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

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 1

This SBB No. 1 dated July 8, 2025 for **Project ID No. DBM-2025-38, "Subscription to the Vulnerability Assessment and Penetration Testing Solution for the DBM,"** 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.

PARTICULAR(S)/QUERY(IES)	AMENDMENT(S)/CLARIFICATION(S)
Section III. Bid Data Sheet **xxx** 4. List of names containing the bidder's pool of testers with at least five (5) of any of the following certifications for the whole team, together with the copies of their corresponding certificates: 4.1 Offensive Security Certified Professional (OSCP) 4.2 Offensive Security Experienced Penetration Tester (OSEP) 4.3 Offensive Security Certified Expert (OSCE) 4.4 Offensive Security Wireless Professional (OSWP) 4.5 Certified Information Systems Auditor (CISA) 4.6 GIAC Penetration Tester (GPEN) 4.7 GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) 4.8 GIAC Web Application Penetration Tester (GWAPT) 4.9 GIAC Mobile Device Security Analyst (GMOB) 4.10 GIAC Assessing and Auditing Wireless Networks (GAWN) 4.11 GIAC Experienced Penetration Tester (GX-PT) 4.12 Certified Cloud Security Professional (CCSP) 4.13 CompTIA PenTest+ ce 4.14 CompTIA Cybersecurity Analyst (CySA+ ce)	**Section III. Bid Data Sheet** **xxx** 4. List of names containing the bidder's pool of testers with at least five (5) of any of the following certifications for the whole team, together with the copies of their corresponding certificates: **4.1. CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)** **4.2. ISC2 CERTIFIED IN CYBERSECURITY** **4.3. CERTIFIED INFORMATION SECURITY MANAGER (CISM)** **4.4. CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL (CRISC)** 4.5. Offensive Security Certified Professional (OSCP) 4.6. Offensive Security Experienced Penetration Tester (OSEP) 4.7. Offensive Security Certified Expert (OSCE) 4.8. Offensive Security Wireless Professional (OSWP) 4.9. Certified Information Systems Auditor (CISA) 4.10. GIAC Penetration Tester (GPEN) 4.11. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) 4.12. GIAC Web Application Penetration Tester (GWAPT)

4.15 Certified AppSec Practitioner (CAP) 4.16 Certified AppSec Pentester (CAPen) 4.17 Certified Network Security Practitioner 4.18 Practical Network Penetration Tester (PNPT) 4.19 Certified Red Team Professional (CRTP) 4.20 eLearnSecurity Junior Penetration Tester (eJPT) 4.21 eLearnSecurity Certified Professional Penetration Tester (eCCPT) 4.22 EC-Council Certified Ethical Hacker (CEH) 4.23 EC-Council Certified Security Analyst (ECSA) 4.24 ISO 27001 ISMS Lead Auditor	4.13. GIAC Mobile Device Security Analyst (GMOB) 4.14. GIAC Assessing and Auditing Wireless Networks (GAWN) 4.15. GIAC Experienced Penetration Tester (GX-PT) 4.16. Certified Cloud Security Professional (CCSP) 4.17. CompTIA PenTest+ ce 4.18. CompTIA Cybersecurity Analyst (CySA+ ce) 4.19. Certified AppSec Practitioner (CAP) 4.20. Certified AppSec Pentester (CAPen) 4.21. Certified Network Security Practitioner 4.22. Practical Network Penetration Tester (PNPT) 4.23. Certified Red Team Professional (CRTP) 4.24. eLearnSecurity Junior Penetration Tester (eJPT) 4.25. eLearnSecurity Certified Professional Penetration Tester (eCCPT) 4.26. EC-Council Certified Ethical Hacker (CEH) 4.27. EC-Council Certified Security Analyst (ECSA) ~~4.27. ISO 27001 ISMS Lead Auditor~~
xxx	**xxx**
Section V. Special Conditions of Contract	**Section V. Special Conditions of Contract**

GCC Clause	
	xxx

GCC Clause	
	xxx
5	**IN ORDER TO ASSURE THAT MANUFACTURING DEFECTS SHALL BE CORRECTED BY THE SUPPLIER, A WARRANTY SECURITY SHALL BE REQUIRED FROM THE SUPPLIER FOR A MINIMUM PERIOD OF THREE (3) MONTHS, IN CASE OF EXPENDABLE**

