REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF BUDGET AND MANAGEMENT

GENERAL SOLANO ST., SAN MIGUEL, MANILA

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 1

This SBB No. 1 dated October 24, 2023 for **Project No. DBM-2024-02, "Subscription to the Vulnerability Assessment and Penetration Testing (VAPT) for the Department of Budget and Management,"** 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.

PARTICULARS			**AMENDMENTS/ CLARIFICATIONS**	
Section III. Bid Data Sheet			**Section III. Bid Data Sheet**	
ITB Clause			**ITB Clause**	
5.3	For this purpose, contracts similar to the Project shall: a. refer to the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks. If the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks forms part of a bigger contract, only the cost component of the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks shall be considered for purposes of comparing the value thereof to at least fifty		**5.3**	For this purpose, contracts similar to the Project shall: a. refer to the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, **OR SUBSCRIPTION TO, AND IMPLEMENTATION OF, CYBER SECURITY DETECTION AND RESPONSE SOLUTIONS**. If the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, **OR SUBSCRIPTION TO, AND IMPLEMENTATION OF, CYBER SECURITY DETECTION AND RESPONSE SOLUTIONS**. form~~s~~ part of a bigger contract, only the cost component of the subscription to the deployment

	percent (50%) of the ABC; and xxx		and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, **OR SUBSCRIPTION TO, AND IMPLEMENTATION OF, CYBER SECURITY DETECTION AND RESPONSE SOLUTIONS**. shall be considered for purposes of comparing the value thereof to at least fifty percent (50%) of the ABC; and xxx
xxx		xxx	
20	The bidder with the Lowest Calculated Bid shall submit ALL of the following post-qualification requirements: xxx 4. Securities Exchange Commission Registration. 5. Certifications, either as Ethical Hacker or Penetration Tester Professional, of the local contractor's pool of testers	**20**	The bidder with the Lowest Calculated Bid shall submit ALL of the following post-qualification requirements: xxx 4. ~~Securities Exchange Commission Registration.~~ **BUREAU OF INTERNAL REVENUE (BIR) CERTIFICATE OF REGISTRATION (COR BIR FORM 2303)** 5. Certifications, either as Ethical Hacker, ~~or~~ Penetration Tester Professional, **OR EQUIVALENT CYBERSECURITY CERTIFICATIONS, SUCH AS INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM (ISC2),** of the local contractor's pool of testers.
Section VII. Technical Specifications **xxx** **Annex A** **Detailed Technical Specifications**		**Section VII. Technical Specifications (REVISED)** **xxx** **Annex A** **Detailed Technical Specifications**	

xxx		**xxx**
4. QUALIFICATIONS OF THE CONTRACTOR		**4. QUALIFICATIONS OF THE CONTRACTOR**
4.1. The contractor must have at least five (5) years in the IT Security Industry based on the Securities and Exchange Commission Registration to be submitted as post-qualification requirement.		4.1. The contractor must have at least five (5) years of **EXPERIENCE** in ~~the~~ IT ~~Security~~ Industry or **CONSULTING BUSINESS** based on the ~~Securities and Exchange Commission Registration~~ **BUREAU INTERNAL REVENUE (BIR) CERTIFICATE OF REGISTRATION (COR BIR FORM 2303)** to be submitted as post-qualification requirement**.**
4.2 The contractor must have a pool of testers that has any of the following certifications, which shall be submitted as post-qualification requirement: 4.2.1 Ethical Hacker; or 4.2.2 Penetration Tester Professional.		4.2 The contractor must have a pool of testers that has any of the following certifications, which shall be submitted as post-qualification requirement: 4.2.1 Ethical Hacker; ~~or~~ 4.2.2 Penetration Tester Professional; or 4.2.3 **EQUIVALENT CYBERSECURITY CERTIFICATIONS, SUCH AS INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM (ISC2).**
5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK		**5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK**
5.1 The contractor shall provide a fully automated Software-as-a-Service (SaaS) VAPT solution with the following features and functionality, but not limited to: 5.1.1. Can be integrated with the DBM's existing Web Application Firewall (WAF). 5.1.2. Can validate open services, WAF protection, employee credential usage, and CVE exploitability. 5.1.3 Can run vulnerability xxx. 5.1.4. Can describe vulnerabilities xxx. 5.1.5. Must suppress false positive vulnerabilities. 5.1.6. Can classify xxx. 5.1.7. Shall be able to test xxx 5.1.8. Shall be able xxx. 5.1.9. Can handle testing xxx. 5.1.10. Shall be able to xxx 5.1.11. The solution xxx. 5.1.12. Shall be able xxx. 5.1.13. Can detect xxx.		5.1 The contractor shall provide a ~~fully automated~~ Software-as-a-Service (SaaS) VAPT solution with the following features and functionality, but not limited to: ~~5.1.1. Can be integrated with the DBM's existing Web Application Firewall (WAF).~~ ~~5.1.2.~~ **5.1.1** Can validate open services, ~~WAF protection~~, employee credential usage, and CVE exploitability. ~~5.1.3~~ **5.1.2** Can run vulnerability xxx. ~~5.1.4~~. **5.1.3** Can describe vulnerabilities xxx. ~~5.1.5. Must suppress false positive vulnerabilities.~~ ~~5.1.6.~~ **5.1.4** Can classify xxx. ~~5.1.7.~~ **5.1.5** Shall be able to test xxx ~~5.1.8.~~ **5.1.6** Shall be able xxx. ~~5.1.9~~. **5.1.7** Can handle testing xxx. ~~5.1.10~~. **5.1.8** Shall be able to xxx ~~5.1.11.~~ **5.1.9** The solution xxx. ~~5.1.12.~~ **5.1.10** Shall be able xxx. ~~5.1.13.~~ **5.1.11** Can detect xxx.

