DEVELOPMENT BANK OF THE PHILIPPINES
Head Office: Sen. Gil J. Puyat Avenue corner
Makati Avenue, Makati City, Philippines

SUPPLEMENTAL BID BULLETIN NO. 1

28 August 2025

Attention: **All prospective bidders for the project**

BID REFERENCE NO. G-2025-20: ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES (ABC: PhP 165,000,000.00 for three years or PhP55,000,000.00 per year inclusive of all applicable taxes)

Please be informed of the following:

1. The deadline of submission and opening of bids is hereby revised as follows:

ACTIVITY	DATE AND TIME		VENUE
	FROM	TO	
Submission of Eligibility, Technical, and Financial Proposals*	3 September 2025 (Wednesday) ON OR BEFORE 9:00 AM	**5 September 2025 (Friday) ON OR BEFORE 9:00 AM**	6/F BAC Secretariat, DBP Head Office, Makati City
Opening of Eligibility, Technical, and Financial Proposals	3 September 2025 (Wednesday) 9:30 AM	**5 September 2025 (Friday) 9:30 AM**	12/F Suite 5, DBP Head Office, Makati City or via Zoom Meeting

Late submissions shall not be accepted

2. **Please refer to Please refer to Section III. Bid Data Sheet (BDS) of the Philippine Bidding Documents for the detailed procedure and options for the payment of bidding documents and the submission of bids. As indicated in the Invitation to Bid, bidders must settle the required payment for the bidding documents before the deadline of the submission and receipt of bids.**

   Additionally, bidders are encouraged to submit their bid proposals (either manual or online submission) at least one day prior to the deadline to avoid late submissions. Bidders may attend the bid opening through Zoom Meeting App.

   For online submission of bids, bidders are reminded to email the BAC Secretariat of their intent to submit electronically at least one day prior to the deadline of bid submission. This is to give ample time for the Secretariat to prepare and generate the link wherein bidders will upload their proposals.

3. **Responses to Queries or Request for Clarifications is provided under Annex A attached in this Supplemental Bid Bulletin No. 1 dated 28 August 2025.**

4. **Revisions made on the Technical Specifications:**
(Please refer to REVISED FORM 9 for the Revised Technical Specifications attached in this Supplemental Bid Bulletin No. 1 dated 28 August 2025)

FROM	TO
NONE	**IX. BIDDING DOCUMENTS** ...*xxx* 5. Certification from the solutions provider indicating that the solutions being offered can be integrated with on premise McAfee SIEM. 6. Requirements for the following personnel: • Local/global Support Engineers (at least two) o Certificate of employment indicating full-time employee. o Certification (at least one per Engineer) indicating Cybersecurity Support Engineer. • Onsite Support Engineer (at least one) o Certificate of employment indicating that the personnel is a full-time employee. o Curriculum Vitae were indicated that the personnel have 2 years' work experience as an IT Security Support Engineer. o Certification on MDR Solution being offered. o Training Certificate (at least 2) on IT Security Fundamentals. • Data Privacy Officer (at least two): o Certificate of employment indicating full-time employee. o DPO Certification by an accredited provider. • Technical Account Manager (at least one): o Certificate of employment from the solutions provider/principal indicating full-time employee. o Curriculum Vitae were indicated experience (at least 2 years) as Technical Account Manager.

FROM	TO
	• Project Manager: o Certificate of employment for the assigned personnel indicating the date of hire. o Resume or Curriculum Vitae indicating the personnel assigned have at least three (3) years' experience in Project Management and have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippines banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date). o Certification for Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

5. **Revisions made on the Bidding Forms:**

(Please refer to REVISED FORM 9 for the Revised Technical Specifications attached in this Supplemental Bid Bulletin No. 1 dated 28 August 2025)

FROM	TO
FORM 9 Certificate of Conformance to the Terms of Reference	**REVISED FORM 9** **Certificate of Conformance to the Revised Terms of Reference**
FORM 9-A Terms of Reference and specifications	**REVISED FORM 9-A** **Revised Terms of Reference and specifications**

6. **Revision on the Checklist of Requirements**
(Please see the Revised Checklist of Requirements as attached in this Supplemental Bid Bulletin No. 1 dated 28 August 2025)

FROM	TO
TAB 10 Accomplished Certificate of Conformance to the Terms of Reference **per *FORM 9*, duly signed by the bidder's authorized representative.** The complete Terms of Reference and specifications are also attached as *FORM 9-A* for reference.	**TAB 10** Accomplished ***Certificate of Conformance to the Revised Terms of Reference*** **per *REVISED FORM 9 (attached in the Supplemental Bid Bulletin No. 1 dated 28 August 2025),* duly signed by the bidder's authorized representative.** The complete ***REVISED Terms of Reference and specifications*** are also attached as ***REVISED FORM 9-A (attached in the Supplemental Bid Bulletin No. 1 dated 28 August 2025),*** for reference.

FROM	TO
NONE	**TAB 14** Certification from the solutions provider indicating that the solutions being offered can be integrated with on premise McAfee SIEM.
	TAB 15 Documents for each of the local/global Support Engineers (at least two personnel): 1. Certificate of employment indicating that the personnel is a full-time employee. 2. Certification (at least one per Engineer) indicating Cybersecurity Support Engineer.
	TAB 16 Documents for the Onsite Support Engineer (at least one personnel): 1. Certificate of employment indicating that the personnel is a full-time employee. 2. Curriculum Vitae indicating that the personnel have 2 years of work experience as an IT Security Support Engineer. 3. Certification on MDR Solution being offered. 4. At least two (2) training Certificates on IT Security Fundamentals.
	TAB 17 Documents for each of the Data Privacy Officers (at least two personnel): 1. Certificate of employment indicating that the personnel is a full-time employee 2. DPO Certification by an accredited provider.
	TAB 18 Documents for the Technical Account Manager (at least one personnel): 1. Certificate of employment from the solutions provider/principal indicating full-time employee. 2. Curriculum Vitae indicating at least 2 years of experience as Technical Account Manager.

FROM	TO
	TAB 19 Documents for the Project Manager: 1. Certificate of employment for the assigned personnel indicating the date of hire. 2. Resume or Curriculum Vitae indicating the personnel assigned have at least three (3) years' of experience in Project Management and have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippines banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date). 3. Certification for Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

7. **Bidders are reminded to use REVISED FORM 9 for the Certificate of Conformance to the Revised Terms of Reference and REVISED FORM 9-A for the Revised Technical Specifications as attached in this Supplemental Bid Bulletin No. 1 dated 28 August 2025 and submit together with ALL other required documents for the submission and opening of eligibility, technical, and financial documents.**

8. **The Eligibility, Technical Documents and Financial Proposals must be properly tabbed for easy reference and must be submitted in sequence/order per Revised Checklist of Requirements.**

9. The BAC shall no longer entertain any question/request for clarification after the issuance of this Bid Bulletin.

10. Please be advised that bids submitted after the deadline shall only be marked for recording purposes, shall not be included in the opening of bids, and shall be returned to the bidder unopened.

This Supplemental Bid Bulletin No. 1 is issued for the guidance and information of all concerned.

(SIGNED)
The DBP Bids and Awards Committee

ANNEX A (page 1 of 7)

Responses to Queries or Request for Clarifications

Bidder No. 1

#	Page in FORM 9-A	Reference	Statement	BID Queries	TWG Reply
1				Do we need to put remarks or responses on Form 9-A?	There is no need.
2				Do we need to put remarks or responses on Annex A of Form 9-A?	Yes
3				Is Annex A of Form 9-A intended solely for DBP's post-qualification purposes or the bidder will have to indicate response or compliance to this section?	The bidder will have to indicate response or compliance to Annex A of
4	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	2. The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).	Can we submit certifications that are comparable or equivalent to the specified certifications? The stated ISO standards are vendor specific and may not aligned to other aspect of what is required. Our proposed solution is certified in ISO 27001, ISO27017, ISO 27018, ISO27032 and ISO 27701.	Should comply as stated in the requirements.
5	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	2. The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).	Can we request to allow SOC 2 OR SOC 3 certifications since the main difference between SOC 2 and SOC 3 lies in the target audience.	Should comply as stated in the requirements.
6	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.	What is your current brand and version of SIEM?	McAfee
7	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.	Is the current SIEM hosted on-premises or cloud?	On-premise

8	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.	What is the required integration to DBP's SIEM? Do we ingest its content? OR We push content into DBPs SIEM?	Push-content
9	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	6. The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.	Can we request to reduce the required number of Data Protection Officer to at least 1 and submit the Notarized Registration Form, Secretary Certificate of appointment and NPC Portal view of the NPC Approval?	No
10	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	6. The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.	Can we also submit a Secretary certificate in an appointing a 2nd DPO for purposes of identifying a backup of our current DPO.	Yes, provided Employment Certificate indicating full-time employee and with DPO Training Certificates.
11	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise	10.3. Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.	Can we submit comparable or equivalent certification such as AgilePM for our assigned Project Manager?	Should comply as stated in the requirements.
12	Page 10	III. Scope of Work, B. Solutions Platform Requirement		What is the primary email system of DBP. Can we get the actual plans	Microsoft
13	page 13	III. Scope of Work, B. Solutions Platform Requirement B.5. Cloud based Email Threat Security	3. Deployment Modes 3.1 The proposed solution must support for inline deployment mode via MX redirection (active analysis and blocking/quarantie of threats).	For email protection deployment modes. Can this requirement allow different deployment models such as API inline or MX Inline? Requiring to support BOTH methods will have different impacts on securing DBP's email security. Different solutions has different approaches to provide enhance BEC and Advance threat email protection.	MX Inline
14		III. Scope of Work, B. Solutions Platform Requirement B.6. Server Security and Protection	1. General Server Security 1.4. The proposed solution must protect a wide range of platforms including but not limited to: AIX, Almalinux, Amazon Linux, CentOS, CloudLinux, Debian, Oracle Linux, RHEL, Micracle Linux, Red Hat OpenShift, Rocky Linux, Solaris, SUSE Linux, Ubuntu Linux and Windows including legacy OS.	Could you confirm how many DBP servers operates on AIX?	4

