve (12) months with comprehensive searchability. The retention of the logs shall be within the duration of the contract, after which, the logs will be archived and given to the DBM in an agreed format.

Configuration Management Database	
13. Is there a configuration management database in place with all the asset details, role and criticality?	13. There is no configuration management database in place. For this project, the contractor shall integrate the existing end points for 1500 Devices consistent with Item 5.1.1.15 of the Revised Detailed Technical Specifications.
Use of DBM's Microsoft License	
14. Since you have an existing Microsoft E5 license, can the service provider use DBM's Microsoft Sentinel to deliver the SOC services?	14. No. The contractor should provide all the required licenses for the project consistent with item 5.1.1 of the Revised Detailed Technical Specifications.
15. Is Microsoft Defender Vulnerability Management agent already deployed on all the endpoints?	15. Not all endpoints have windows defender agent deployed. It is however noted that the contractor is expected to provide all the required licenses for the project consistent with item 5.1.1 of the Revised Detailed Technical Specifications.
Threat Intelligence Solution Integration	
16. Would the Threat Intelligence solution be integrated with the SIEM solution?	16. Yes. The Threat Intelligence solution should be integrated with the Subscription to the Cyber Security Operations Center as detailed under item 5.1.1.1 of the Revised Detailed Technical Specifications.
17. Do you have any commercial threat intelligence solution in place?	17. No. The DBM has no available threat intelligence solution in place, however as indicated in item 5.1.4 of the Revised Detailed Technical Specifications, the threat intelligence solution should be integrated in the SOC service.
Security Alert Notification and Advisory Service	
18. Do you have any security alert notification like security newsfeeds or threat indicator notification (paid/free subscription)?	18. Under this project, we do not require Security Alert Notification, instead, as stipulated in item 5.4.3 of the Revised Detailed Technical Specifications, the contractor must include onboarding and advisory services throughout the period of engagement.
19. What will be the expectations for the contractor in terms of the consultation/advisory services to be provided?	19. As indicated in item 5.4.4 of the Revised Detailed Specifications, for the advisory service, the contractor is expected to provide strategic and threat intelligence advisory by industry sector.
Response / Resolution Time	
20. Does the four-hour resolution time cover only P1/critical incidents?	20. On the resolution time, the reported IT incident shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report or on case to case basis depending on the severity & complexity of the incident.
21. Does the response time only cover acknowledgment of the incident?	21. No. The incident response time refers to the notification time or how long the service provider notifies DBM of an incident

22. For Level 1 Support, may we ask the average incident calls that DBM will potentially incur per month	22. There is no baseline data on the incident response as this is the first implementation of the subscription to SOC.
Installation of XDR Solution to provide Threat Hunting and Response Service 23. Can we assume that the MSP provider can install an agent on top of your XDR solution to provide Threat Hunting and Response Service and perform all of the requirements from 5.8.1 to 5.8.5?	23. Yes. As related to item 5.1.2.6 of the Revised Detailed Technical Specifications, the Contractor can install an agent on top of the XDR solution to provide Threat Hunting and Response Service.
Requirement for Takedown Services 24. Are you requiring unlimited take down services for fake applications, malicious servers, website, or social media accounts?	24. No. The project does not require unlimited take down services for fake applications, malicious servers, website, or social media accounts. As stipulated in item 5.1.1.14 of the Revised Detailed Technical Specifications, the proposed solution should provide 12-months data retention and data ingestion; and item 5.1.2.10 of the Revised Detailed Technical Specifications, the SOC solution must include log collection capabilities at no additional cost, circumventing peak event rates, data volume and number of log sources.
25. Rather than having an unlimited data ingestion that will affect to increase the pricing, please provide the breakdown of all data sources (OS, Data Source Type, Location (HO/DR), Deployment Type (On-prem, VM, Cloud), and its quantity) to properly size the requirement.	25. This project will not require unlimited data ingestion consistent with item 5.1.1.14 of the Revised Detailed Technical Specifications which states that the proposed solution should provide 12-months data retention and data ingestion. As to the breakdown of data sources, this will be provided during the pre-implementation meeting after the contractor has signed the NDA consistent with item 8.1 of the Revised Detailed Technical Specifications.
26. For 5.1.2.10 - Solution providers do not offer unlimited data ingestion capability/ feature. May we please ask for detailed information of log sources that will be ingested into SIEM for scoping and capacity planning during peak and non-peak events	26. Instead of unlimited data ingestion capability/ feature, as stipulated in item 5.1.1.14 of the Revised Detailed Technical Specifications, the proposed solution should provide 12-months data retention and data ingestion. As to the details of the log sources that will be ingested into SIEM, item 5.1.2.10 of the Revised Detailed Technical Specifications provides that the SOC solution must include log collection capabilities **at no additional cost, circumventing peak event rates, data volume and number of log sources.**
On Ad Hoc Consultation 27. Please clarify the ad-hoc consultation schedule (8x5, 24x7).	27. For this project, no ad-hoc consultation is being required. What is required instead is an ad-hoc