5.1.14. Provide automated remediation playbooks for vulnerabilities.		~~5.1.14.~~ **5.1.12** Provide ~~automated~~ remediation playbooks for vulnerabilities.
5.1.15. Can provide Reporting, as follows:		~~5.1.15.~~ **5.1.13.** Can provide Reporting, as follows:
5.1.14.1 Must generate xxx		~~5.1.14.1~~ **5.1.13.1** Must generate xxx
5.1.14.2 Centralized xxx		~~5.1.14.2~~ **5.1.13.2** Centralized xxx
5.1.14.3 Various format xxx		~~5.1.14.3~~ **5.1.13.3** Various format xxx
5.1.14.4 Provide xxx.		~~5.1.14.4~~ **5.1.13.4** Provide xxx.
5.1.16. Artificial Intelligence xxx		~~5.1.16.~~ **5.1.14.** Artificial Intelligence xxx
5.1.14.5 Can identify xxx		~~5.1.14.5~~ **5.1.14.1** Can identify xxx
5.1.14.6 Identify critical xxx		~~5.1.14.6~~ **5.1.14.2** Identify critical xxx
5.1.14.7 Provide executive xxx		~~5.1.14.7~~ **5.1.14.3** Provide executive xxx
5.1.14.8 Provide threat xxx		~~5.1.14.8~~ **5.1.14.4** Provide threat xxx
5.1.17. Continuous Monitoring		~~5.1.17.~~ **5.1.15** Continuous Monitoring
5.1.14.9 Can provide xxx		~~5.1.14.9~~ **5.1.15.1** Can provide xxx
5.1.14.10 Can provide xxx		~~5.1.14.10~~ **5.1.15.2** Can provide xxx
5.1.18. Must have the following key benefits for the use of DBM:		~~5.1.18~~. **5.1.16** Must have the following key benefits for the use of DBM:
5.1.14.11 Continuous Assets xxx		~~5.1.14.11~~ **5.1.16.1** Continuous Assets xxx
5.1.14.12 GDPR/CCPA xxx		~~5.1.14.12~~ **5.1.16.2** GDPR/CCPA xxx
5.1.14.13 Exploitability xxx		~~5.1.14.13~~ **5.1.16.3** Exploitability xxx
5.1.14.14 Continuous visibility xxx		~~5.1.14.14~~ **5.1.16.4** Continuous visibility xxx
5.1.14.15 Reduce the risk xxx		~~5.1.14.15~~ **5.1.16.5** Reduce the risk xxx
5.1.14.16 Locate and xxx		~~5.1.14.16~~ **5.1.16.6** Locate and xxx
5.1.14.17 Better prioritize xxx		~~5.1.14.17~~ **5.1.16.7** Better prioritize xxx
5.1.14.18 Identify misconfigurations xxx		~~5.1.14.18~~ **5.1.16.8** Identify misconfigurations xxx
5.1.19. The VAPT Solution must have the following capabilities:		~~5.1.19.~~ **5.1.17.** The VAPT Solution must have the following capabilities:
5.1.14.19 AI Based prioritization.		~~5.1.14.19 AI Based prioritization.~~
5.1.14.20 AI based threat actor prediction.		~~5.1.14.20 AI based threat actor prediction.~~
5.1.14.21 Continuous discovery		~~5.1.14.21~~ **5.1.17.1** Continuous discovery
5.1.14.22 Alerts and Notifications		~~5.1.14.22~~ **5.1.17.2** Alerts and Notifications
5.1.14.23 Evidence Collection		~~5.1.14.23~~ **5.1.17.3** Evidence Collection
5.1.14.24 Exploitability Validation		~~5.1.14.24~~ **5.1.17.4** Exploitability Validation
5.1.14.25 Exploit Trends Identification		~~5.1.14.25~~ **5.1.17.5** Exploit Trends Identification
5.1.14.26 Risk Scoring		~~5.1.14.26~~ **5.1.17.6** Risk Scoring
5.1.14.27 SaaS breach validation		~~5.1.14.27~~ **5.1.17.7** SaaS breach validation
5.1.14.28 Data leak discovery		~~5.1.14.28~~ **5.1.17.8** Data leak discovery
5.1.14.29 Threat Intelligence - xxx		~~5.1.14.29~~ **5.1.17.9** Threat Intelligence - xxx
5.1.14.30 Multi-Factor Authentication.		~~5.1.14.30~~ **5.1.17.10** Multi-Factor Authentication.
5.1.14.31 Messaging Integrations.		
5.1.14.32 Technology Identification.		
5.1.14.33 Test Scheduling.		