SECTION III. BID DATA SHEET

#	Page in Bidding Document	Reference	Statement	BID Queries	TWG Reply
15	Page 18 of Bidding Document	ITB Clause 5.3	For this purpose, contracts similar to the Project shall be: A contract similar to the project refers to any Cybersecurity Managed Services solutions which includes the delivery, subscription, installation, and/or maintenance and support. a. Completed within the last five (5) years prior to the deadline for the submission and receipt of bids contracts with the following options: SLCC Requirement Options 1 Single contract equivalent to at least fifty percent (50%) of the ABC for one year; OR 2 At least two (2) similar contracts, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for	We have completed cybersecurity projects under contracts that involved the supply, delivery, installation, and configuration of solutions, along with comprehensive maintenance support for three years. - Remedial and Preventive Maintenance - 24 x 7 Service Desk Support - 24 x 7 Technical Support and Product Support - Service Delivery Management Service for the duration of the contract - Next Day Hardware Replacement Service **Can you consider the above-described projects as similar contracts?** Additionally, we intend to submit two aggregated contracts. One of these meets more than 25% of the One-Year ABC. The second contract, which we propose to include to fulfill the required 50% threshold, was completed six years ago, specifically in 2019. **Can you consider the contract that has finished 6 years ago as part of our SLCC submission, despite its completion date.**	Should comply as stated in the requirements.
				What is the allotted timeframe for the winning bidder to complete the deployment of all EDR agents?	Within 6 weeks after release of NTP.

Bidder No. 2

#	Page in FORM 9-A	Reference	Statement	BID Queries	TWG Reply
1	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	2. The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).	Is it possible to relax this requirement to allow at least three of the certifications mentioned?	Should comply as stated in the requirements.
2	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.	May we know the brand of the SIEM for possible integration with the platform?	McAfee
3	Page 3	B.2 XDR (Extended Detection and Response)	1. The proposed solution must not be of the same brand and Service Provider that DBP is currently using with Shared Cyber Defense Solution. It must be complementing and not conflicting with the current installed solutions.	Kindly provide details of your existing Cyber Defense Solution.	> Crowdstrike > Extrahop
4			Sletter Subject: Request for Extension of Bidding Document Submission Deadline	***Request for extension of Bidding Document Submission Deadline (2***	No

Bidder No. 3

#	Page	Section	Technical Clarification	TWG Reply
1	81	A.2 Customization, Data Retention and Coverage	Are there other expectations from onsite Support Engineer aside from mentioned in A.2	Yes, as long as it is related to the expertise of the Support Engineer.
2	81	A.2 Customization, Data Retention and Coverage	Are there requirements to forward activity logs from Solution being offered to the SIEM/SOAR if available?	Yes
3	86	B.3. Network Threat Prevention / IPS (Intrusion Prevention System	How many total users will be included in all the Security Awareness campaigns?	4000 to 5000 users
4	100	B.9. CSOC Facility Layout	In terms of implementation, does it included cabling requirements?	Yes
5	102	VII SERVICE LEVEL AGREEMENT (SLA)	Is the onsite Engineer expected to report on DBP every weekday as part of their incident-handling responsibilities with the solutions being offered>	Yes
6	102	VII SERVICE LEVEL AGREEMENT (SLA)	Does it exclude workstation or endpoint-level response actions such as containment or remediation?	No, it may include workstation or endpoint-level response monitored by IT Security Personnel.
7	81	Section 3: A.1 item 6 The solution must have at least two(2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implmentation period of the project.	Can this be removed?	No
8	81	Section 3: A.1 item 10.3 Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel	Can PMP be changed to CAPM	No

Bidding Document Requirements (During Opening of Bids)

#	Page in FORM 9-A	Reference	Statement	Requirements Included in the Opening of Bids
6	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/ licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.	Certification from the solutions provider indicating that the solutions offered can be integrated with on premise McAfee SIEM.
7	Page 1	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	4.The solutions provider/principal must provide a 24 x 7 x 365 Cyber Security Operations Center (CSOC) of the solutions being offered for the period of three (3) years with certified cybersecurity support engineers provided locally and globally. Please refer to Figure 1 (CSOC Network Diagram) and Figure 2 (CSOC Facility Layout) for additional details.	Requirements for local/global Support Engineers (at least two): > Certificate of employment indicating full-time employee. > Certification (at least one per Engineer) indicating Cybersecurity Support Engineer
8	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	5.The solutions provider/principal must deploy the Managed Detection and Response plus Remediation MDR+R-SOC services with the following technical expertise: 5.1.A dedicated onsite support engineer as full-time employee (during the contract period) of the solutions provider and must provide proof of Certificate of Employment and Curriculum Vitae. 5.2.The assigned support engineer must have at least: two (2) years of work experiences as an IT security support engineer, certification on MDR+R solution being offered, and two (2) formal trainings on IT Security Fundamentals.	Requirements for onsite Support Engineer: > Certificate of employment indicating that the personnel is a full-time employee. > Curriculum Vitae where indicated that the personnel has 2 years work experience as an IT Security Support Engineer. > Certification on MDR Solution being offered > Training Certificate (at least 2) on IT Security Fundamentals

9	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	6. The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.	The solution provider must have at least two(2) certified Data Privacy Officers (DPO) supported by the following: > Certificate of employment indicating full-time employee > DPO Certification by an accredited provider.
13	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	9.The solutions provider/principal must deploy a local technical account manager to oversee the continuous improvement of selected technologies installed in DBP's environment. The technical account manager must not be outsourced and must be a full-time employee of the solutions provider/principal, with proof of Certificate of Employment and Curriculum Vitae.	Requirements for Technical Account Manager: > Certtification of employment from the solutions provider and/or principal indicating full-time employee > Curriculum Vitae where indicated experience (at least 2 years) as Technical Account Manager.
14	Page 2	III. Scope of Work, A. Solutions Provider Criteria A.1.Certification Expertise and Reference	10.The solutions provider must designate a Project Manager who must be employed with the solutions provider for at least five (5) years before the bid opening and have at least three (3) years' experience in project management.	Must submit the following: > Certificate of Employment for the assigned personnel indicating the date of hire. > Resume or Curriculum Vitae indicating that the personnel assigned have at least three (3) years experience in Project Management and have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date). > Certification for Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

REVISED FORM 9

(use Bidder's Official Letterhead)

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

CERTIFICATE OF CONFORMANCE TO THE REVISED TERMS OF REFERENCE AND SPECIFICATIONS

I/we, _____ the authorized representative/s of _____ *(name of company)* _____, hereby certify the following:

- That we have thoroughly read and understood the complete set of the bidding documents for the project, particularly the Scope of Works/Terms of Reference, its specifications and requirements, including all revisions, amendments, and supplemental bulletins.

- That should we be awarded the contract, we shall conform and comply to all specifications and requirements as specified in the project's bidding documents and its Terms and Reference.

_____	_____
Name and Signature of Representative	*Name of Company (Bidder)*
_____	_____
Position	*Address*
_____	_____
Contact Numbers	*Date Signed*

I. BACKGROUND

As the current threat landscape continues to evolve and with tightening regulatory requirements, The Development Bank of the Philippines (DBP) due to its continuing reliance in the use of technology as part of its continuing effort to reinforce several layers of protection to preserve its information assets security and become cyber-resilient, DBP seeks to engage a third-party service provider for subscription to a managed detection and response plus remediation solution to immediately detect, contain and remediate attacks.

II. APPROVED BUDGET FOR THE CONTRACT (ABC)

The approved Budget for the Contract (ABC) is **FIFTY-FIVE MILLION PESOS** (PhP55,000,000.00) annually or **ONE HUNDRED SIXTY-FIVE MILLION PESOS** (Php165,000,000.00) for three (3) years. ABC is inclusive of the technical services, all other costs and expenses, Value Added Tax (VAT), and other applicable taxes.

III. SCOPE OF WORK

The engagement shall cover one lot supply, delivery, installation, configuration and subscription of a MANAGED DETECTION AND RESPONSE PLUS REMEDIATION SOLUTION with maintenance support by a service provider, including use of its proprietary technology.

A. SOLUTIONS PROVIDER CRITERIA

A.1. Certification, Expertise and Reference

1. The solutions provider must be an authorized partner of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.
2. The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).
3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.
4. The solutions provider/principal must provide a 24 x 7 x 365 Cyber Security Operations Center (CSOC) of the solutions being offered for the period of three (3) years with certified cybersecurity support engineers provided locally and globally. Please refer to Figure 1 (CSOC Network Diagram) and Figure 2 (CSOC Facility Layout) for additional details.

5. The solutions provider/principal must deploy the Managed Detection and Response plus Remediation MDR+R-SOC services with the following technical expertise:
   5.1. A dedicated onsite support engineer as full-time employee (during the contract period) of the solutions provider and must provide proof of Certificate of Employment and Curriculum Vitae.
   5.2. The assigned support engineer must have at least: two (2) years of work experiences as an IT security support engineer, certification on MDR+R solution being offered, and two (2) formal trainings on IT Security Fundamentals.
6. The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.
7. The solutions provider must have at least 8 years of experience in the ICT industry and must possess extensive knowledge and skills in the latest security technologies, with at least three (3) years of experience in providing cybersecurity solutions preferably on an Enterprise MDR+R-SOC services.
8. The solutions provider must have a similar installed base enterprise cybersecurity solution in private or government entity for the past three (3) years.
9. The solutions provider/principal must deploy a local technical account manager to oversee the continuous improvement of selected technologies installed in DBP's environment. The technical account manager must not be outsourced and must be a full-time employee of the solutions provider/principal, with proof of Certificate of Employment and Curriculum Vitae.
10. The solutions provider must designate a Project Manager who must be employed with the solutions provider for at least five (5) years before the bid opening and have at least three (3) years' experience in project management.