		SUPPLIES, OR A MINIMUM PERIOD OF ONE (1) YEAR, IN CASE OF NON-EXPENDABLE SUPPLIES, AFTER ACCEPTANCE OF THE DBM OF THE DELIVERED GOODS. **THE OBLIGATION FOR THE WARRANTY SHALL BE COVERED BY EITHER A RETENTION MONEY IN AN AMOUNT EQUIVALENT TO ONE PERCENT (1%) OF EVERY PROGRESS PAYMENT, OR A SPECIAL BANK GUARANTEE EQUIVALENT TO ONE PERCENT (1%) OF THE TOTAL CONTRACT PRICE.** **THE SAID AMOUNT SHALL BE RELEASED AFTER THE LAPSE OF THE WARRANTY PERIOD, OR, IN THE CASE OF EXPENDABLE SUPPLIES, AFTER CONSUMPTION THEREOF: PROVIDED, HOWEVER, THAT THE SUPPLIES DELIVERED ARE FREE FROM PATENT AND LATENT DEFECTS AND ALL THE CONDITIONS IMPOSED UNDER THE CONTRACT HAVE BEEN FULLY MET.**
xxx		**xxx**

Annex "A"

DETAILED TECHNICAL SPECIFICATIONS

xxx

9.0 PERFORMANCE REVIEW AND ASSESSMENT

9.1 The service provider shall maintain a satisfactory level performance throughout the contract period based on the following set of performance criteria:

ITEM	**PERFORMANCE CRITERIA**	**MINIMUM WEIGHT**	**MAXIMUM WEIGHT**
I	Conformity to the technical requirements	25	30
II	Timeliness in the delivery of services	25	30
III	Behavior of personnel (courteous, professional and knowledgeable)	10	15
IV	Response to complaints	10	15
V	Compliance with set office policies for such services	10	10
TOTAL	**PERFORMANCE RATING PASSING RATE: 80 POINTS**	**80**	**100**

Annex "A"

DETAILED TECHNICAL SPECIFICATIONS (REVISED)

xxx

9. PERFORMANCE REVIEW AND ASSESSMENT

9.1 The service provider shall maintain a satisfactory level performance throughout the contract period based on the following set of performance criteria:

ITEM	**PERFOR-MANCE CRITERIA**	**~~MINIMUM~~ WEIGHT**	**~~MAXIMUM~~**
I	Conformity to the technical requirements	25	~~30~~
II	Timeliness in the delivery of services	25	~~30~~
III	Behavior of personnel (courteous, professional and knowledgeable)	~~10~~**20**	~~15~~
IV	Response to complaints	~~10~~**20**	~~15~~
V	Compliance with set office policies for such services	10	~~10~~
TO-TAL	PERFORMANCE RATING PASSING RATE: 80 POINTS		~~**80**~~ **100**

xxx	**xxx**
10. Warranties of the Service Provider	**10. Warranties of the Service Provider**
xxx	**xxx**
	10.10 IN ORDER TO ASSURE THAT MANUFACTURING DEFECTS SHALL BE CORRECTED BY THE SUPPLIER, A WARRANTY SECURITY SHALL BE REQUIRED FROM THE SUPPLIER FOR A MINIMUM PERIOD OF THREE (3) MONTHS, IN CASE OF EXPENDABLE SUPPLIES, OR A MINIMUM PERIOD OF ONE (1) YEAR, IN CASE OF NON-EXPENDABLE SUPPLIES, AFTER ACCEPTANCE OF THE DBM OF THE DELIVERED GOODS. **THE OBLIGATION FOR THE WARRANTY SHALL BE COVERED BY EITHER A RETENTION MONEY IN AN AMOUNT EQUIVALENT TO ONE PERCENT (1%) OF EVERY PROGRESS PAYMENT, OR A SPECIAL BANK GUARANTEE EQUIVALENT TO ONE PERCENT (1%) OF THE TOTAL CONTRACT PRICE.** **THE SAID AMOUNT SHALL BE RELEASED AFTER THE LAPSE OF THE WARRANTY PERIOD, OR, IN THE CASE OF EXPENDABLE SUPPLIES, AFTER CONSUMPTION THEREOF: PROVIDED, HOWEVER, THAT THE SUPPLIES DELIVERED ARE FREE FROM PATENT AND LATENT DEFECTS AND ALL THE CONDITIONS IMPOSED UNDER THE CONTRACT HAVE BEEN FULLY MET.**

xxx **Attachment 2. Technical Requirements for the VAPT Solution** **xxx** 6. Support multiple relay attempts by reusing connection errors in SMB and HTTP protocols and forwarding them to different target hosts. **xxx** 21.1. Can provide scorecard for health of external facing assets **xxx** 22. Must have the following key benefits for the use of DBM **xxx** 25. Shall use methodologies and frameworks based on industry standards and best practices such as the following:	**xxx** **Attachment 2. Technical Requirements for the VAPT Solution** **(REVISED)** **xxx** 6. Support for multiple relay attempts by **CAPTURING** and reusing connection errors in SMB and HTTP protocols, **WHICH CAN THEN BE AUTOMATICALLY OR MANUALLY FORWARDED** to target different hosts. **xxx** 21**.**1 Can provide scorecard for health of ~~external~~ **INTERNET** facing assets **xxx** 22. Must have **AT LEAST** the following key benefits or **THEIR EQUIVALENT** for the use of DBM. **xxx** 25. Shall use methodologies and frameworks based on industry standards and best practices **OR SUBSETS OF THE FOLLOWING:**
Queries: **Statement of Largest Completed Contract** 1. Instead of specifically requiring VAPT (Vulnerability Assessment and Penetration Testing), may we request if this can be revised to any cybersecurity or ICT services?	**Clarifications:** 1. No. The original requirement is maintained to specifically require VAPT services, as this is necessary to ensure the bidder's relevant experience and capacity to meet the project's technical requirements.