		~~5.1.14.31~~ **5.1.17.11** Messaging Integrations. ~~5.1.14.32~~ **5.1.17.12** Technology Identification. ~~5.1.14.33~~ **5.1.17.13** Test Scheduling.
5.1.20. The VAPT Solution must have a dashboard for the following: 5.1.14.34 Infrastructure Assets xxx 5.1.14.35 Cloud Assets xxx 5.1.14.36 Websites • xxx • ML based identification 5.1.14.37 Number of employees xxx 5.1.14.38 Data leaks xxx		~~5.1.20.~~ **5.1.18.** The VAPT Solution must have a dashboard for the following: ~~5.1.14.34~~ **5.1.18.1** Infrastructure Assets xxx ~~5.1.14.35~~ **5.1.18.2** Cloud Assets xxx 5.1.14.36 **5.1.18.3** Websites • xxx • ~~ML based identification~~ ~~5.1.14.37~~ **5.1.18.4** Number of employees xxx ~~5.1.14.38~~ **5.1.18. 5** Data leaks
5.1.21. Shall use methodologies and frameworks based on industry standards and best practices such as the following: 5.1.14.39 Open Worldwide xxx 5.1.14.40 Penetration xxx 5.1.14.41 SysAdmin, xxx 5.1.14.42 National Institute xxx 5.1.14.43 Center of xxx 5.1.14.44 Cloud xxx 5.1.14.45 Exploit xxx 5.1.14.46 Adversarial xxx		5~~.1.21.~~ **5.1.19.** Shall use methodologies and frameworks based on industry standards and best practices such as the following: ~~5.1.14.39~~ **5.1.19.1** Open Worldwide xxx ~~5.1.14.40~~ **5.1.19.2** Penetration xxx ~~5.1.14.41~~ **5.1.19.3** SysAdmin, xxx ~~5.1.14.42~~ **5.1.19.4** National Institute xxx ~~5.1.14.43~~ **5.1.19.5** Center of xxx ~~5.1.14.44~~ **5.1.19.6** Cloud xxx ~~5.1.14.45~~ **5.1.19.7** Exploit xxx ~~5.1.14.46~~ **5.1.19.8** Adversarial xxx
5.1.22. The VAPT solution xxx		~~5.1.22.~~ **5.1.20.** The VAPT solution xxx **5.1.21. MUST PROVIDE ASSISTANCE IN PATCH MANAGEMENT TO TEST, IDENTIFY, AND PRIORITIZE PATCHING NEEDS AND APPLY FIXES, SOFTWARE UPDATES, ADD FEATURES THAT HELP IN MITIGATING VULNERABILITIES AND REDUCING THE RISK OF CYBER-ATTACKS.**
xxx		xxx
5.5 The contractor shall conduct the following on a monthly basis, during enhancements, and when necessary such as but not limited to:		5.5 The contractor shall conduct the following ~~on a monthly basis, during enhancements, and when necessary such as but not limited to~~: **ACTIVITIES USING THE METHODOLOGIES AND FRAMEWORKS BASED ON ANY INDUSTRY STANDARDS AND BEST PRACTICES:**
5.5.1. Perform discovery, vulnerability assessment, and penetration testing on the following DBM System Applications and IT Assets: 5.1.14.47 Twenty (20) xxx 5.1.14.48 Ten (10) DBM xxx		5.5.1. Perform **ONE (1)** discovery, vulnerability assessment, and penetration testing **USING GRAY BOX APPROACH AND BLACK BOX APPROACH, SUBJECT TO NECESSARY LEGAL**