    Must submit the following:

    10.1. Certificate of Employment for the assigned personnel indicating the date of hire.
    10.2. Resume or Curriculum Vitae indicating that the personnel assigned have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date).
    10.3. Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

A.2. Customization, Data Retention and Coverage

1. The solutions provider must deliver customized reports and dashboard. They must tailor the reports and dashboard to align with DBP's specific organizational requirements and cybersecurity challenges.
2. The solutions provider must formulate a complete Knowledge Transfer (KT) on the application, tools, agents, sensors, data collection and data analysis of the proposed solution.
3. The solutions provider must provide continuous collection and centralized storage of all security data for behavioral analytics.
4. The solutions provider must provide data retention of at least 90 days, with options to extend based on DBP's operational and regulatory requirements.

Compliance with industry standards and legal mandates for data storage and privacy.

5. The solutions provider must provide a visibility of lateral movement across the network and other parts of the infrastructure
6. The solutions provider must support detection and response for threats involving managed and unmanaged endpoints, servers, networks, managed email users/mailbox and remote users. Detection mechanisms must include signature-based, behavioral, and AI-driven techniques, with automated response workflows and alerting.

A.3. Trainings, Security Awareness and Other Requirements

1. The solutions provider must formulate a comprehensive cybersecurity training program with TESDA-accredited training center for the following modules and participants:
   1.1. Basic Administration for at least ten (10) participants
   1.2. Knowledge Transfer (Minimum of One (1) knowledge transfer session provided onsite with complete materials.)
2. The solutions provider must develop an Annual Security Posture Assessment Plan, which includes a comprehensive evaluation of DBP's security measures and recommendations for enhancements.
3. The solutions provider must conduct phishing simulation with a unified platform that allows DBP to perform unlimited phishing simulation exercises and security awareness trainings.
4. The solutions provider must include Security Awareness licenses for at least 500 users per campaign and allow tracking of campaigns.
5. The solutions provider must provide phishing simulation tool with standard templates and allow creation of custom templates. The phishing simulation tool must allow recipients to be chosen from different data sources such as but not limited to Active directory, Microsoft Entra ID and Okta.
6. The solutions provider must provide phishing simulation tool with training campaigns. The training campaigns must have training programs in video and interactive format and be targeted for a list of recipients. The training programs must include the following training categories:
   6.1. Business Email Compromise
   6.2. Executives
   6.3. Malware
   6.4. Mobile Security
   6.5. Password Protection
   6.6. Phishing
   6.7. Physical Security
   6.8. Safe Web Browsing
   6.9. Security Beyond the Office
   6.10. Security Essentials
   6.11. Social Engineering
7. The solutions provider must provide phishing simulation tool which allows custom templates to include company images including logos and informative content to the training campaign notification email.

B. SOLUTIONS PLATFORM REQUIREMENT

Summary List of Required Licenses, Equipment and Services:	
Solutions	Technical Specifications
Endpoint Protection (Workstations)	4750 endpoints

Managed Detection and Response plus Remediation
Terms of Reference

Endpoint Detection and Response	5500 sensors
Server Protection	750 servers
Network Detection and Response *	2 units with 1Gbps each of traffic inspection
Network Threat Prevention/IPS (Intrusion Prevention System) *	1 unit – 10Gb inspection throughput; 2 segment 100GbE with bypass option
Cloud Email Security	5000 mailbox
Security Awareness (Phishing Simulation)	500 users
CSOC Layout	1 Lot

* All facility/solution components (servers/nodes) must be equipped with dual power supplies. This ensures power redundancy and enhances system availability in the event of a power source failure.

* Any facility/solution components (servers/nodes) that requires a direct connection to the core switch—based on its designated function or operation demands—must be equipped with a network interface supporting a minimum throughput of 10Gbps. This ensures compatibility with existing network infrastructure.

B.1. Threat Detection and Continuous Monitoring

1. Threat Hunting and Threat Intelligence

2. The proposed solution must be able to monitor for advanced threat protection security alerts, breaches, anomalies and advanced persistent threats within the scope of licenses installed under this project.
3. The proposed solution must have defined hunting techniques that are implemented using the capabilities from existing Bank's Anti-APT (Advanced Persistent Threats) technologies, proposed EDR (Endpoint Detection and Response), Email Sensor and Network Forensic device.
4. The proposed solution must provide a 24x7x365 Managed Threat Hunting Service.
5. The proposed solution must conduct continuous Vulnerability Management, Phishing Simulation Exercises and (IR) Incident Response as needed.
6. The proposed solution must have proven and established protocols for threat hunting, defined threat hunting process and triggers for threat hunts and hunt success measurement.
7. The proposed solution must conduct threat hunting based on analysis of suspicious signals, custom detection rules, and internal threat intelligence research.
8. The proposed solution must contain active threats detected, by isolating endpoints and removing malicious files or processes.
9. The proposed solution must provide integration with threat intelligence feeds for the identification of IoC (Indicators of Compromise).
10. The proposed solution must have defined indicators that will trigger a proactive threat hunt.
11. The proposed solution must support sharing of IoCs across multivendor security stack.
12. The proposed solution must provide proactive threat reports for verified threats and/or provide emerging threat reports on emerging threats affecting multiple organizations, designed to help the organization stay ahead of high-profile cyber-attacks.

13. Visibility and Detection

14. The proposed solution must provide a comprehensive visibility across network, endpoint, server, and email.
15. The proposed solution must have visibility into data sources including endpoint device, email, network packet/session.
16. The proposed solution must provide monitoring and detection of behavioral anomalies on unmanaged devices.
17. The proposed solution must provide monitoring and detection of behavioral anomalies for users.
18. The proposed solution must provide analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, email and user events over time.
19. The proposed solution must have identity analytics to detect user-based threats such as lateral movement.
20. The proposed solution must provide optimized and customizable detections and BIOCs (Behavioral Indicator of Compromises).

B.2. XDR (Extended Detection and Response)

1. The proposed solution must not be of the same brand and Service Provider that DBP is currently using with Shared Cyber Defense solution. It must be complementing and not conflicting with the currently installed solutions.
2. The proposed solution must be able to collect and correlate XDR activity data for one or more vectors using the same brand, including but not limited to - endpoints, emails, servers and networks.
3. The proposed solution must include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking for the proposed sensors for endpoints, servers, email, identities and network. It must be regularly updated to improve threat detection capabilities and reduce false positive alerts.
4. The proposed solution must have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements.
5. The proposed solution must allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.
6. The proposed solution must be able to analyze and determine if certain indicators signal an ongoing attack, enabling IT Admins and CSOC team to take timely prevention, investigation, and mitigation actions against targeted attack campaigns.
7. The proposed solution must list all the events that are mapped into the MITRE ATT&CK framework, the CSOC Analyst can use these events as starting point to do further investigations.
8. The proposed solution must provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.
9. The proposed solution must have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.
10. The proposed solution must have an AI-powered chatbot to guide with the investigations and automatically provide answers to any questions related to cybersecurity.
11. The proposed solution must generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.
12. The proposed solution must provide different search methods, filters, and an easy-to-use Kibana-like query language to identify, categorize, and retrieve search results.

Managed Detection and Response plus Remediation
Terms of Reference

13. The proposed solution must provide a unified platform that enables security teams to take immediate response and track actions across email, identity, endpoints, and networks.
14. The proposed solution must be able to take response actions directly from the platform's investigation workbench.
15. The proposed solution must be able to automate response and remediation actions by identifying compromised accounts, applying advanced analytics, streamlining response rules, and making contextualized decisions from the platform's security playbook.
16. The proposed solution must have the ability to Add or Remove supported indicators of compromise to the block list, including but not limited to File Hash, URL, IP address, Email Addresses and Domains.
17. The proposed solution must allow automatic and manual collection of files and objects from specified endpoints.
18. The proposed solution must support automatic and manual sweeping based on solutions provider curated and third-party custom intelligence to search the environment for indicators of compromise.
19. The proposed solution must be able to view information about suspicious objects obtained by analyzing the suspicious file in a sandbox, a secure virtual environment.
20. The proposed solution must allow a CSOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Intelligence Information).
21. The proposed solution must have the capability to automate a variety of actions usings playbooks to help reduce workload and speed up security tasks and investigations.
22. The proposed solution must have the capability to create playbooks from scratch or use built-in templates to suit the organization's specific needs.
23. The proposed solution must be capable of integrating with a cybersecurity platform that can manage the organization's Email, Identity, Endpoint, Network and XDR solution all in a single console.
24. The proposed solution must provide insights into the organization's security posture using an executive level dashboard. It must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors.
25. The proposed solution must have the capability to provide recommended actions to harden the environment with security configuration against future potential attacks.
26. The proposed solution must have a highly customizable dashboard that provides widgets displaying statistics from Attack Surface, Email, Identity, Endpoint, Network, SecOps and XDR.
27. The proposed solution must be able to produce manual and scheduled reports that can be customized to display company information and logo. The generated reports must at least support PDF format and can be sent to specified email recipients.
28. The proposed solution must provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.
29. The proposed solution must be able to integrate with common SIEM and SOAR solutions.
30. The proposed solution must be able to integrate with 3rd party LDP solutions for Single Sign-On (SSO) requirements.
31. The proposed solution must provide connectors ready to integrate with other supported third-party security solutions (provide a list) or via API.