Qualifications of the Service Provider 2. We would also like to request that the required number of certifications for the pool of testers be reduced from at least five (5) to three (3).	2. The original technical requirement under Section 4 of the DTS is maintained. The requirement of at least five (5) certifications for the pool of testers remains necessary to ensure adequate expertise and capability in delivering the VAPT services.
Scope of Work for VAPT Solution 3. We would like to request that the requirement for a centralized dashboard for VAPT reporting be revised, made optional, or alternatively allow for the delivery of VAPT reports directly to end-users via email.	3. No. The centralized dashboard under Section 5.4 of the DTS for VAPT reporting is retained as a mandatory requirement. This feature is essential to ensure real-time visibility, efficient monitoring, and secure access to assessment results by authorized stakeholders.
Warranties of the Service Provider 4. Is it possible for the requirements to be virtual, or must they be on-site?	4. Yes, A hybrid arrangement may be considered; however, the actual fulfillment of the requirements must be conducted on-site to ensure proper validation, effective coordination, and adherence to security protocols—particularly those applicable to on-premises systems.
Attachment 1. Scope of Work for VAPT Solution **5.1.3. One hundred sixty (160) virtual servers** 5. Please clarify whether the VAPT activities referenced in this section are intended to cover only servers and applications, or whether endpoints are also included. A breakdown by asset type would be appreciated.	5. The VAPT activities under Section 5.1.3 shall cover websites, DBM internal applications, and servers. Each application is counted per website or application, regardless of the number of underlying hosts, while servers are

	counted as one server per host or IP address. A detailed breakdown of the applications, servers, and related assets will be provided to the winning bidder during the pre-implementation meeting.
5.2 The list of external assets may be updated once a year to account for any future changes in the systems and infrastructure 6. Will the penetration testing scope remain fixed throughout the contract duration, or will there be changes or additions each year? If so, may we know the process and timing for these updates?	6. The total count of assets for VAPT will remain fixed throughout the contract duration; however, the specific assets may change over time due to system updates or replacements.
6.1. Perform one (1) discovery per year, monthly vulnerability assessments, and automated penetration testing using gray and white box approach, subject to necessary legal approvals for Two Hundred Fifty-Six (256) IP addresses/hosts. 7. The section appears to imply a white-box or gray-box testing methodology. Would the DBM consider a black-box testing approach instead? Kindly confirm the intended methodology.	7. No, the DBM will not consider a black-box testing approach under Section 6.1. Please refer to the specified testing methodology outlined in the requirements.
6.8 Configure the VAPT solution to be able to execute manual testing activities to be able to verify remediation activities in an ad-hoc manner. 8. Please confirm whether the subscription to the VAPT solution includes both the tool/software and the professional services (e.g., implementation, configuration, testing, reporting, and support), or if these are considered separate deliverables.	8. The subscription includes both the VAPT solution and the associated professional services.

16. The solution can discover relative domains, detect known and unknown assets, discover sub-domains, IPV4/6, discover cloud assets of the DBM. 9. May we clarify if there are scoped cloud assets, applications, and instances for this project? The request: Removal of cloud assets or rephrase the technical clause to: "16. The solution can detect unknown and unknown assets, IPV4/6, weak and vulnerable user credential of the DBM."	9. Cloud assets are within the scope of the service provider. The corresponding domains and sub-domains will be provided during the pre-implementation meeting.
	<u>Note: Attached for guidance of the bidders is the Detailed Technical Specifications (Revised) which shall for part of the Bidding Documents.</u>

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 July 15, 2025, right after the opening of bids.

- For guidance and information of all concerned.

[redacted]

RAMON VICENTE B. ASUNCION
Assistant Secretary
Vice Chairperson, DBM-BAC [redacted]

Annex "A"

DETAILED TECHNICAL SPECIFICATIONS
(REVISED)

1. PROJECT TITLE

Subscription to the Vulnerability Assessment and Penetration Testing Solution for the DBM.

2. OBJECTIVE

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

2.2. The comprehensive evaluation through the subscription to VAPT Solution 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 VAPT Solution shall cover independent assessments, including non-destructive tests, to evaluate the security posture internal and external DBM systems from a hacker's perspective.

2.3. The DBM requires a **single VAPT Solution or Tool** that allows InfoSec end-users to proactively assess the security posture of IT systems. The solution should provide comprehensive vulnerability detection capabilities while being accessible to non-technical users.