5.1.14.49 One hundred forty xxx xxx 5.5.12. Shall submit the following xxx. 5.1.14.50 Executive Summary: xxx 5.1.14.51 Scope and Methodology: xxx 5.1.14.52 Risk Assessment: xxx 5.1.14.53 Detailed Findings: xxx 5.1.14.54 Exploitation Details: xxx 5.1.14.55 Recommendations: xxx 5.1.14.56 Appendix: xxx		**APPROVALS,** on the following DBM System Applications and IT Assets: ~~5.1.14.47~~ **5.5.1.1** Twenty (20) xxx ~~5.1.14.48~~ **5.5.1.2** Ten (10) DBM xxx ~~5.1.14.49~~ **5.5.1.3** One hundred forty xxx xxx 5.5.12. Shall submit the following xxx. ~~5.1.14.50~~ **5.5.12.1** Executive Summary: xxx ~~5.1.14.51~~ **5.5.12.2** Scope and Methodology: xxx ~~5.1.14.52~~ **5.5.12.3** Risk Assessment: xxx ~~5.1.14.53~~ **5.5.12.4** Detailed Findings: xxx ~~5.1.14.54~~ **5.5.12.5** Exploitation Details: xxx ~~5.1.14.55~~ **5.5.12.6** Recommendations: xxx ~~5.1.14.56~~ **5.5.12.7**Appendix: xxx
Statement of Single Largest Completed Contract which is Similar in Nature c. The similar contract for this Project shall refer to the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks. If the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks forms part of a bigger contract, only the cost component of the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks shall be considered for purposes of comparing the value thereof to at least fifty percent (50%) of the ABC.		**Statement of Single Largest Completed Contract which is Similar in Nature** **(REVISED)** c. The similar contract for this Project shall refer to the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, **OR SUBSCRIPTION TO, AND IMPLEMENTATION OF, CYBER SECURITY DETECTION AND RESPONSE SOLUTIONS.** If the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, **OR SUBSCRIPTION TO, AND IMPLEMENTATION OF, CYBER SECURITY DETECTION AND RESPONSE SOLUTIONS** form~~s~~ part of a bigger contract, only the cost component of the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, **OR SUBSCRIPTION TO, AND IMPLEMENTATION OF, CYBER SECURITY DETECTION AND RESPONSE SOLUTIONS** shall be considered for purposes of comparing the value thereof to at least fifty percent (50%) of the ABC.

Bid-Securing Declaration Form xxx ***[Jurat]*** *[Format shall be based on the latest Rules on Notarial Practice]*		**Bid-Securing Declaration Form** **(REVISED)** xxx ~~***[Jurat]***~~ ~~*[Format shall be based on the latest Rules on Notarial Practice]*~~ **SUBSCRIBED AND SWORN TO BEFORE ME IN [PLACE OF EXECUTION], PHILIPPINES ON THIS [DATE OF NOTARIZATION], AFFIANT EXHIBITING BEFORE ME HIS/HER COMPETENT EVIDENCE OF IDENTITY [VALID IDENTIFICATION ISSUED BY THE GOVERNMENT].** **NOTARY PUBLIC** **DOC. NO. __________;** **PAGE NO. __________;** **BOOK NO. __________;** **SERIES OF __________.**
Omnibus Sworn Statement xxx ***[Jurat]*** *[Format shall be based on the latest Rules on Notarial Practice]*		**Omnibus Sworn Statement** **(REVISED)** xxx ~~***[Jurat]***~~ ~~*[Format shall be based on the latest Rules on Notarial Practice]*~~ **SUBSCRIBED AND SWORN TO BEFORE ME IN [PLACE OF EXECUTION], PHILIPPINES ON THIS [DATE OF NOTARIZATION], AFFIANT EXHIBITING BEFORE ME HIS/HER COMPETENT EVIDENCE OF IDENTITY [VALID IDENTIFICATION ISSUED BY THE GOVERNMENT].** **NOTARY PUBLIC** **DOC. NO. __________;** **PAGE NO. __________;** **BOOK NO. __________;** **SERIES OF __________.**