B.3. Network Threat Prevention/IPS (Intrusion Prevention System)

1. Network Intrusion Prevention System.

   1.1. The proposed IPS solution must be an appliance-based on a hardened OS shipped by-default from manufacturer.
   1.2. The proposed IPS solution must be able to store at least 200 million historical events.
   1.3. The proposed IPS solution must allow the update and distribution of latest security updates to be manually, automatically or based on schedule to the IPS device.
   1.4. The proposed IPS solution must be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through IPS.
   1.5. The proposed IPS solution must serve as a central point for IPS security policies management including versioning, rollback, import and export(backup) tasks.
   1.6. The proposed IPS solution must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report.
   1.7. The proposed IPS solution must support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis
   1.8. The proposed IPS solution must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
   1.9. The proposed IPS solution must support the archiving and backup of events and export to NFS, SMB, SCP or sFTP
   1.10. The proposed IPS solution must be able to support the syslog CEF (Common Event Format) for SIEM integration.
   1.11. The proposed IPS solution must support Active Directory for user ID correlation.
   1.12. The proposed IPS solution must support AFC (Adaptive Filter Configuration) which will alert or disable ineffective filter in case of noisy filters.
   1.13. The proposed IPS solution must support 3rd party VA (Vulnerability Assessment) scanners (e.g. Qualys, Rapid7 or Tenable) to fine tune the IPS policy
   1.14. The proposed IPS solution must support 'threat insights' dashboard that show correlated data such as how many breached host, how many IoC data, 3rd party VA scan integration data and how many pre-disclosed vulnerabilities are discovered.
   1.15. The proposed IPS solution must be able to integrate with the existing Endpoint and Server Security solution to share IoC (Indicator of Compromise) feed with IPS for protection.
   1.16. The proposed IPS solution must be integrated with the XDR platform for single visibility of events and management.

2. Network IPS Security.
   2.1. The proposed IPS solution must provide intrusion prevention functionality out of the box, with approximately 20% of filters enable in blocking mode by default

2.2. The proposed IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine
2.3. The proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic, detect and block unknown threats associated with known malware families as well as unknown malware in real-time as they enter and cross the network
2.4. The proposed IPS filters must be categorized into the following list for easy management.
  2.4.1. Exploits
  2.4.2. Identity Theft/Phishing
  2.4.3. Reconnaissance
  2.4.4. Security Policy
  2.4.5. Spyware
  2.4.6. Virus
  2.4.7. Vulnerabilities
  2.4.8. Network Equipment
  2.4.9. Traffic Normalization
  2.4.10. Peer to Peer
  2.4.11. Internet Messaging
  2.4.12. Streaming Media
  2.4.13. Filters not limited to Microsoft, Adobe, SCADA/ICS system.
2.5. The proposed IPS solution must provide the following security features on top of the IPS filters:
  2.5.1. Domain Generation Algorithm (DGA) Defense family of filters to detect DNS requests from malware infected hosts that are attempting to contact their command and control (C&C) hosts using DGAs.
  2.5.2. Ransomware protection
  2.5.3. Identify malicious Internet Protocol (IP)
2.6. The proposed IPS solution must be able to support granular security policy enforcement based on the following methods:
  2.6.1. Per IPS device (all segments)
  2.6.2. Per physical segment uni-direction and bi-directional
  2.6.3. Per 802.1Q VLAN Tag uni-direction and bi-directional
  2.6.4. Per CIDR IP address range
  2.6.5. Per 802.1Q VLAN Tag and CIDR as well
  2.6.6. Firewall policy per security profile
2.7. The proposed IPS solution must have a vulnerability-based filters as part of the security policies.
2.8. The proposed IPS solution must support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods
2.9. The proposed IPS solution must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc
2.10. The proposed IPS solution must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C
2.11. The proposed IPS solution must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment
2.12. The proposed IPS solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploitability type and the reputation score
2.13. The proposed IPS solution must be able to provide zero-day filters.

2.14. The proposed IPS solution must have the ability to view attack activities base on continent and countries
2.15. The proposed IPS solution must allow drill-down to view detailed threat source and destination data on each attack type

3. Network IPS appliance.
   3.1. The proposed IPS appliance must support a centralized management server for enterprise management of up to 25 IPS devices.
   3.2. The proposed IPS appliance must have at least 64GB RAM and 800GB storage (2x800GB SSD, RAID 1), 1RU and with redundant hot-swappable power supply.
   3.3. The proposed IPS appliance must have a Dual 1GbE RJ45/Dual 25GbE SFP28 with out-of-box remote management capabilities
   3.4. The proposed IPS appliance must have a flexible and scalable licensing model capable of up to 40Gbps of inspection throughput. The inspection throughput required must be a minimum of 10Gbps.
   3.5. The proposed IPS appliance must support up to 300million concurrent connections
   3.6. The proposed IPS appliance must support up to 1M new connections per second.
   3.7. The proposed IPS appliance must have a latency of less than forty (60) microseconds.
   3.8. The proposed IPS appliance must have at least 2segment 100GbE SR4 Bypass interface.
   3.9. The proposed IPS appliance must have a built-in power failure bypass module that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedures
   3.10. The proposed IPS appliance must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors.
   3.11. The proposed IPS appliance must support hitless OS upgrade/Reboot which allow upgrading of the IPS operating system without required network downtime.

B.4. Network Detection and Response (NDR)

1. NDR Security.
   1.1. The proposed NDR solution must be able to monitor multiple network segments (including internal network east-west traffic) for lateral movements.
   1.2. The proposed NDR solution must be able to monitor over 100 network protocols to identify targeted attacks, advanced threats, and ransomware.
   1.3. The proposed NDR solution must provide detection of known and unknown malware being transmitted through a variety of communications channels such as: HTTP, SMTP, IMAP, POP3, and FTP
   1.4. The proposed NDR solution must be able to detect zero-day malware such as document exploits.
   1.5. The proposed NDR solution must provide detection of known malicious communications such as Command and Control and Data Exfiltration
   1.6. The proposed NDR solution must provide detection of targeted attacks and advanced threats
   1.7. The proposed NDR solution must provide details of attackers' network activity

1.8. The proposed NDR solution must have built-in sandboxing technology. It must be a custom sandbox that allows the DBP to upload their tailor fitted image on the box.
1.9. The proposed NDR solution must be able to integrate with the proposed email, endpoint and server solution for automatic and seamless blocking of malicious files, IPs, or URLs
1.10. The proposed NDR solution must provide a configurable dashboard for quick access to critical information
1.11. The proposed NDR solution must provide extensive detection techniques utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.
1.12. The proposed NDR solution must have an automated response. Once an unknown C&C connection has been detected inside the network, it must be able to share to the IPS or supported firewall solution for blocking.

2. NDR Appliance,
2.1. The proposed NDR appliance must be managed by the solutions provider, control and visibility must be extended to DBP.
2.2. The proposed NDR appliance must include a regular (at least quarterly and/or as needed) preventive maintenance.
2.3. The proposed NDR appliance must include 2 units of at least 1 Gbps each.
2.4. The proposed NDR appliance must support packet level analysis.
2.5. The proposed NDR appliance must be installed in monitoring mode only
2.6. The proposed NDR appliance must report to a unified XDR platform for event correlation across proposed endpoint, server and email sensors.

3. NDR Sandboxing.
3.1. The proposed NDR solution must support custom Windows and MacOS Sandbox.
3.2. The proposed NDR solution must be able to provide threat execution and evaluation summary
3.3. The proposed NDR solution sandbox reports must be exportable
3.4. The proposed NDR solution must be able to track system file and registry modification
3.5. The proposed NDR solution must be able to detect system injection behavior detection
3.6. The proposed NDR solution must be able to detect network connections initiated
3.7. The proposed NDR solution must support the following content types for document exploits: PDF, XLS, DOC, SWF, RTF
3.8. The proposed NDR solution must support the following compressed files: ZIP, RAR, PKZIP, LZH
3.9. The proposed NDR solution must support the following Microsoft OS file formats: EXE, DLL, SYS, CHM, LNK

B.5. Cloud based Email Threat Security

1. Threat Detection and Protection.
1.1. The proposed solution must have protection from AETs (Advanced Evasion Techniques) using malformed emails.
1.2. The proposed solution must have retroactive alerting for URLs later determined to be malicious.

1.3. The proposed solution must extract and block suspicious URLs embedded in PDF files within emails.
1.4. The proposed solution must detect and block advanced threats in emails: attachment, URL, and impersonation-based attacks.
1.5. The proposed solution must dynamically analyze attached files, including those with password-protection and TLS (Transport Layer Security) encryption.
1.6. The proposed solution must have a collaboration protection capability to detect malicious files found in SharePoint, OneDrive, Teams, Google Drive, Box, and Dropbox.
1.7. The proposed solution must have an IP reputation checking capability to block emails from known sources of spam emails (RBL- Realtime Blackhole Lists).
1.8. The proposed solution must have domain authentication capabilities (e.g. SPF, DKIM, DMARC)
1.9. The proposed solution must protect against spam, malware, phishing, BEC (Business Email Compromise), and ransomware email attacks.
1.10. The proposed solution must be able to identity and detect graymail based on their category (e.g. marketing and newsletter, social network notifications, forum notifications, bulk email message)
1.11. The proposed solution must support file sanitization (or Content Disarm and Recovery) to neutralize all unfamiliar code hiding in emails that contain active content such as macros in the email attachments.
1.12. The proposed solution must have an attachment password guessing capability which attempts to find passwords in email content to access password-protected attachments, making it possible to scan and detect any malicious payload in these files.
1.13. The proposed solution must have a predictive machine learning scanning capability to find unknown malware before cloud sandboxing and improve delivery efficiency.
1.14. The proposed solution must support cloud sandboxing of suspicious file attachments and suspicious URLs found in email.
1.15. The proposed solution must provide URL rewriting and URL time of click protection capabilities.
1.16. The proposed solution must have a web reputation technology to scan URLs in email messages and track the credibility of web domains by assigning a reputation score based on factors including website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing attacks that are designed to trick users into providing personal information.
1.17. The proposed solution must support URL extractions from QR codes to stop phishing, ransomware, and BEC attacks.
1.18. The proposed solution must support dynamic URL scanning and crawl on the web pages of untested URLs in real-time to determine whether the pages contain malicious patterns to keep users from zero-day phishing attacks.
1.19. The proposed solution must leverage artificial intelligence (AI)-based computer vision to analyze branded website elements and recognize fake sites to protect users against credential phishing.
1.20. The proposed solution must have an AI-based computer vision to recognize key elements of a valid cloud service log-on page or forms to help prevent users from submitting credentials to untrusted sites and help them get rid of account compromise.