2.4. The provision of the VAPT solution is vital to support the prioritization of security requirements that will help the DBM achieve the following objectives:

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

2.4.2 Identify the risk level to which DBM is exposed, so that appropriate countermeasures can be developed and applied, provide actionable insights and remediation guidance to mitigate identified risks.

2.4.3 Improve overall security awareness among stakeholders, ensuring that risks are understood, and necessary measures are taken to protect sensitive data, avoid financial losses, and prevent operational disruptions.

2.4.4 Strengthen the DBM's cybersecurity posture by proactively managing risks and enhancing its defenses.

3. DURATION OF CONTRACT

The Subscription Period for the project shall be three (3) years from the issuance of the **Proof of Subscription**. The Proof of Subscription shall only be issued by the Service Provider within

seven (7) calendar days after the complete set up, installation, and configuration of all licenses for all environments.

The setup, installation, and configuration must be completed within thirty (30) calendar days from the receipt of the Notice to Proceed (NTP).

4. QUALIFICATIONS OF THE SERVICE PROVIDER

4.1 The service provider must have at least five (5) years of experience in IT Security Industry. Copy of BIR Certificate of Registration or any certification showing that the service provider has at least five (5) years of experience in IT Security Industry will be requested to be submitted during post-qualification.

4.2 The service provider must have in their employment and located in the Philippines a pool of testers that have at least five (5) of any of the following certifications. Copy of professional and human resources certifications will be requested to be submitted during post-qualification.

4.2.1. Certified Information Systems Security Professional (CISSP)
4.2.2. ISC2 Certified in Cybersecurity
4.2.3. Certified Information Security Manager (CISM)
4.2.4. Certified in Risk and Information Systems Control (CRISC)
4.2.5. Offensive Security Certified Professional (OSCP)
4.2.6. Offensive Security Experienced Penetration Tester (OSEP)
4.2.7. Offensive Security Certified Expert (OSCE)
4.2.8. Offensive Security Wireless Professional (OSWP)
4.2.9. Certified Information Systems Auditor (CISA)
4.2.10. GIAC Penetration Tester (GPEN)
4.2.11. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
4.2.12. GIAC Web Application Penetration Tester (GWAPT)
4.2.13. GIAC Mobile Device Security Analyst (GMOB)
4.2.14. GIAC Assessing and Auditing Wireless Networks (GAWN)
4.2.15. GIAC Experienced Penetration Tester (GX-PT)
4.2.16. Certified Cloud Security Professional (CCSP)
4.2.17. CompTIA PenTest+ ce
4.2.18. CompTIA Cybersecurity Analyst (CySA+ ce)
4.2.19. Certified AppSec Practitioner (CAP)
4.2.20. Certified AppSec Pentester (CAPen)
4.2.21. Certified Network Security Practitioner
4.2.22. Practical Network Penetration Tester (PNPT)
4.2.23. Certified Red Team Professional (CRTP)
4.2.24. eLearnSecurity Junior Penetration Tester (eJPT)
4.2.25. eLearnSecurity Certified Professional Penetration Tester (eCCPT)

4.2.26. EC-Council Certified Ethical Hacker (CEH)
4.2.27. EC-Council Certified Security Analyst (ECSA)

4.3 The service provider shall provide the solution described in the Scope of Work in a in accordance with industry standards and best practices. In line with this:

4.3.1 The service provider must have a brochure detailing their proposed VAPT Solution which will be requested to be submitted during post qualification.

4.3.2 The service provider shall undergo a Proof of Concept (PoC) of the proposed submitted solution that includes the detailed proposed methodology and approach, in accordance with industry standards and best practices, and the testing of its compliance with the technical requirements and competencies of the contractor to deliver the services defined on the scope of work which shall be conducted as a post-qualification requirement. An executed Non-Disclosure Agreement (NDA) must be submitted by the service provider at least two (2) working days prior to the commencement of the PoC. All PoC preparations, including the setup and configuration of the PoC environment, must be configured at least two (2) working days before the scheduled start of the live PoC demonstration.

Note: Proof of Concept (PoC) is requested to be presented during the post-qualification.

5. SCOPE OF WORK FOR VAPT SOLUTION

This section provides details of the scope of work for VAPT Solution and deliverables from the service provider. The scope of the VAPT Solution will cover the following components:

5.1 Vulnerability Assessment: Comprehensive scanning and analysis of the network, systems, and applications to identify vulnerabilities.

5.2 Penetration Testing: Simulated attacks on the IT infrastructure to exploit identified vulnerabilities and assess the potential impact.

5.3 Reporting: Detailed reporting of findings, including:
- 5.3.1 Executive summary of vulnerabilities and risks
- 5.3.2 Technical details of vulnerabilities discovered
- 5.3.3 Recommended remediation measures
- 5.3.4 Risk assessment for each identified vulnerability

5.4 A single centralized dashboard of all findings, vulnerabilities, risk, and other relevant information that would provide the DBM an overall view of its cyber security health.