		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. Statement of Single Largest Completed Contract which is Similar in Nature (Revised);** **3. Bid-Securing Declaration Form (Revised); and** **4. Omnibus Sworn Statement (Revised).**
Queries:		**Clarifications:**
1. For the Qualifications under the Detailed Technical Specifications, do you strictly require that the firm is in Information Technology (IT) business for at least five (5) years?		1. As reflected in item 4.1 of the revised Annex A (Detailed Technical Specifications), we require that the firm is in the **IT business/industry or consulting business for at least five (5) years**.
2. Can we just limit the Social Engineering activities to the conduct of monthly email phishing to 200 targeted individuals?		2. No, the social engineering simulation indicated under item 5.1.5 of the revised Annex A (Detailed Technical Specifications) shall not be limited to phishing activities. The activities for social engineering would be determined, as necessary.
3. Is the future IFMIS applications/systems already included in the total count of 20 public-facing application and 10 internal application?		3. Yes, the future IFMIS applications/systems are already included in the total count, as indicated in item 5.5.1 of the revised Annex A (Detailed Technical Specifications).
4. How many systems/applications are currently in the development pipeline?		4. There is no exact number as the systems/applications which are currently in the development pipeline will be based on the assessment to be conducted by the enterprise, solutions, and data architects that will be procured in a separate project.
5. Does the 12-month subscription include the setup?		5. No, consistent with item 2 of the revised Annex A (Detailed Technical Specifications), the Subscription Period for the project is twelve (12) months from the completion of the delivery, integration, and configuration phase or ***set up*** for the project. The contractor shall be able complete the set up (30) calendar days from the receipt of the Notice to Proceed consistent with item 5.5 of the revised Annex A (Detailed Technical Specifications).

6. Can we use an International project for our SLCC?		6. Yes, international projects can be used for the SLCC as long as it meets the requirements as stated in the SLCC form. Consistent with GPPB Resolution No. 16-2020, dated 16 September 2020, the SLCC submitted shall contain the following information: - Name of the completed contract with contract date, period and amount, which should correspond to the required percentage of the ABC to be bid. - Relevant period or delivery date when the said SLCC was completed Bidders are also advised to provide the contact information including working email and contract amount in peso denomination for purposes of validation.
7. Can other VAPT engagements, security risk assessments, or other similar projects qualify as SLCC?		7. Yes, as long as it qualifies as: - subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, or - subscription and implementation of cyber security detection and response solutions.
8. Do you require an automated remediation?		8. No, as indicated under item 5.1.12 of Annex A (Detailed Technical Specifications), we will no longer require an automated remediation.

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 October 31, 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 the Vulnerability Assessment and Penetration Testing (VAPT) for the Department of Budget and Management

2. OBJECTIVES

The project aims to systematically identify and prioritize vulnerabilities in the DBM's IT systems through automated scans, risk assessments, and controlled ethical hacking simulations.

The comprehensive evaluation through the subscription to VAPT shall exploit vulnerabilities, assess potential risks, and recommend actionable solutions, to enable the DBM to strengthen its cybersecurity posture, safeguard sensitive data, and ensure the integrity of its digital infrastructure against evolving threats. The subscription to VAPT shall cover independent assessments, including non-destructive tests, to evaluate the security posture internal and external DBM systems from a hacker's perspective.

This supports the prioritization of security requirements that will help the DBM achieve the following objectives:

2.1. Gain a better understanding of potential vulnerabilities and threats that may be visible from an external and internal network;

2.2. Assess and identify all weaknesses in the DBM application including its web application;

2.3. Identify the risk level to which DBM is exposed, so that appropriate countermeasures can be developed and applied; and

2.4. Raise awareness on Cybersecurity threats to DBM employees.

3. DURATION OF SUBSCRIPTION

The Subscription Period for the project is 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 Industry or consulting business based on the Bureau Internal Revenue (BIR) Certificate of Registration (COR BIR FORM 2303) to be submitted as post-qualification requirement.

4.1 The contractor must have a pool of testers that has any of the following certifications, which shall be submitted as post-qualification requirement:

4.1.1 Ethical Hacker;
4.1.2 Penetration Tester Professional; or
4.1.3 Equivalent cybersecurity certifications, such as international information system security certification consortium (ISC2).