1.21. The proposed solution must detect display name spoofing and be able to analyze messages from external senders with a look-alike display name as used in the company.
1.22. The proposed solution's BEC detection must support adding and maintaining a list of HPU (High-Profile Users) and HPD (High-Profile Domains).
1.23. The proposed solution's BEC detection must check the email header for behavior analysis and the email content for intention analysis.
1.24. The proposed solution's BEC detection must support Writing Style DNA technology and provide authorship analysis to detect email attacks impersonating high-profile users.
1.25. The proposed solution must check for unusual signals or behaviors in email (e.g. the sender has not sent any email in at least the past 30 days, unfamiliar sender discussing payment related issues, etc.)
1.26. The proposed solution must provide account takeover protection and alert if an account has been compromised to steal data, deliver malware, or conduct internal and supply chain phishing.
1.27. The proposed solution must offer DLP (Data Loss Prevention) capability both for email messages and files in cloud collaboration services.
1.28. The proposed solution must offer an email encryption capability and be able to encrypt email content for confidentiality.
1.29. The proposed solution must be able to retro-scan historical email messages to identify and stop previously unknown or undetected threats in messages, such as spam, phishing, and malware, and take automated remediation actions using the latest pattern files and machine learning technologies.
1.30. The proposed solution must be able to rescan historical URLs in users' email metadata and perform automated remediation (automatically taking configured actions or restoring quarantined messages) using the latest pattern files updated by the web reputation services.
1.31. The proposed solution must be able to run a manual scan and perform an on-demand scan of targets including exchange mail stores, SharePoint sites, and file stores.
1.32. The proposed solution must be able to integrate with MIP (Microsoft Information Protection) to decrypt and scan MIP-encrypted emails and files.
1.33. The proposed solution must be able to decrypt and scan MIP-encrypted email messages/attachments in Exchange Online and MIP- encrypted files in SharePoint, OneDrive, and MS Teams.
1.34. The proposed solution must include an email continuity feature and provide a standby email system for virtually uninterrupted use of email in the event of a mail server outage.
1.35. The proposed solution must be able to keep the incoming email messages for at least 10 days and be able to restore email messages to the email server once it's back online within the 10-day period, if a planned or unplanned outage occurs.
1.36. The proposed solution must have a continuity mailbox available instantly and automatically providing end users the ability to read, forward, download and reply to any email messages and have continued email access during an outage.
1.37. The proposed solution must have the ability to delete the selected email message from the selected mailboxes.
1.38. The proposed solution must have the ability to move the selected email message to the quarantine folder and quarantine the message from all affected mailboxes.

1.39. **The proposed solution must be able to prevent or mitigate cyberthreats and other email attacks with solutions provider or DBP's feed threat intelligence.**

2. Advanced Threat Alerts and Forensics.
   2.1. The proposed solution must provide detailed information on every advanced threat alert, including alert ID, date and time, sender's email address, targeted email addresses, malicious email subject, MD5 hash, malicious URL or attachment, originating email server, email status, threat classification, and severity.
   2.2. The proposed solution must provide dynamic analysis of malware file types, vulnerable applications, and operating systems.
   2.3. The proposed solution must provide forensic evidence including malicious files and network activity packet captures.
   2.4. The proposed solution must provide malware communications report detailing URL analysis and raw requests.
   2.5. The proposed solution must provide native report on operating system changes, services, registry keys, and system configuration changes.
   2.6. The proposed solution must provide threat intelligence report with detailed information on detected threats, including risk level, affected software, vulnerability information, and remediation patches.

3. Deployment Modes.
   3.1. The proposed solution must support for inline deployment mode via MX redirection (active analysis and blocking/quarantine of threats).
   3.2. The proposed solution must support API for internal email inspection.
   3.3. The proposed solution must be Cloud-based with no hardware or software to install.
   3.4. The proposed solution must provide real-time, dynamic threat protection.
   3.5. The proposed solution must be ISO27001 compliant, adhering to the Information Security Management System (ISMS) standard.
   3.6. The proposed solution must be 99.9% availability guaranteed.

4. Access Control.
   4.1. The proposed solution must limit domains and domain groups access for users (Full or Read Only access).
   4.2. The proposed solution must not allow users to modify policies outside their assigned domains and groups.

5. Customization and User Interface.
   5.1. The proposed solution must provide customizable email digest templates in the Web UI.
   5.2. The proposed solution must provide end-user portal for quarantine management and review of malicious emails.

6. Integration and Compatibility.
   6.1. The proposed solution must provide integration with an XDR platform for alert correlation.

7. Dashboard and Reporting.
   7.1. The proposed solution must provide native dashboard statistics with threat map displaying threat locations.
   7.2. The proposed solution must provide daily digests of quarantined emails for specific users/recipients.

7.3. The proposed solution must provide executive summary report of email traffic, content analysis, and threat categories.

8. Email Handling Rules.
   8.1. The proposed solution must provide creation of allow and deny rules based on criteria such as reverse DNS validation, sender country internet domain suffix, recipient email address, sender IP address, sender email address, and sender email domain.
   8.2. The proposed solution must have the ability to drop, quarantine, deliver, route, BCC (Blind Carbon Copy), insert custom headers, and modify the subject of emails based on specific criteria.
   8.3. The proposed solution must have the ability to bypass antivirus and antispam scanning based on specific criteria.

9. File Type Analysis.
   9.1. The proposed solution must provide dynamic analysis of attached file types and/or extensions such as EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives.

B.6. Server Security and Protection.

1. General Server Security.
   1.1. The proposed solution must have an option for on-premise management for server protection over physical and virtual servers.
   1.2. The proposed solution must allow the on-premise management server to connection to a cloud-based unified XDR platform.
   1.3. The proposed solution must provide layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.
   1.4. The proposed solution must protect a wide range of platforms including but not limited to: AIX, AlmaLinux, Amazon Linux, CentOS, CloudLinux, Debian, Oracle Linux, RHEL, Micracle Linux, Red Hat OpenShift, Rocky Linux, Solaris, SUSE Linux, Ubuntu Linux and Windows including legacy OS.
   1.5. The proposed solution must have multiple security modules listed below, providing a line of defense at the server in a single agent:

      1.5.1. Anti-Malware
         1.5.1.1. The proposed anti-malware solution must provide agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, trojans, and spyware.
         1.5.1.2. The proposed anti-malware solution must allow manual and schedule scans to be configured.
         1.5.1.3. The proposed anti-malware solution must be able to provide Web Reputation filtering to protect against malicious web sites
         1.5.1.4. The proposed anti-malware solution must have an option to configure its detection and prevention level from cautious, moderate to aggressive and extra aggressive for its protection capabilities.
         1.5.1.5. The proposed anti-malware solution must have Predictive Machine Learning to protect against unknown malware.

1.5.1.6. The proposed anti-malware solution must have behavioral monitoring to protect against suspicious activity and unauthorized changes including ransomware.

1.5.1.7. The proposed anti-malware solution must provide ransomware protection, that can backup & restore encrypted documents.

1.5.1.8. The proposed anti-malware solution must scan process memory for malware.

1.5.2. Device Control

1.5.2.1. The proposed device control solution must support USB mass storage, autorun function and mobile – MTP (Media Transfer Protocol) /PTP (Picture Transfer Protocol).

1.5.2.2. The proposed device control solution must have option to choose from full access, read only and block.

1.5.3. Intrusion Detection and Prevention System

1.5.3.1. The proposed solution must be able to provide HIPS (Host Intrusion Prevention System) /HIDS (Host-Based Intrusion Detection System) features.

1.5.3.2. The proposed solution must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.

1.5.3.3. The proposed solution must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.

1.5.3.4. The proposed solution must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.

1.5.3.5. The proposed solution must be able to provide protection against known and zero-day attacks

1.5.3.6. The proposed solution must provide protection that can be pushed out to thousands of servers in minutes without a system reboot.

1.5.3.7. The proposed solution must include out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services.

1.5.3.8. The proposed solution must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code

1.5.3.9. The proposed solution must include exploit rules to stop known attacks and malwares.

1.5.3.10. The proposed solution must assist in compliance of PCI DSS (Payment Card Industry Data Security Standard) to protect web applications and the data being process.

1.5.4. Firewall

1.5.4.1. The proposed solution must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.

1.5.4.2. The proposed solution must have fine-grained filtering (IP and MAC addresses, ports).
1.5.4.3. The proposed solution must have coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)
1.5.4.4. The proposed solution must have prevention of denial of service (DoS) attack
1.5.4.5. The proposed solution must allow policies per network interface
1.5.4.6. The proposed solution must have detection of reconnaissance scans.

1.5.5. Integrity Monitoring
1.5.5.1. The proposed solution must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real-time.

1.5.6. Virtual Patching
1.5.6.1. The proposed solution must provide virtual patching which shields vulnerable systems that are awaiting a security patch. It must automatically shield vulnerable systems within hours and push out protection to thousands of workloads within minutes.
1.5.6.2. The proposed solution must have the intelligence to provide recommended virtual patching rules to protect against OS & Application vulnerabilities.
1.5.6.3. The proposed solution must be able to create scheduled tasks to run recommendation scan to discover new rules to apply.
1.5.6.4. The proposed solution must be able to automatically assign new virtual patching rules through scheduled tasks.
1.5.6.5. The proposed solution must be able to automatically unassign virtual patching rules after physical patch has been installed.
1.5.6.6. The proposed solution must support more than 350 distinct applications for virtual patching but not limited to web applications, databases, etc.