	report consistent with item 5.1.2.1 of the Revised Detailed Technical Specifications.
Existing Score Card Solution 28. Does the DBM have an existing Security Score Card Solution or an equivalent Security Ratings & Cybersecurity Risk Management Solution on which we will collect data.	28. The DBM has no existing scorecard or an equivalent Security Ratings & Cybersecurity Risk Management Solution. This is also not a requirement under the project, since the project is a subscription.
Composition of the SOC Solution 29. Does the SOC Platform pertains to SIEM and SOAR?	29. The SOC solution should be composed of integrated SIEM, SOAR, Threat Intelligence, and User and Entity Behavior Analytics (UEBA) as indicated in item 5.1.1.1 of the Revised Detailed Technical Specifications.
Data Sources 30. Is the Microsoft 365 and XDR solution of DBM part of the data sources that must be ingested in the MSP SOC Platform to provide context for identity, email, endpoint, and multi-cloud functions?	30. Yes. The Microsoft 365 and cortex XDR solution will be a part of the data sources.
Vulnerability Management Solution 31. Can we assume that DBM has an existing Vulnerability Management solution to incorporate vulnerability data to the MSP SOC Platform? If not, do we need to consider this in our proposal? How many assets do we need to consider?	31. There's no existing vulnerability management solution, this solution is part of another procurement project, hence no need to include in the proposal.
Ownership of the License 32. Please verify if DBM is okay in owning the license.	32. The licenses for the Subscription to Cyber Security Operations Center shall be owned by the DBM.
33. Please verify if DBM has a valid Microsoft license for the duration of the project.	33. As to the Microsoft licenses, the DBM cannot provide information as this is not within the scope of the project.
On Cluster 34. In line with Item 5.1.1.11 of the Detailed Technical Specifications, Is DBM considered a cluster? If yes, how many agencies are part of the cluster?	34. The details of the clusters will be provided during the pre-implementation meeting, after the contractor has signed the NDA consistent with items 5.2 and 8.1 of the Revised Detailed Technical Specifications.
Schedule of the Requirements 35. Can the Delivery, Integration, and Configuration be extended to 90 days?	35. No. Consistent with item 5.4 of the Revised Detailed Technical Specifications, the delivery, integration and configuration of SOC shall be within 60 days upon the receipt of Notice to Proceed.
36. Please clarify if license duration should cover both "Delivery, Integration, and Configuration of the Cyber Security Operations Center (SOC)"	36. The subscription period does not cover the period of Delivery, Integration and Configuration. The subscription period will only start once the