5.5 The complete service coverage and details are provided in **Attachment 1 Scope of Work for VAPT Solution**, attached herewith and made an integral part of this document.

5.6 The service provider shall maintain a satisfactory level of performance throughout the duration of the contract, in accordance with the performance criteria outlined in **Section 9: Performance Review and Assessment** of this Detailed Technical Specification (DTS).

6. TECHNICAL REQUIREMENTS FOR THE VAPT SOLUTION

6.1. The complete requirement of the VAPT solution tool, along with detailed information, is provided in Attachment 2: Technical Requirement of the VAPT solution tool, which is attached herewith and forms an integral part of this document.

7. SERVICE LEVEL AGREEMENT

The DBM shall maintain a Service Level Agreement with the service provider, 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 service provider, or collected from any securities or warranties posted by the service provider.

Component	Description	Liquidated Damages
Delivery, Integration, and Configuration	The SERVICE PROVIDER shall deliver, integrate, and configure the VAPT Solution within thirty (30) calendar days upon receipt of the Notice to Proceed (NTP).	1/10th of 1% of the total contract price shall be imposed per day of delay.
Availability	The VAPT solution must be guaranteed 99.9% uptime/ availability per month, with a monthly downtime cap of 43.2 minutes.	1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per minute of downtime.
Submission of VAPT Reports	Shall submit the following VAPT reports, as defined in item of Section V. Scope of Work for VAPT Solution, within the first week of the succeeding month, subject to ICTSS Information Security Team approval (as detailed in item 5.3 in Section V. Scope of Work for VAPT Solution of Section VII. Technical Specifications)	1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per day of delay.

Component	Description	Liquidated Damages
Technical Support	During the subscription period, the SERVICE PROVIDER 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 equivalent of the quarterly payment shall be imposed per day of delay.

8. TERMS OF PAYMENT

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

Year	Milestone	Required Outputs and Supporting Documents	Payment
Year 1 (Quarter 1-Quarter 3)	Configuration and Technical Maintenance	• 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; • Shall conduct the monthly deliverables as detailed in item 5. Scope of Work for VAPT Solution and item 6. Technical Requirements for VAPT Solution;	• Payment for Year 1 shall be made on a quarterly basis and shall be payable in three (3) tranches: • 1/3- within the Month 1-Month 3 of Project implementation upon submission of the 3-months completion report. • 1/3- within the Month 4-Month 6 of project implementation upon submission of the quarterly completion report.

		• Shall submit the VAPT Monthly Reports as detailed in item 5.3. of 5. Scope of Work for VAPT Solution; • Shall provide Technical Trainings detailed in item 11 in Attachment 1: Scope of Work for VAPT Solution; • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the Undersecretary for Information and Communications Technology (ICT) Group; • Non-Disclosure Agreement (NDA); • Valid and updated Tax Clearance Certificate; • Submission of Annual Status and Progress Report of the Year 1 subscription for the last tranche payment of the year; and • Performance Review and Assessment Document from End-User Representatives with at least 80 points passing rate for the last tranche payment of the year;	• 1/3- within the Month 7-Month 9 of project implementation upon submission of the 3-months completion report.
Year 2 (Quarter 4-Quarter 7)	Configuration and Technical Maintenance	• As-built documentation of the VAPT Solution; • Pre-implementation meeting with DBM Representatives;	• Payment for Year 2 shall be made on a quarterly basis and shall be payable in four (4) tranches:

		• Work plan of activities for the duration of the project and a Deployment and/or Solution Architecture: • Shall conduct the monthly deliverables as detailed in item 5. Scope of Work for VAPT Solution and item 6. Technical Requirements for VAPT Solution; • Shall submit the VAPT Monthly Reports as detailed in item 5.3. of 5. Scope of Work for VAPT Solution; • Shall provide Technical Trainings detailed in item 11 in Attachment 1: Scope of Work for VAPT Solution; • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the Undersecretary for Information and Communications Technology (ICT) Group; • Non-Disclosure Agreement (NDA); and • Valid and updated Tax Clearance Certificate; • Submission of Annual Status and Progress Report of the Year 2 subscription for the	• 1/4 - within the Month 10-Month 12 of Project implementation upon submission of the 3-months completion report. • • 1/4 - within the Month 13-Month 15 of Project implementation upon submission of the 3-months completion report. • 1/4 - within the Month 16-Month 18 of project implementation upon submission of the quarterly completion report. • 1/4 - within the Month 19-Month 21 of project implementation upon submission of the 3-months completion report.