1.5.7. Log Inspection
1.5.7.1. The proposed solution must be able to provide the capability to inspect logs & events generated by operating systems & applications
1.5.7.2. The proposed solution must be able to automatically recommend and assign relevant log inspection rules to the server based on the operating system & applications installed
1.5.7.3. The proposed solution must be able to automatically recommend and unassign log inspection rules that are not required
1.5.7.4. The proposed solution must have predefined template for operating system and enterprise application to avoid manual creation of the rules
1.5.7.5. The proposed solution must allow creation of customized rules to support custom application

1.5.8. Application Control

1.5.8.1. The proposed solution must be able to monitor changes made to the server compared to baseline software
1.5.8.2. The proposed solution must be able to allow or block the software and optionally lock down the server from unauthorize change
1.5.8.3. The proposed solution must allow maintenance mode to allow installation of software and changes OS
1.5.8.4. The proposed solution must have an alert when unauthorized scripts and application are executed.
1.5.8.5. The proposed Application Control solution must support the following software:
1.5.8.5.1. Windows applications (.exe, .com, .dll, .sys)
1.5.8.5.2. Linux libraries (.so) and other compiled binaries and libraries
1.5.8.5.3. Java .jar and .class files, and other compiled byte code
1.5.8.5.4. PHP, Python, and shell scripts, and other web apps and scripts that are interpreted or compiled on the fly
1.5.8.5.5. Windows PowerShell scripts, batch files and other Windows-specific scripts (.wsf, .vbs, .js)

B.7. Endpoint Protection, Detection and Response with Remediation

1. General Endpoint Protection and EDR.
   1.1 The proposed solution must be able to integrate with the proposed Network Detection and Response Solution.
   1.2 The proposed solution must be able to automatically receive IOCs regarding alert detections from existing Network Advance Threat Platform.
   1.3 The proposed solution must be a SaaS based endpoint security and EDR solution.
   1.4 The proposed solution must have an option to deploy a hardened service gateway to act as a forward proxy service that connects on-premise solutions to the cloud-based platform.
   1.5 The proposed solution must be managed through the unified XDR platform.
   1.6 The proposed solution must be able to analyze and validate network alerts by finding evidence of matching threat activity on endpoints quickly.
   1.7 The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence.
   1.8 The proposed solution must allow for detection, validation and containment through the native interface.
   1.9 The proposed solution must able to isolate at-risk endpoints to run an investigation and resolve security issues and restore the connection promptly when all issues have been resolved.
   1.10 The proposed solution must allow creation of custom indicators of compromise, and support those shared by others using OpenIOC format.
   1.11 The proposed solution must display inactive hosts i.e. the number of monitored hosts that have not checked in for 30 days or more.
   1.12 The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence including

known malware, malware variants/key functions, methodology and behavioral IOCs.

1.13 The proposed solution must allow creation of custom indicators of compromise coming from past/ongoing investigations or external entities.

1.14 The proposed solution must have anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. It must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.

1.15 The proposed solution must support the ability to exclude applications or files from exploit detection.

1.16 The proposed solution must support the recording of recent activity on each endpoint in an indexed and searchable lookback cache, minimally file writes, registry operations, network connections, DNS resolutions, URL collection, process loaded in memory.

1.17 The proposed solution must be able to remotely acquire files and other triage information for investigation purposes.

1.18 The proposed solution must be able to remotely connect to an endpoint and dump process memory.

1.19 The proposed solution must have the ability to remotely connect and execute custom PowerShell or Bash scripts.

1.20 The proposed solution must have the ability to execute custom YARA rules on the specified endpoints.

1.21 The proposed solution must have the ability to view and terminate active processes on a specific endpoint or multiple endpoints.

1.22 The proposed solution must offer a built-in graphical triage viewer to ease security operations and require no more than an entry level CSOC analysts and/or IR responder skillset to operate

1.23 The proposed solution must support concurrent searches across all endpoints.

1.24 The proposed solution must have the ability to pull locally stored data from specified endpoints in near real-time to support high priority hunt and forensic operations

1.25 The proposed solution must provide full visibility into commands issued via the native operating system shell (i.e., Windows command prompt or Bash). It must also provide full visibility into commands issued via augmented shells, such as Windows PowerShell.

1.26 The proposed solution must be able to read and display locally stored data from specified endpoints

1.27 The proposed solution must support containment of suspected hosts while maintaining access to the endpoint forensics solution for investigation as well as other whitelisted resources used for investigation or remediation.

1.28 The proposed solution must be able to automatically terminate exploited applications or automatically prevent any payload from exploited application to run.

1.29 The proposed solution must be able to notify end-user automatically when isolating at-risk endpoints ensuring seamless user experience.

1.30 The proposed solution must allow grouping of endpoints into host sets based on distinguishing attributes. It must be able to identify and label high-value hosts.

1.31 The proposed solution must be able to throttle the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests.

1.32 The proposed solution must at the minimum support the following prevention capabilities:
   i. Antimalware with signature/Pattern based detection
   ii. Ransomware protection
   iii. Machine learning - pre-execution and runtime
   iv. Browser exploit protection
   v. Behavior monitoring
   vi. Injection protection
   vii. Script protection
   viii. Anti-exploit
   ix. C&C communication prevention
   x. Application control
   xi. File less malware prevention
   xii. File/web reputation

1.33 The proposed solution must support proxy, fully configurable in the Web UI and in the CLI.

1.34 The proposed solution must support tamper protection, such as requiring password to uninstall the agent from an endpoint.

1.35 The proposed solution must be able to regulate the number of indicators and exploit alerts processed by the service provider solution.

1.36 The proposed solution must also include Anti-virus protection and machine learning protection.

1.37 The proposed solution's machine learning must have pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.

1.38 The proposed solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and must have feature with documents to be protected from unauthorized encryption or modification.

1.39 The proposed solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.

1.40 The proposed solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source/Destination/ Port/Protocol/Application to provide stateful inspection and high performance network virus scanning.

1.41 The proposed solution must have an integrated Application Control to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities.

1.42 The proposed Application Control solution must provide global and local real-time threat intelligence based on good file reputation data correlated across a global network.

1.43 The proposed Device Control solution must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The devices able to be restricted must include but not limited to the following:
   i. USB Storage Drives (Also able to disable autorun)
   ii. CD-ROM
   iii. Floppy Disk
   iv. Network Drives

1.44 The proposed Device Control solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT , Imaging Devices, Wireless Nic, Infrared devices

1.45 The proposed solution must have an integrated Data Loss Prevention capability to provide data leakage prevention.
1.46 The proposed solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (trojans, registry entries, and viral files).
1.47 The proposed solution must be able to schedule and provide on-access malware scan support. e.g. Requests for full scans, quick scans, and memory scans (which scan running processes).
1.48 The proposed solution must support malware remediation. e.g. removing artifacts created by the malware and revert changes the malware made to other files or registry entries.
1.49 The proposed solution must provide global and exception policies to control malware protection.
1.50 The proposed solution must be able to support malware definitions downloadable either from the Internet or service provider solution
1.51 The proposed solution must be able to download false positive malware information.
1.52 The proposed solution must support malware alert throttling. Alerts generated when malware is detected on endpoints are throttled to limit the maximum number of alerts produced for a single infection in a given time interval.
1.53 The proposed solution must classify attack detections using the taxonomy defined in the MITRE ATT&CK framework.
1.54 The proposed solution must provide automated analysis and visualization of an attack; including entity relations graphing, production of an event timeline and initial assessment of severity/impact/confidence level.
1.55 The proposed solution must provide vulnerability protection solution integrated on a single security agent.
1.56 The proposed solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.
1.57 The proposed solution must support at least Windows 7 Operating System.

B.8. Firewall Monitoring

1. The solution provider must provide continuous firewall log monitoring 24x7.
2. The solution provider must provide detection of security anomalies such as:
   2.1. Unauthorized access attempts
   2.2. Policy violations
   2.3. Port Scans, DoS attempts, or unusual traffic patterns
   2.4. Denial of Service (DoS) or DDoS attempts
   2.5. Intrusion attempts (via IPS)
   2.6. Command and Control (C2) communications
   2.7. Access to malicious or phishing websites
   2.8. Unusual traffic patterns or spikes
   2.9. Use of unauthorized or risky applications
3. The solution provider must provide escalation of critical alerts according to severity and predefined SLAs.
4. The solution provider must generate monthly monitoring reports including:
   4.1. Alert Summary
   4.2. Top Talkers

4.3. Policy usage
4.4. Threat trends

B.9. CSOC Facility Layout

Technical Specifications	Quantity
1. Videowall 2 x 3 Display, Diagonal Size 55", Resolution 1920x1080 (min), with wall-mounting brackets.	6 units
2. Videowall Controller (Minimum Core i9 12th Gen) and Videowall Management Software	1 unit
3. Triple Monitor Workstation with table console, chair and peripherals.	3 sets
4. Uninterruptible Power Supply (UPS) covering the power load requirements of the CSOC equipment.	1 lot
5. Air Cooling Unit (ACU) covering the CSOC area	1 lot
6. Networks (42u Modular Rack, 24port POE Switch, cablings, roughing in materials and accessories).	1 lot
7. Other Miscellaneous Components (video capture card, graphic card, HDMI extender/splitter, USB extender, wall plate, etc.)	1 lot
8. Installation, Configuration and Knowledge Transfer.	1 lot

IV. PERIOD COVERAGE

The contract of the project shall cover the delivery, subscription, installation, configuration, testing and commissioning including training, maintenance and after Sales Support. Which will commence upon receipt of the ***Notice to Proceed*** by the bidder. License subscription will start upon issuance of the Certificate Acceptance by DBP.

V. IMPLEMENTATION DELIVERABLES

The selected service provider shall provide 3 years subscription of Cloud Based Email Security for 5,000 mailbox, 5500 sensors of Endpoint Detection and Response (EDR), Endpoint Protection (workstation)for 4,750 endpoints and on-premise EDR solution for 750 Servers, 2 units of on-premise Network Forensics/ Packet Capture Solution, 1 unit of Network Intrusion Prevention System (IPS) with 3 years maintenance support, Security awareness license for 500 users and 1 lot Cyber Security Operation Center (CSOC) Facility Layout (Section III under B.8).