and "Subscription to Cyber Security Operation," which is 12 months + 60 days equivalent to 14 months?	Delivery, Integration and Configuration has been completed consistent with item 5.4 of the Revised Detailed Technical Specifications. The maximum period to complete the project is 14 months.
37. What is the duration of the SIEM? Annual?	37. The duration of the SIEM is annual in accordance with items 3 & 5.1.1.1 of the Revised Detailed Technical Specifications.
Qualification of the Contractor 38. Can the contractor be a consulting firm with experience in cybersecurity?	38. No. As stipulated in item 4.1 of the Revised Detailed Technical Specifications, **the contractor must have at least five (5) years of experience in the IT Security industry** based on the Securities and Exchange Commission Registration to be submitted as one of the post-qualification requirements.
39. Does the pool of certified professional who will handle DBM SOC monitoring and security incident must be with the service provider's organization at least one (1) year before the bid opening and must submit Resume/CV of the Proposed Personnel, Company ID, and Certificate of Employee for all the personnel to be assigned.	39. No. The pool of Certified Professionals **is only** required to provide proof of certifications for the following as indicated in item 4.3 of the Revised Detailed Technical Specifications: i. The Open Group Architecture Framework (TOGAF) ii. Certified Ethical Hacker (CEH) or any equivalent certification iii. Certified in Information Technology Infrastructure Library (ITIL) Framework iv. Certified Information Security Manager (CISM) v. Cisco Certified Network Professional (CCNP) or any equivalent certification from other technology provider vi. Palo Alto Networks Certified Network Security Administrator (PCNSA) or any equivalent certification from other technology provider vii. Fortinet Certified Network Security or any equivalent certification from other technology provider; and viii. COMPTIA SECURITY + or any equivalent security certification. There is no need to submit Resume/CV of the Proposed Personnel, Company ID, and Certificate of Employes. Further, the project has no requirements as to how long the assigned personnel has been employed with the Contractor.
40. Does any of the following be considered as an equivalent to Certified Information Security Manager (CISM)?	40. No. CISSP, CEH, CTIA, and ECIH **are not considered** as an equivalent certification for Certified Information Security Manager (CISM).

• Certified Information Systems Security Professional (CISSP) • Certified Ethical Hacker (CEH) • EC Council Certified Threat Intelligence Analyst (CTIA) • EC Council Certified Incident Handler (ECIH)	
41. For network related certifications such as CCNP, PCNSA, Fortinet NE7, are these mandatory requirements since management of firewalls/other network devices is not within the scope of the project?	41. Yes. These are mandatory requirements which shall be submitted as post-qualification documents. Consistent with item 4.3 of the Revised Detailed Technical Specifications, the pool of Certified Professionals shall provide proof of certifications as part of the post qualification requirements for the following: i. The Open Group Architecture Framework (TOGAF) ii. Certified Ethical Hacker (CEH) or any equivalent certification iii. Certified in Information Technology Infrastructure Library (ITIL) Framework iv. Certified Information Security Manager (CISM) v. Cisco Certified Network Professional (CCNP) or any equivalent certification from other technology provider vi. Palo Alto Networks Certified Network Security Administrator (PCNSA) or any equivalent certification from other technology provider vii. Fortinet Certified Network Security or any equivalent certification from other technology provider; and viii. COMPTIA SECURITY + or any equivalent security certification.
42. Can we relax the qualifications of the contractor?	42. The qualification for the contractor has been eased allowing the bidders to submit any two of the certifications regardless if it belongs to a different individual or not as reflected in 4.3 of the revised Detailed Technical Specifications. Note however that Items 4.1 and 4.2 of the Revised Detailed Technical Specifications have been retained.
<u>Bidder's Statement of All Ongoing Contracts</u> 43. Can the Value of Outstanding Contract in the Statement of Ongoing Contracts be ***<u>smaller</u>*** than the Value of Outstanding Contracts in the NFCC Computation? The reason for this is that several clients refuse to disclose certain details, due to strict NDAs.	43. No. The bidder/s are requested to provide the amount consistent with GPPB Circular 04-2022 dated September 16, 2020 where for the Statement of the Bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, the following information are mandatory:

	i. Names of outstanding contracts with other contracting party, i.e., PE or private company allowed by the rules, contract date, period and **amount or value**; and **(emphasis supplied)** ii. For Goods, kinds of Goods and dates of delivery. GPPB Non-Policy Matter Opinion No. 041-2014 dated October 9, 2014 likewise provides 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."
44. Some of our clients are not willing to disclose certain details such as contract value and contract dates, original receipts. What can be done about this	44. GPPB Non-Policy Matter Opinion No. 041-2014 dated October 9, 2014 provides 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."
Single Largest Completed Contracts and Statement of All Ongoing Contracts 45. Can the requirement for SLCC be relaxed from SOC Solution to Manage Firewall?	45. No. The SOC solution on the SLCC shall be retained as the purpose of this requirement is to ensure that the contractor has the technical experience and capability to carry out the project.
Subcontracting 46. Can portions of the delivery be subcontracted? If Yes, up to what percentage is allowed?	46. Yes. In accordance with GPPB Resolution No. 15-2020, dated July 28, 2020, the contractor is allowed to subcontract a portion of the project and shall be limited to twenty percent (20%) of the project. For this project, sub-contracting will be limited only to the conduct of trainings from third party provider consistent with ITB Clause 7 of the Bid Data Sheet and item 5.4.11 of the Revised Detailed Technical Specifications. As to the requirements, GPPB Resolution No. 15-2020 provides that the **bidder may identify the subcontractor to whom a portion of the Works will be subcontracted at any stage of the bidding process or during contract implementation.** If the bidder opts to disclose the name of the subcontractor **during bid submission**, the bidder shall include the required documents as part of the