5. TECHNICAL REQUIREMENTS AND SCOPE OF WORK

5.1 The contractor shall provide a Software-as-a-Service (SaaS) VAPT solution with the following features and functionality, but not limited to:

5.1.1 Can validate open services, employee credential usage and CVE exploitability.
5.1.2 Can run vulnerability assessment scan on one time and on continuous basis.
5.1.3 Can describe vulnerabilities per assets and mitigation.
5.1.4 Can classify and prioritize vulnerabilities based on AI Exploit Prediction Scoring System (EPSS).
5.1.5 Shall be able to test the internal and external-facing network services and resources of the DBM. Likewise, the scope of the vulnerability assessment will be limited to DBM's (production, testing, staging) environment underpinning the DBM. The project shall also include social engineering simulation on its management and employees.
5.1.6 Shall be able to have a security/vulnerability assessment to the DBM's Internal Applications/Systems, and existing Integrated Financial Management Information System (IFMIS) applications/systems.
5.1.7 Can handle testing of future IFMIS applications/systems that may be developed and/or identified within the subscription period.
5.1.8 Shall be able to have a security/vulnerability assessment to DBM domains, networks, servers, etc.
5.1.9 The solution can discover relative domains, detect known and unknown assets, discover sub-domains, IPV4/6, discover cloud assets of the DBM, discover DNS and email misconfiguration.
5.1.10 Shall be able to detect critical, high, medium, and low vulnerabilities. Risk score and exploitable vulnerabilities.
5.1.11 Can detect data leaks, cloud exposure, and employee credential data leaks.
5.1.12 Provide remediation playbooks for vulnerabilities.
5.1.13 Can provide Reporting, as follows:
5.1.13.1 Must generate report of vulnerabilities
5.1.13.2 Centralized dashboard
5.1.13.3 Various format for report downloads.
5.1.13.4 Provide report for top five (5) risks and per scan type.

5.1.14 Artificial Intelligence

5.1.14.1 Can identify sensitive data leakage with generative AI.
5.1.14.2 Identify critical paths for threat actors.
5.1.14.3 Provide executive exposures review.
5.1.14.4 Provide threat actor prediction and put in Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrix.

5.1.15 Continuous Monitoring
5.1.15.1 Can provide scorecard for health of external facing assets.
5.1.15.2 Can provide insights of attacks and actions to improve security posture.

5.1.16 Must have the following key benefits for the use of DBM:
5.1.16.1 Continuous Assets Discovery and Monitoring (CIS 1 & 2).
5.1.16.2 GDPR/CCPA Compliance (Leak Monitoring and Security by design).
5.1.16.3 Exploitability validation (BOD 22-01).
5.1.16.4 Continuous visibility during incident recovery (NIST - Recover).
5.1.16.5 Reduce the risk of unknown assets (blind spots/shadow IT).
5.1.16.6 Locate and remediate exposures faster & more effectively.
5.1.16.7 Better prioritize patch and remediation efforts.
5.1.16.8 Identify misconfigurations & process failures.

5.1.17 The VAPT Solution must have the following capabilities:
5.1.17.1 Continuous discovery
5.1.17.2 Alerts and Notifications
5.1.17.3 Evidence Collection
5.1.17.4 Exploitability Validation
5.1.17.5 Exploit Trends Identification
5.1.17.6 Risk Scoring
5.1.17.7 SaaS breach validation

5.1.17.8 Data leak discovery
5.1.17.9 Threat Intelligence - Employee Credential leak identification and validation.
5.1.17.10 Multi-Factor Authentication.
5.1.17.11 Messaging Integrations.
5.1.17.12 Technology Identification.
5.1.17.13 Test Scheduling.

5.1.18 The VAPT Solution must have a dashboard for the following:
5.1.18.1 Infrastructure Assets
- Subdomains - Total, Monitored and Exposed
- Hosts - Exposed ports per host

5.1.18.2 Cloud Assets

- Integrated and identified accounts – Total and Configured for testing
- Cloud Storage – Identified – Private and Publicly exposed

5.1.18.3 Websites

- Identified – Monitored and Vulnerable
- Behind Web Application or not
- Screenshots per identified service

5.1.18.4 Number of employees which leaked passwords were identified

5.1.18.5 Data leaks

5.1.19 Shall use methodologies and frameworks based on industry standards and best practices such as the following:

5.1.19.1 Open Worldwide Application Security Project (OWASP)

5.1.19.2 Penetration Testing Execution Standard (PTES)

5.1.19.3 SysAdmin, Audit, Network, and Security (SANS)

5.1.19.4 National Institute of Standards and Technology (NIST)

5.1.19.5 Center of Internet Security (CIS)

5.1.19.6 Cloud Security Alliance (CSA)

5.1.19.7 Exploit Prediction Scoring System (EPSS)

5.1.19.8 Adversarial Tactics, Techniques, and Common Knowledge or MITRE ATT&CK

5.1.20 The VAPT solution must be guaranteed with 99.9% uptime/ availability per month, with a monthly downtime cap of 43.2 minutes.

5.1.21 Must provide assistance in patch management to test, identify, and prioritize patching needs and apply fixes, software updates, add features that help in mitigating vulnerabilities and reducing the risk of cyber-attacks.