		last tranche payment of the year; and • Performance Review and Assessment Document from End-User Representatives with at least 80 points passing rate for the last tranche payment of the year;	
Year 3 (Quarter 8-Quarter 11)	Configuration and Technical Maintenance	• 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; • Shall conduct the monthly deliverables as detailed in item 5. Scope of Work for VAPT Solution and item 6. Technical Requirements for VAPT Solution; • Shall submit the VAPT Monthly Reports as detailed in item 5.3. of 5. Scope of Work for VAPT Solution; • Shall provide Technical Trainings detailed in item 11 in Attachment 1: Scope of Work for VAPT Solution; • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the Undersecretary for Information and	• Payment for Year 3 shall be made on a quarterly basis and shall be payable in four (4) tranches: • 1/4 - within the Month 22-Month 24 of project implementation, upon submission of 3-months completion report • 1/4 - within the Month 25-Month 27 of Project implementation upon submission of the 3-months completion report. • 1/4 - within the Month 28-Month 30 of project implementation upon submission of the quarterly completion report. • 1/4 - within the Month 31-Month 33 of project implementation upon submission of the 3-months completion report.

		Communications Technology (ICT) Group; • Non-Disclosure Agreement (NDA); and • Valid and updated Tax Clearance Certificate; • Submission of Annual Status and Progress Report of the Year 3 subscription for the last tranche payment of the year; and • Performance Review and Assessment Document from End-User Representatives with at least 80 points passing rate for the last tranche payment of the year;	
Year 4 (Quarter 12-Quarter 13)	Configuration and Technical Maintenance	• 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; • Shall conduct the monthly deliverables as detailed in item 5. Scope of Work for VAPT Solution and item 6. Technical Requirements for VAPT Solution; • Shall submit the VAPT Monthly Reports as detailed in item 5.3. of 5. Scope of Work for VAPT Solution;	• Payment for Year 4 shall be made on a quarterly basis and shall be payable in two (2) tranches: • 1/2 - within the Month 34-Month 36 of project implementation, upon submission of 3-months completion report • 1/2 - within the Month 37-Month 39 of project implementation, upon submission of 3-months completion report

		• Shall provide Technical Trainings detailed in item 11 in Attachment 1: Scope of Work for VAPT Solution; • Sales Invoice/Billing Statement; • Certificate of Acceptance issued by the Undersecretary for Information and Communications Technology (ICT) Group; • Non-Disclosure Agreement (NDA); and • Valid and updated Tax Clearance Certificate; • Submission of Annual Status and Progress Report of the Year 4 subscription for the last tranche payment of the year; and • Performance Review and Assessment Document from End-User Representatives with at least 80 points passing rate for the last tranche payment of the year;	

Pursuant to the Bureau of Internal Revenue Regulation No. 017-2024 dated September 17, 2024, the Service Provider shall present their valid and updated Tax Clearance Certificate to the End-user Unit, prior to the final payment of the contract. Failure to present a valid and updated Tax Clearance shall entitle the DBM to suspend the final payment due to the Service Provider.

9. PERFORMANCE REVIEW AND ASSESSMENT

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

ITEM	PERFORMANCE CRITERIA	WEIGHT
I	Conformity to the technical requirements	25
II	Timeliness in the delivery of services	25
III	Behavior of personnel (courteous, professional and knowledgeable)	20
IV	Response to complaints	20
V	Compliance with set office policies for such services	10
TOTAL	**PERFORMANCE RATING** **PASSING RATE: 80 POINTS**	**100**

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

9.3 The OCIO shall conduct an annual assessment or evaluation one month before the end of the yearly subscription, based on the above-cited criteria, to ensure compliance of the Service Provider with the detailed technical specifications, as well as with the other terms and conditions imposed by the DBM during the contract period.

9.4 Based on its assessment, the DBM may pre-terminate the contract for failure of the Service Provider to perform its obligations thereon following the procedures prescribed under the Guidelines on Termination of Contracts provided in ANNEX "I": Guidelines on Termination of Contracts of the 2016 Revised IRR of RA No. 9184.

10. WARRANTIES OF THE SERVICE PROVIDER

10.1 The service provider warrants that it shall strictly conform to the terms and conditions of this Detailed Technical Specifications.

10.2 The service provider warrants that the technical staff assigned are qualified to provide the deliverables required to the satisfaction of the DBM.

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

10.4 The service provider'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.

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

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

10.7 The service provider shall neither assign, transfer, pledge, nor subcontract any part of or interest in the contract, but joint ventures are allowed.

10.8 The service provider shall identify the certified technical staff who will be given authority to access and operate the specified equipment. The DBM, through the ICTSS, shall be informed within five (5) calendar days, through formal notice, of any change or replacement of technical staff assigned.

10.9 The service provider shall maintain the confidentiality and integrity of the DBM's data and information systems and comply with all applicable data protection and privacy laws.

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

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

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

11. CONFIDENTIALITY OF DATA

11.1 The service provider shall be required to sign a Non-Disclosure Agreement (NDA).

11.2 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.