	technical components of the bid. A subcontractor that is identified during **contract implementation** must comply with the eligibility criteria and documentary requirements. The implementing or end-user unit shall determine whether the subcontractor complies with the eligibility criteria and documentary requirements, and secure the approval of the HoPE.
47. Is getting the services of an "Authorized IT Security Training Center" to conduct training and certification considered as subcontracting?	47. Yes. For the case of this project, sub- contracting will be limited only to the conduct of trainings from third party provider consistent with ITB Clause 7 of the Bid Data Sheet. The amount of which shall not exceed 20% of the project in accordance with the Bidding Documents.
Schedule of the Submission and Opening of Bids 48. Due to the Public Holidays in PH, can we request for an extension of 1 week for Proposal Submission?	48. The schedule of submission and opening of Bids has been moved from November 7, 2023 to November 17, 2023.

Other matters:

- The "No Contact Rule" shall be strictly observed. Bidders are not allowed to communicate with any member of the Bids and Awards Committee, Technical Working Group or Secretariat effective November 14, 2023 right after the opening of bids.

- For guidance and information of all concerned.

Digitally signed by Ramon Vicente B. Asuncion

RAMON VICENTE B. ASUNCION
Director IV
Vice Chairperson, DBM-BAC

Annex “A”

DETAILED TECHNICAL SPECIFICATIONS
(Revised)

1. PROJECT TITLE

Subscription to Cyber Security Operations Center (SOC)

2. OBJECTIVES

The Subscription to Cyber SOC aims to:

1. Continuously monitor the DBM's network, systems, applications, and digital assets to detect and identify any suspicious or malicious activities, such as unauthorized access, data breaches, malware infections, and other cyber threats;
2. Proactively implement preventive measures to stop potential threats before they can cause harm. This involves implementing advanced security technologies, conducting vulnerability assessments, and applying security best practices to reduce the organization's attack surface; and
3. Rapidly respond to security incidents to minimize their impact and prevent their escalation. This involves analyzing incidents, identifying their root causes, containing threats, and implementing effective mitigation strategies.

3. DURATION OF THE SUBSCRIPTION

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

4. QUALIFICATIONS OF THE CONTRACTOR

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

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

4.3 The contractor must have a pool of Certified Professionals who will handle DBM SOC monitoring and security incidents, these professionals shall have any two (2) of the following certifications:

4.3.1 The Open Group Architecture Framework (TOGAF)
4.3.2 Certified Ethical Hacker (CEH) or any equivalent certification
4.3.3 Certified in Information Technology Infrastructure Library (ITIL) Framework
4.3.4 Certified Information Security Manager (CISM)
4.3.5 Cisco Certified Network Professional (CCNP) or any equivalent certification from other technology provider
4.3.6 Palo Alto Networks Certified Network Security Administrator (PCNSA) or any equivalent certification from other technology provider
4.3.7 Fortinet Certified Network Security or any equivalent certification from other technology provider; and
4.3.8 COMPTIA SECURITY + or any equivalent security certification.

4.4 The contractor must have a SOC 2 Type II Attestation report and/or ISO 27001 certification for managed information and communications technology services or similar, done at least in 2021, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in place. This shall be submitted as a post qualification requirement.

5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK

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

5.1.1 SOC

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

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

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

5.1.1.2.1 Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

5.1.1.2.2 Detect previously undetected threats and minimize false positives using built-in analytics and threat intelligence.

5.1.1.2.3 Investigate threats with artificial intelligence, and hunt for suspicious activities based on the scale of severity.