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 a week from the pre-implementation meeting with DBM representatives. Said work plan shall be validated and subject to approval of Undersecretary for Information and Communications Technology (ICT) Group.

5.4 The contractor shall deliver, integrate, and configure the VAPT Solution (as detailed in item 5.1) within thirty (30) calendar days from the receipt of the NTP.

5.5 The contractor shall conduct the following activities using the methodologies and frameworks based on any industry standards and best practices:

5.5.1 Perform one (1) discovery, vulnerability assessment, and penetration testing using gray box approach and black box approach, subject to necessary legal approvals, on the following DBM System Applications and IT Assets:

5.5.1.1 Twenty (20) DBM Public-facing applications
5.5.1.2 Ten (10) DBM internal applications
5.5.1.3 One hundred forty (140) virtual servers

5.5.2 Determine if current cyber security controls are sufficient against both unauthenticated and authenticated penetration testing.
5.5.3 Identify and categorize vulnerabilities based on severity, exploitability, and potential impact.
5.5.4 Identify vulnerabilities such as SQL injection, cross-site scripting, and insecure direct object references.
5.5.5 Controlled penetration testing to identify vulnerabilities in network devices, protocols, and configurations.
5.5.6 Debriefing session with DBM to discuss the findings, clarify any questions, and provide additional insights.
5.5.7 Conduct knowledge transfer sessions to help DBM understand the identified vulnerabilities and how to address them effectively.
5.5.8 Simulate real-world attacks to exploit vulnerabilities. These must consider the latest, most common, and most persistent types of threats to the particular type of application or system being tested.
5.5.9 Shall employ automated procedures to identify and exploit vulnerabilities.
5.5.10 Shall provide technical guidance to ICTSS security team to ensure the effectiveness of fixes.
5.5.11 Shall perform post-remediation verification testing after fixes have been applied to the initial VAPT findings.
5.5.12 Shall submit the following VAPT monthly reports within the first week of the succeeding month, subject to ICTSS Security Team approval.

5.5.12.1 **Executive Summary**: A high-level overview for non-technical stakeholders, summarizing the findings and the overall security posture.
5.5.12.2 **Scope and Methodology**: Clearly defines what was tested, the testing methods used, and any limitations or constraints during the assessment.
5.5.12.3 **Risk Assessment:** Categorizing vulnerabilities based on their severity, usually using a scale like low, medium, high, and critical. This report must have a risk matrix.
5.5.12.4 **Detailed Findings**: Specific vulnerabilities discovered, along with detailed information on each, such as the

affected system, description, evidence of exploitation, and recommendations for remediation.

5.5.12.5 **Exploitation Details**: For penetration testing, this would include the steps taken to exploit vulnerabilities to demonstrate the potential impact.

5.5.12.6 **Recommendations:** Actionable steps to address and mitigate the identified vulnerabilities, often prioritized based on severity.

5.5.12.7 **Appendix**: Additional information, such as technical details, logs, screenshots, or any supporting documentation.

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

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

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

Technical Training	**Schedule**	**No. of Participants**	**Duration**
Certified Penetration Testing Professional (CPENT)	Within two (2) months from the receipt of Notice to Proceed	Five (5) ICTSS participants	Forty (40) hours

The contractor shall issue individual training certificates and training materials for each of the participants.

5.8 The contractor shall provide as-built documentation of the VAPT 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 software/IT equipment employed in the project as well as procedures for configuration, integration, usage, backup, and restoration within thirty (30) calendar days from the receipt of NTP.

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	The CONTRACTOR shall deliver, integrate, and configure the VAPT Solution within thirty (30) calendar days from the receipt of the NTP.	1/10th of 1% of the total contract price shall be imposed per day of delay.
Availability	The VAPT solution must be guaranteed with 99.9% uptime/ availability per month, with a monthly downtime cap of 43.2 minutes.	1/10th of 1% of the monthly payment shall be imposed per minute of downtime.
Submission of VAPT Reports	Shall submit the following VAPT monthly reports within the first week of the succeeding month, subject to ICTSS Security Team approval (as detailed in item 5.5.12)	1/10th of 1% of the monthly payment shall be imposed per day of delay.
Technical Support	During the subscription period, the CONTRACTOR shall provide/render twenty-four hours a day, seven days a week technical support service. Technical support can be delivered in the form of a telephone call, electronic mail, and/or on-site support. Problems reported/concerns shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report.	1/10th of 1% of the monthly payment shall be imposed per day of delay.
Documentation	The contractor shall provide as-built documentation of the VAPT 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 software/IT equipment employed in the project as well as procedures for installation, configuration, integration, usage, backup, and restoration within thirty (30) calendar days from the receipt of NTP.	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 the technical staff assigned are qualified to provide the deliverables required to the satisfaction of the DBM.