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

ATTACHMENT 1
SCOPE OF WORK FOR VAPT SOLUTION

The following provides the details of the Scope of Work for VAPT Solution that the service provider shall provide and comply with:

1. The service provider shall conduct a pre-implementation meeting with Information and Communications Technology Systems Service (ICTSS) – Information Security Division (ISD) representatives within seven (7) calendar days from the receipt of the Notice to Proceed (NTP) and within seven (7) calendar days from the start of each subsequent subscription period, so that all the necessary preparations, ideal set-up, service provider's familiarization, and other implementation matters are discussed and finalized.
2. The service provider shall provide a work plan of activities for the duration of the project and a Deployment and/or Solution Architecture within fourteen (14) calendar days from the receipt of NTP and within fourteen (14) calendar days from the start of each subsequent subscription period . Said work plan shall be validated and subject to the approval of the Undersecretary for Information and Communications Technology (ICT) Group.
3. The service provider shall provide the solution described in the Scope of Work in a timely, professional, and efficient manner, and in accordance with industry standards and best practices.
4. The service provider shall assign a dedicated team of cybersecurity professionals to the project, with appropriate skills, experience, and certifications.
5. The service provider shall conduct the following scope of activities using the methodologies and frameworks defined below:

    5.1. Perform credentialed penetration testing through manual and automated Gray box testing approach every six (6) months, subject to necessary legal approvals, on the following:

        5.1.1. Twenty (20) DBM Public-facing applications

        5.1.2. Ten (10) DBM Internal applications

        5.1.3. One hundred sixty (160) virtual servers

    5.2. The list of external assets may be updated once a year to account for any future changes in the systems and infrastructure.

    5.3. Perform the penetration testing utilizing the Open Source Security Testing Methodology Manual (OSSTMM) Framework and if applicable the Open Web Application Security Project (OWASP) Continuous Testing Framework.

    5.4. Conduct automated Blackbox Vulnerability Assessment and Penetration Testing (VAPT) on a quarterly basis and submit the corresponding report within fifteen (15) calendar days following the end of each quarter. The Blackbox VAPT report shall include, at a minimum, the following information:

        5.4.1. An Executive Summary that contains at least information about the approach used, scope,

and overview of assessment and recommendation.

5.4.2. Penetration Test Assessment Summary that contains a summary of findings.

5.4.3. Compromised Walkthrough that contains detailed walkthrough of activities done on the compromised asset.

5.4.4. Remediation Summary that contains short-term, medium-term, and long-term remediation activities to mitigate the findings.

5.4.5. Technical Findings Details that contain at least the Common Vulnerability Scoring System (CVSS), description, security impact, affected asset, remediation, and if available external references.

5.4.6. Appendices contain additional relevant information, such as findings severities, exploited hosts/assets, compromised accounts, or any other supporting documentation.

6. The service provider shall configure the following activities on the automated VAPT Solution:

6.1. Perform one (1) discovery per year, monthly vulnerability assessments, and automated penetration testing using gray and white box approach, subject to necessary legal approvals for Two Hundred Fifty-Six (256) IP addresses/hosts.

6.2. Configure the VAPT solutions to be able to run automated monthly schedule scans and generate reports.

6.3. Configure automated monthly and ad-hoc reports to contain at least the following information:

6.3.1. Executive Summary: A high-level overview for nontechnical stakeholders, summarizing the findings and the overall security posture.

6.3.2. Scope and Methodology: Clearly defines what was tested, the testing methods used, and any limitations or constraints during the assessment.

6.3.3. 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.

6.3.4. Detailed Findings: Specific vulnerabilities discovered, along with detailed information on each, such as the affected system, description, evidence of exploitation, and recommendations for remediation.

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

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

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

6.4. Identify and categorize vulnerabilities based on severity, exploitability, and potential impact.

6.5. Identify vulnerabilities such as SQL injection, cross-site scripting, and insecure direct object references.

6.6. Automated and controlled penetration testing to identify vulnerabilities and exploit these

vulnerabilities.

6.7. Configure simulated real-world attacks to exploit vulnerabilities. These must consider the latest, most common, and most persistent types of threats to the application or system being tested.

6.8. Configure the VAPT solution to be able to execute manual testing activities to be able to verify remediation activities in an ad-hoc manner.

7. Debriefing session with DBM to discuss the findings, clarify any questions, and provide additional insights.
8. Conduct knowledge transfer sessions to help the DBM understand the identified vulnerabilities and how to address them effectively.
9. Shall provide technical guidance to ICTSS security team to ensure the effectiveness of fixes.
10. In the event the subscription ends, the service provider must remove any installed agents or software in the DBM systems and infrastructure related to the VAPT Solution.
11. The service provider shall provide Technical Training to be conducted by an Authorized IT Security Training Center. The Technical Training should be a classroom type based on the following schedule:

Technical Training	**Schedule**	**No. of Participants**	**Duration**
CompTIA Network+	Within two (2) months from the receipt of NTP	Four (4) ICTSS-ISD Participants	Forty (40) hours
	Within three (3) months from the receipt of NTP	Three (3) ICTSS-ISD Participants	Forty (40) hours
CompTIA Linux+	Within four (4) months from the receipt of NTP	Three (3) ICTSS-ISD Participants	Forty (40) hours
	Within five (5) months from the receipt of NTP	Three (3) ICTSS-ISD Participants	Forty (40) hours

12. The service provider shall issue individual training certificates and training materials for each of the participants.
13. The service provider 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.