A. **Work Plan**. This must contain, at a minimum, the following:
   1. Scope
   2. Breakdown of regular activities for Manage Detection and Response plus Remediation
   3. Deliverables

B. **Technology Deployment.** All required endpoint and network technology shall remain fully operational throughout the engagement period. The deployment and disposition of these technologies shall be carried out by the Service Provider, under the monitoring of DBP. Additionally, the Service Provider must utilize a reliable tool for deploying and un-installing the agent.

   The Service Provider must provide weekly status report with the following details:
   - Number of successful and unsuccessful endpoints installation.

- Failures or errors encountered during the installation/uninstallation
- Status per endpoint (e.g. success, failed, pending) including timestamp per hostname and IP Address.

C. **Conduct of Managed Detection and Response plus Remediation Service** (based on the Scope as indicated in Section III)

D. **Status Reporting.** A weekly, monthly & quarterly status report of all activities performed shall be provided to DBP on a regular basis, until closure of engagement.

E. **Reports.** The Managed Detection and Response plus Remediation engagement shall provide, but not limited to the following reports:

1. Regular management reporting of detected emerging threats, trends and actionable mitigation.
2. Personalized intelligence reports that offer insight into organization's risk profile, key findings, attacker profiles and motivations, and industry-specific intelligence.
3. Investigation and analysis reports
4. Remediation activities and solutions applied
5. All documentations must be available in the MDR plus Remediation Service Portal.

F. **Documentation and Training**

The Managed Detection and Response plus Remediation Service Provider must provide a complete documentation for every deliverable and at every end of each development stage and milestone. The procuring entity shall exclusively own all documents and shall reserve the right to reproduce at no additional cost.

The documentation must be written in English of durable construction with concise and high-quality presentation to include but not limited to the following:

- User Manuals / Technical / Reference Manuals
- System / Operation Manuals / Troubleshooting and Installation Guides
- System Design and Architecture
- As Built Documents

All documentation must be in hard and soft copies in Microsoft Word for Windows and PDF format.

The Managed Detection and Response plus Remediation Service Provider must provide the necessary comprehensive training program which shall cover the operation and maintenance of the Proposed Managed Detection and Response plus Remediation Service and Solutions for at least 10 participants.

VI. PAYMENT TERMS

The Approved Budget for the Contract (ABC) is one hundred sixty-five million pesos (Php165,000,000.00) for three (3) years and will be payable quarterly.

The payments shall be made under the following terms and condition:

Managed Detection and Response plus Remediation
Terms of Reference

The Managed Detection and Response plus Remediation Solution shall be paid quarterly and will only be processed once all Deliverables and completed reports have been submitted and will start upon issuance of Certificate of Acceptance.

Deliverables	No. of Weeks	Completion Time
Detailed Work Plan	2	2 weeks after the release of the Notice to Proceed (NTP)
Delivery, installation and configuration of Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments and other tools required for the setup including connection of all data sources	4	Within 4 weeks after Approval of the Detailed Work Plan
Identification and Creation of Use Cases	4	Within 4 weeks after implementation of Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments and other tools.
Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments Process Documentation	4	Within 4 weeks after approval of Identification and Creation of Use Cases
MDR plus Remediation with Vulnerability & Compromise Assessment Report Monitoring		
Weekly Report		Weekly reporting of all MDR plus Remediation related security activities of the previous week submitted every Tuesday of the following week.
Monthly Report		Previous month Reports should be submitted within every first week of the succeeding month.
Quarterly Report		Previous quarter Reports should be submitted within every first week of the succeeding quarter.

Issuance of Certificate of Acceptance will be upon completion / submission of the requirements and conditions stated in the deliverables.

All payments are subject to applicable withholding taxes.

VII. SERVICE LEVEL AGREEMENT (SLA).

The Service Provider is required to provide the following modes of Support/SLA as necessary; the on-site Engineer or Online Support must be readily available and may include telephone calls, messaging, and/or email.

Severity	Acknowledgement	Target Initial Response
Severity 1 (critical – Incident causes a complete loss of service or a major security breach that significantly impacts operations or data)	15 minutes	Within 30 minutes

Severity 2 (high – Incident results in significant service degradation or a major security threat with potential impact but does not halt operations)	15 minutes	Within 2 local business hours
Severity 3 (medium – Incident causes moderate impact, with limited service disruption or a non-critical security vulnerability.)	15 minutes	Within 4 local business hours
Severity 4 (low – Incident causes minimal impact, with a minor service disruption or a low-risk security concern)	15 minutes	Within 1 local business day

The solutions provider/principal must also define an Escalation Matrix based on above SLA including assigned personnel.

VIII.PERFORMANCE SECURITY

The Service Provider is required to submit a performance security in any of the following forms and percentages:

Form of Performance Security	**Minimum % of the Total Contract Price**
Cash, cashier's/ manager's check issued by a Universal or Commercial Bank	Five percent (5%)
Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a Foreign Bank.	
Surety Bond callable upon demand issued by a surety or insurance company together with certificate issued by Insurance Commission certifying the surety or insurance company is authorized to issue such surety bond.	Thirty percent (30%)

Performance Security will correspond to the agreed total contract price and shall be effective and in full force and effect until the duration of the contract.

The Performance Security shall be denominated in Philippine Pesos and in favor of DBP and shall be forfeited (forfeit cash or call on the bond/guarantee if surety bond or Bank guarantee) in the event it is established that the Service Provider is in default in any of its obligations under the contract.

The Performance Security shall remain valid and effective until issuance by the DBP of the Final Certificate of Acceptance. A retention money or special bank guarantee equivalent to five percent (5%) of the Total Contract Price shall be submitted by the Service Provider within five (5) working days after issuance of Notice to Proceed to cover the three-year's warranty for the support and maintenance on Managed Detection and Response plus Remediation Solution.

The full amount shall be released provided that DBP has not filed any claims against the Service Provider and that all conditions stipulated in the contract have been fully met.

The Service Provider shall extend the validity of the Performance Security in the event of extension of the contract.

IX. BIDDING REQUIREMENTS

Documents required for the Bid Opening:

1. Statement of completed contract of a similar nature within the past five (5) years, from the date of submission and receipt of bids, either a single contract similar to the project equivalent to at least 50% of the ABC, or at least two (2) similar contract, the sum of which must at least be equivalent to 50% of the ABC, provided the largest of these similar contracts must be at least 25% of the ABC. A similar contract refers to any Cybersecurity Managed Services solution includes the delivery, subscription, installation, and/or maintenance and support.

2. The solutions provider must be an authorized partner/reseller of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.

3. Accomplished Annex A: Summary of Technical Compliance for the proposed solution, ensuring it is cross-referenced with all of DBP's terms of reference, duly signed by the bidder's authorized representative

4. The solutions provider/principal must comply with the following industry certifications and standards at a minimum:

    - ISO 27001 (Information Security Management Systems)
    - ISO 27014 (Governance and Information Security)
    - ISO 27034 (Application Security).
    - System and Organization Controls (SOC) 2
    - System and Organization Controls (SOC) 3
    - Payment Card Industry Data Security Standard (PCI DSS).

5. Certification from the solutions provider indicating that the solutions offered can be integrated with on premise McAfee SIEM.

6. Requirements for the following personnel:
    - Local/global Support Engineers (at least two)
        - Certificate of employment indicating full-time employee.
        - Certification (at least one per Engineer) indicating Cybersecurity Support Engineer
    - Onsite Support Engineer (at least one)
        - Certificate of employment indicating that the personnel is a full-time employee.
        - Curriculum Vitae were indicated that the personnel have 2 years' work experience as an IT Security Support Engineer.
        - Certification on MDR Solution being offered
        - Training Certificate (at least 2) on IT Security Fundamentals
    - Data Privacy Officer (at least two)
        - Certificate of employment indicating full-time employee
        - DPO Certification by an accredited provider.
    - Technical Account Manager (at least one)

- Certification of employment from the solutions provider/principal indicating full-time employee
- Curriculum Vitae were indicated experience (at least 2 years) as Technical Account Manager

- Project Manager
  - Certificate of Employment for the assigned personnel indicating the date of hire.
  - Resume or Curriculum Vitae indicating the personnel assigned have at least three (3) years' experience in Project Management and have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date).
  - Certification for Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

X. NON-DISCLOSURE CONDITION

The winning Bidder shall strictly adhere to the confidentiality agreement with the Bank. Information about DBP and its operation in this document is considered proprietary and confidential and must be treated as such by the recipients of this Technical Specifications. In the same manner, the responses to the Technical Specification which shall be specified as confidential shall not be disclosed to any third party.

1. Each party agrees to hold and maintain confidential all materials and information which shall come into its possession or knowledge in connection with the project or its performance, and not to make use hereof other than for the purpose of this project.

2. After completion of the project, all materials, data, proprietary information and other related documents provided to the winning bidder, and which are hereby deemed owned by DBP shall be returned to DBP.

3. The winning bidder undertake that it shall make appropriate instructions to its employees who need to have access to such information and materials to satisfy and comply with its confidential obligation as set forth in this Section.

4. This confidentiality obligation shall survive even after the termination of the contract.

5. The winning bidder shall, likewise, oblige the provider to be bound by this confidentiality contract.

6. The winning bidder's breach of this confidentiality provision shall entitle DBP to legal and other equitable remedies including but not limited to the immediate cancellation of the contract and shall entitle DBP for claim for damages and injunctive relief under the circumstances. DBP may also elect to terminate further access by the winning bidder to any data and information.

7. A Non-Disclosure Agreement between DBP and the winning bidder will form part of the contract that outlines confidential material, knowledge, or information that both parties wish to share with one another for certain purposes but wish to restrict access for or by third parties.