7.3 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.

7.4 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.

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

7.6 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 there from.

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

7.8 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 formal notice, of any change or replacement of technical staff assigned.

8. CONFIDENTIALITY OF DATA

8.1 The contractor shall be required to sign a Non-Disclosure Agreement (NDA).

8.2 The DBM Enterprise Network System, its components, parts and all products, products samples and specifications, data, ideas, technology, and technical/nontechnical 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 Quarterly payment shall be made as reflected in Annex A.1 (Schedule of Payment), subject to the accomplishment/ submission of the specific deliverables and the following documentary requirements:

9.1.1 Sales Invoice / Billing Statement; and

9.1.2 Certificate of Acceptance issued by the Undersecretary for Information and Communications Technology (ICT) Group.

Annex A. 1
Schedule of Payment

Project Activity/ Detailed Activities	**Deliverables**	**Amount to be paid (% of Total Project Cost)**	**Date of Submission of Deliverables**[1]
1st tranche - Project Plan Documents and Kick-Off	• Setup, integration, and configuration of the VAPT • As-built documentation of the VAPT Solution • Pre-implementation meeting with DBM Representatives • Work plan of activities for the duration of the project and a Deployment and/or Solution Architecture • Submission of the NDA • Shall conduct the monthly deliverables as detailed in item 5.5 in Detailed Technical Specification. • Shall submit the VAPT Monthly Reports as detailed in item 5.5.12 • Shall provide Technical Trainings detailed in item 5.7 in Detailed Technical Specifications.	20% of the total project cost	January (Month 1) to March 2024 (Month 3)
2nd Tranche	• Shall conduct monthly deliverables as detailed in item 5.5 in Detailed Technical Specifications. • Shall submit the VAPT Monthly Reports as detailed in item 5.5.12 Detailed Technical Specifications.	30% of the total project cost	April (Month 4) to June (Month 6) 2024
3rd Tranche	• Shall conduct monthly deliverable as detailed in item 5.5 in Detailed Technical Specifications. • Shall submit the VAPT Monthly Reports as detailed in item 5.5.12 of the Detailed Technical Specifications.	30% of the total project cost	July (Month 7) to September (Month 9) 2024

[1] *See Section VI. Schedule of Requirements for the Specific Schedule of Deliverable*

Project Activity/ Detailed Activities	Deliverables	Amount to be paid (% of Total Project Cost)	Date of Submission of Deliverables[1]
4th Tranche	• Shall conduct monthly deliverable as detailed in item 5.5 in Detailed Technical Specifications. • Shall submit the VAPT Monthly Reports as detailed in item 5.5.12 Detailed Technical Specifications.	20% of the total project cost	October (M10) to December (M12) 2024

Statement of Single Largest Completed Contract which is Similar in Nature

[shall be submitted with the Bid]

(Revised)

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 **October 31, 2018 to October 30, 2023**.

c. The similar contract for this Project shall refer to the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, or subscription to, and implementation of, cyber security detection and response solutions. If the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, or subscription to, and implementation of, cyber security detection and response solutions form part of a bigger contract, only the cost component of the subscription to the deployment and implementation of cyber security testing which identifies and categorizes vulnerabilities within systems, applications, and networks, or subscription to, and implementation of, cyber security detection and response solutions 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

(Revised)

[shall be submitted with the Bid if bidder opts to provide this form of bid security]

REPUBLIC OF THE PHILIPPINES)
CITY OF__________________________) S.S.

BID SECURING DECLARATION

Project Identification No.: ***DBM-2024-02***

To: *[Insert name and address of the Procuring Entity]*

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid Securing Declaration.
2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f),of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.
3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:
   a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
   b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and
   c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this___________day of *[month] [year]* at *[place of execution]*.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

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

NOTARY PUBLIC

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

Omnibus Sworn Statement
(Revised)
[shall be submitted with the Bid]

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF____________________) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

   [If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

   [If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

   [If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

   [If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable;)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

   [If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, procurement agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a partnership or cooperative:] None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, procurement agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, procurement agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and

8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:

   a. Carefully examining all of the Bidding Documents;
   b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
   c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
   d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. **In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.**

IN WITNESS WHEREOF, I have hereunto set my hand this_______day of______, 20 ___at ________________ Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

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

NOTARY PUBLIC

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