ATTACHMENT 2
TECHNICAL REQUIREMENTS FOR THE VAPT SOLUTION
(Revised)

The contractor shall provide an automated VAPT Solution with the following features and functionality, but not limited to:

1. Solution can perform a test with no credentials or detailed knowledge of the tested network.
2. Ability to run a targeted test in DBM network for the following Scenarios:
    2.1. Evaluate password strength, credential reuse, policy violations, and general AD hygiene across multiple hosts and domains.
    2.2. Analyze the most critical web security risks to validate against OWASP Top 10 Vulnerabilities.
3. Can quickly highlight the most critical findings in the GUI/report based on the attack kill chain.
4. Ability to get a detailed explanation of the root cause and how to fix the vulnerability.
5. Should include a wide variety of attacks. All attack scenarios will be automatically mapped to the MITRE ATT&CK Framework, with each scenario represented.
6. Support for multiple relay attempts by capturing and reusing connection errors in SMB and HTTP protocols, which can then be automatically or manually forwarded to target different hosts.
7. Built-in capabilities that can exploit VPNs, firewalls, server Operating Systems, and Endpoint Operating Systems.
8. Can validate open services, employee credential usage, and CVE exploitability
9. Can run vulnerability assessment scan on one time and on a continuous basis.
10. Can describe vulnerabilities per assets and mitigation.
11. Can classify and prioritize vulnerabilities based on AI Exploit Prediction Scoring System (EPSS).
12. 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.
13. 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.
14. Can handle testing of future IFMIS applications/systems that may be developed and/or identified within the subscription period.
15. Shall be able to have a security/vulnerability assessment of DBM domains, networks, servers, etc

16. The solution can discover relative domains, detect known and unknown assets, discover sub-domains, IPV4/6, discover cloud assets of the DBM.
17. Shall be able to detect critical, high, medium, and low vulnerabilities. Risk score and exploitable vulnerabilities.
18. Provide remediation playbooks for vulnerabilities
19. Must provide a centralized dashboard for reporting, as follows:
    19.1. Must generate report of vulnerabilities
    19.2. Centralized dashboard
    19.3. Various format for report downloads.
    19.4. Various format for report downloads.
20. Artificial Intelligence
    20.1. Identify critical paths for threat actors
    20.2. Provide executive exposures review
    20.3. Provide threat actor prediction and put in Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrix.
21. Continuous Monitoring
    21.1. Can provide scorecard for health of internet facing assets
    21.2. Can provide insights of attacks and actions to improve security posture
22. Must have at least the following key benefits or their equivalent for the use of DBM:
    22.1. Continuous Assets Discovery and Monitoring (CIS 1 & 2).
    22.2. GDPR/CCPA Compliance (Leak Monitoring and Security by design).
    22.3. Exploitability validation (BOD 22-01).
    22.4. Continuous visibility during incident recovery (NIST - Recover).
    22.5. Reduce the risk of unknown assets (blind spots/shadow IT).
    22.6. Locate
    22.7. Better prioritize patch and remediation efforts.
    22.8. Identify misconfigurations & process failures.
23. The VAPT Solution must have the following capabilities:
    23.1. Continuous discovery
    23.2. Alerts and Notifications
    23.3. Exploitability Validation
    23.4. Exploit Trends Identification
    23.5. Risk Scoring
    23.6. Multi-Factor Authentication.
    23.7. Technology Identification.
    23.8. Test Scheduling

24. The VAPT Solution must have a dashboard for the following:
    24.1. Infrastructure Assets
        - Subdomains - Total, Monitored and Exposed
        - Hosts - Exposed ports per host
    24.2. Cloud Assets
        - Integrated and identified accounts – Total and Configured for testing
        - Cloud Storage – Identified – Private and Publicly exposed
    24.3. Websites
        - Identified – Monitored and Vulnerable
        - Behind Web Application or not
25. Shall use methodologies and frameworks based on industry standards and best practices or subsets of the following:
    25.1. Open Worldwide Application Security Project (OWASP)
    25.2. SysAdmin, Audit, Network, and Security (SANS)
    25.3. National Institute of Standards and Technology (NIST)
    25.4. Center of Internet Security (CIS)
    25.5. Cloud Security Alliance (CSA)
    25.6. Exploit Prediction Scoring System (EPSS)
    25.7. Adversarial Tactics, Techniques, and Common Knowledge or MITRE ATT&CK
26. The VAPT solution must be guaranteed with 99.9% uptime/availability per month, with a monthly downtime cap of 43.2 minutes.