5.1.1.2.4 Respond to incidents rapidly using built-in orchestration and automation of common tasks.

5.1.1.3 The SOC solution is capable for User and Entity Behavior Analytics (UEBA), which:

5.1.1.3.1 collects logs and alerts from all of its connected data sources;

5.1.1.3.2 Analyzes these logs and alerts; and

5.1.1.3.3 Builds baseline behavioral profiles of DBM entities (such as users, hosts, IP addresses, and application across time and peer group horizon, which shall provide the following information:

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

identify anomalous activities and present evidence clearly and concisely in the form of *contextual enrichments*.

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

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

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

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

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

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

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

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

5.1.1.9.1 Incident created over time
5.1.1.9.2 Incidents created by closing classification, severity, owner, and status
5.1.1.9.3 Mean time to triage
5.1.1.9.4 Mean time to closure
5.1.1.9.5 Incidents created by severity, owner, status, product, and tactics over time
5.1.1.9.6 Time to triage percentiles
5.1.1.9.7 Time to closure percentiles
5.1.1.9.8 Mean time to triage per owner
5.1.1.9.9 Recent activities
5.1.1.9.10 Recent closing classifications

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

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

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

5.1.1.14. The proposed solution should provide 12-months data retention and data ingestion from 1500 devices specified in item 5.1.1.15.

5.1.1.15. The proposed solution should enroll 1500 assets of DBM which includes Desktop, Laptop, Servers, and Network Equipment.

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

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

5.1.1.17.1. **Critical (Priority 1):** security events with highest level of severity, posing an immediate and significant threat to DBM's IT system, data, and operations.
5.1.1.17.2. **High (Priority 2):** security events that have a substantial impact on IT resources, potentially affecting critical systems, services, or sensitive data.
5.1.1.17.3. **Medium (Priority 3):** security events that have noticeable impact but may not require immediate action.
5.1.1.17.4. **Low (Priority 4):** security events with minimal immediate impact and lower likelihood of causing significant harm.

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

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

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

5.1.1.20.1 The SOC must be able to continuously monitor and identify key cyber risks of the third parties identified by DBM.

5.1.1.20.2 The SOC must be able to directly coordinate and assist vendors in remediating their cyber risk on behalf of DBM.

5.1.1.20.3 The SOC must be able to alert DBM and its third parties whenever they may be affected by zero-day vulnerabilities based on the actual cyber findings from monitoring.

5.1.2. Security Information and Event Management (SIEM)

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

5.1.2.2. The SIEM should have the capability to seamlessly integrate with 1300 Microsoft 365 USERS, utilizing XDR for identity, email, 1500 endpoint USERS, and multi-cloud functions. Additionally, it should be able to ingest Microsoft log sources at no additional cost to DBM.

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

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

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

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

5.1.2.7. The SOC solution must have a global threat intelligence subscription service for data enrichment to quickly identify

attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.

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

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

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

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

5.1.3. Security Orchestration, Automation and Response (SOAR)

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

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

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

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

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

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

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

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

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

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

- 5.1.3.9.1 Phishing enrichment and response
- 5.1.3.9.2 Malware endpoint response
- 5.1.3.9.3 Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc.)
- 5.1.3.9.4 Unusual browsing activity
- 5.1.3.9.5 Web attack profiling and blacklisting

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

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

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

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

5.1.4. Threat Intelligence (TI)

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

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

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

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

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

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

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

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

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

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

5.1.4.10.1. Brand protection – company names/domain
5.1.4.10.2. Social media pages
5.1.4.10.3. External Internet Protocol (IP) addresses

5.1.4.10.4. Website and mobile application monitoring
5.1.4.10.5. VIP e-mails
5.1.4.10.6. Sector monitoring Financial, Government, Insurance, and Healthcare
5.1.4.10.7. GitHub
5.1.4.10.8. Custom queries
5.1.4.10.9. Malicious sites during the duration of the contract (i.e., phishing, social media sites, and others)
5.1.4.10.10. Databases that contain large amounts of data found in the deep and dark web
5.1.4.10.11. Third-party queries
5.1.4.10.12. Investigation
5.1.4.10.13. Threat library

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4.11 The contractor shall provide Technical Trainings with certifications to be conducted by an Authorized IT Security Training Centers. The Technical Training should be a face to face classroom type setup based on the following schedule. Any changes in the method of instruction and schedule of technical training shall be approved by the DBM-OCIO.

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

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

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

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

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

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

5.7.2 The contractor shall conduct a monthly vulnerability assessment on all DBM's critical and twenty (20**)** public facing applications/servers. The contractor shall use Common Vulnerability Scoring System (CVSS) version 3.1 or later for risk ranking and prioritizing security vulnerabilities.

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

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

The SOC monthly report shall include the following:

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

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

5.7.4.3 **Vulnerability Assessment Report:** This report details the results of regular vulnerability assessments conducted on the **DBM'S** systems and networks. They

identify–vulnerabilities that need to be addressed to prevent potential breaches.

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

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

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

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

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

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

5.8 Threat Hunting and Response

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

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

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

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

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

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

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

5.8.5.3 The contractor must be able to:

5.8.5.3.1.1. Detect servers launching phishing attacks and take necessary actions.

5.8.5.3.1.2 Take down fake applications that impersonate legitimate ones.

5.8.5.3.1.3 Take immediate action and provide all the context to execute take-down of malicious

servers, websites or social media accounts.

5.9 Incident Response

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

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

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

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

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

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

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

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

5.9.8 The contractor shall deliver insider threat investigation.

5.9.9 The contractor shall assist in the following:

5.9.9.1 Incident handling preparation and execution
5.9.9.2 Crisis management
5.9.9.3 Breach communication

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

5.9.9.5 Remediation

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

5.9.9.7 The reported IT incident shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report or on case to case basis depending on the severity & complexity of the incident.

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

* Incident Response Time refers to the notification time or how long the service provider notifies DBM of an incident.

6. SERVICE LEVEL AGREEMENT

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

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

SOC Platform Availability	As detailed in item 5.1.1.19 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per minute of downtime.
Technical Support	As detailed in item 5.5 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per hour of delay.
Submission of Monthly Cyber SOC Reports	As detailed in item 5.7.4 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per day of delay.
Incident Response Time	As detailed in item 5.9 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per hour of delay.
Technical Training	As detailed in item 5.4.11 of this Detailed Technical Specifications	1/10th of 1% of the monthly payment shall be imposed per day of delay.

7. WARRANTIES OF THE CONTRACTOR

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

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

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

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

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

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

7.7 The contractor shall be liable for loss, damage, or injury caused directly or indirectly through the fault or negligence of its technical

staff assigned. It shall assume full responsibility therefore and the DBM shall be fully released from any liability arising therefrom.

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

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

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

8. CONFIDENTIALITY OF DATA

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

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

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

9. TERMS OF PAYMENT

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

9.1.1 As-built documentation in accordance to item 5.6 of the Detailed Technical Specifications

9.1.2 NDA in accordance to item 8.1 of the Detailed Technical Specifications

9.1.3 SOC Monthly Report, which shall include the following:

- Incident Report
- Threat Intelligence Report
- Vulnerability Assessment Report
- Log Analysis Report
- User Activity Report

- Security Incident Response Plans (SIRP) Report
- Dashboard and Metric Report
- Executive Summary Report
- Cyber Security Update

9.1.4 Sales Invoice / Billing Statement

9.1.5 Training Certificates and Training Materials in accordance to the item 5.4.11 of the Detailed Technical Specifications

9.1.6 Certificate of Acceptance issued by the DBM- ICTSS to be issued on a Monthly basis

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

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

BID FORM

Date : _____
Project Identification No. : **DBM-2024-05**

To: [name and address of Procuring Entity]

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers *[insert numbers]*, the receipt of which is hereby duly acknowledged, we, the undersigned, offer **Subscription to Cyber Security Operations Center** in conformity with the said PBDs for the sum of ***[total Bid amount in words and figures]*** or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the details provided herein and made part of this Bid. The total bid price includes the cost of all taxes.

Particulars	**Total Price**
Subscription to the Cyber Security Operations Center (exclusive of VAT)	
Conduct of Training (exclusive of VAT)	
TOTAL (Exclusive of VAT)	P
Add: 12% VAT	
TOTAL (Inclusive of VAT)	P

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: _____