Managed Detection and Response plus Remediation
Terms of Reference

XI. POST QUALIFICATION REQUIREMENTS

Present a demo of the proposed MDR+R within fifteen (14) calendar days after receipt of Notice of Lowest /Single Calculated Bid to validate compliance to the requirement specifications stated under Section III. Scope of Work. May provide the following documentation to support compliance:

a. Product documentation/manual
b. Actual use cases/white paper
c. Reports generated by the solution
d. Screenshots of the solution

XII. LIQUIDATED DAMAGES

In case the Service Provider is unable to comply with the terms and conditions of this Agreement or fails to satisfactorily deliver the Solution or part of the solution on time inclusive of the duly granted time extension, if any, DBP shall, without prejudice to its other remedies under this Agreement and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance.

Such amount shall be deducted from any money due such as stated in Performance Security Section IX, or which may become due to the Service Provider, or collected from any securities or warranties posted by the Service Provider, whichever is convenient to DBP.

In case the total sum of liquidated damages reaches ten percent (10%) of the total contract price, DBP may rescind or terminate the Agreement, without prejudice to other courses of action and remedies open to it.

XIII. Signing of the Contract

The necessary documents as per the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act (RA) No. 9184 are to be included as part of the Contract. It is assumed that the Service Provider has agreed to the stipulations outlined in this Technical Specifications document.

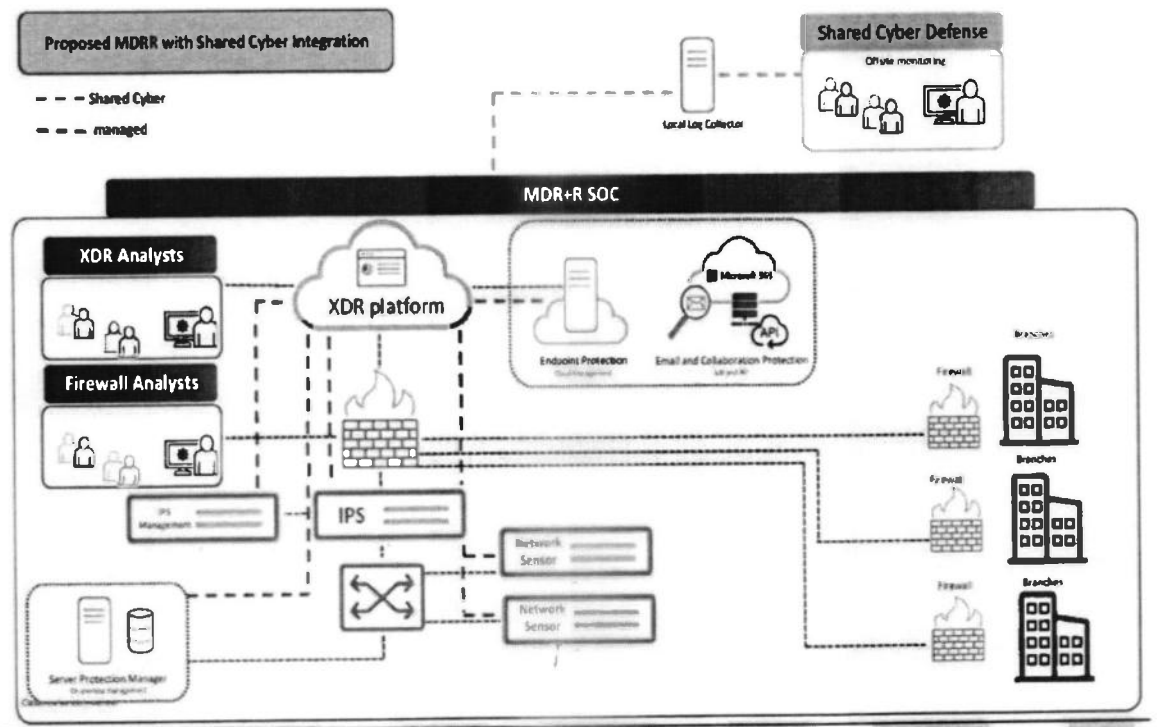
XIV. OGCC Review

The Contract shall be subject to the review of the Office of the Government Corporate Counsel.

Managed Detection and Response plus Remediation
Terms of Reference

Figure 1

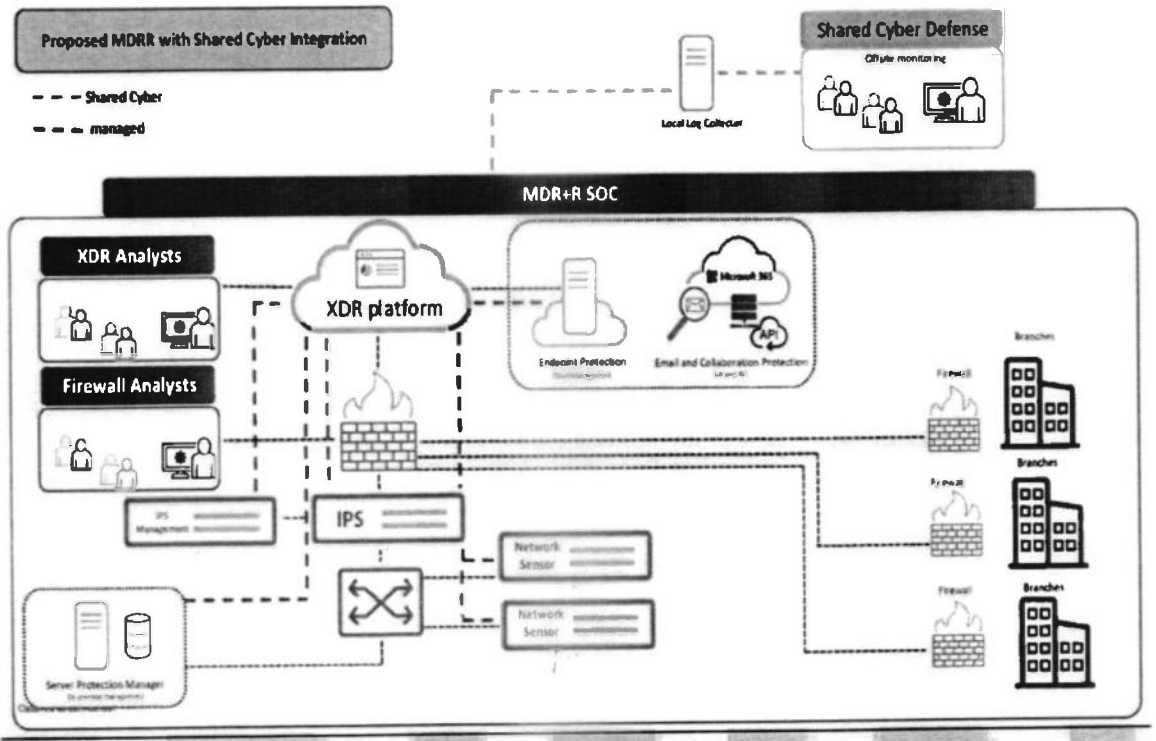
PROPOSED MDR+R CSOC NETWORK DIAGRAM



Managed Detection and Response plus Remediation
Terms of Reference

Figure 1

PROPOSED MDR+R CSOC NETWORK DIAGRAM



ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

TRANSMITTAL FORM

REVISED CHECKLIST OF REQUIREMENTS FOR BIDDERS

Note: Please fill-out this form and submit directly to the BAC Secretariat outside of the sealed envelopes.

FOR MACHINE STAMP (OFFICIAL TIME) BY THE DBP BAC SECRETARIAT
Received:

Name of Bidder: _____

Complete Address: _____

Submitted by: _____

Landline: _____ Email: _____

Item	FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)
LEGAL ELIGIBILITY DOCUMENTS	
TAB 1	If the bidder is a joint venture (JV): **a. If bidding as a formed JV:** Submit the existing valid, duly accomplished, signed and notarized JV Agreement (JVA). The JVA must specifically indicate among others, the following: the partner company that will represent the JV, the shareholdings of each partner company in the JV (to determine which partner company and its nationality has the controlling majority share), and the share of each partner company in the JV. Moreover, please likewise note: 1) If the JV is incorporated or registered with the relevant government agency, all documents listed in this checklist must be under the JV's name and shall submit the PhilGEPS Certificate of Registration under Platinum Category also under the JV's name. 2) If the JV is unincorporated, the PhilGEPS Certificate of Registration under Platinum Membership shall be submitted by each of the JV partners, while submission of the technical and financial eligibility documents (Tab 4 onwards) by any one of the JV partners constitutes collective compliance. **b. If bidding as a JV that is yet to be formed: Submit duly notarized Agreement to Enter into Joint Venture (*Template per FORM 1*).** Please likewise note: PhilGEPS Certificate of Registration under Platinum Membership shall be submitted by each of the JV partners, while submission of the technical and financial documents (Tab 4 onwards) by any one of the JV partners constitutes collective compliance.

Item	FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)
	Please refer to ***FORM 1-A*** and ***FORM 1-B*** for the sample Secretary's Certificate for each of the JV Partners. *Each JV partner must submit its duly notarized Special Power of Attorney or Secretary's Certificate, whichever is applicable, indicating therein the following:* *1. The designated/authorized representative who will sign the Joint Venture Agreement (JVA) or the Protocol to Enter into a JVA;* *2. That they are duly authorized to participate in the bidding as a JV;* *3. The authorized Lead Company to represent the JV;* *4. The person designated as the duly authorized representative of the corporation to the JV, sign the bid proposals/bidding documents, and sign the ensuing contract with DBP.* In case a JV partner is a sole proprietorship and the principal/proprietor opts to designate a representative, FORM 2-A shall be customized to include provisions such as the authority to sign the Protocol/Undertaking to enter a JVA.
TAB 2	Proof of appointment/authority of bidder's representative: a. **Duly notarized Special Power of Attorney** (if the bidder is a sole proprietorship and opts to designate a representative) - ***Template per FORM 2-A*** OR b. **Duly notarized Secretary's Certificate** (if the bidder is a corporation, partnership, cooperative, or joint venture) - ***Template per FORM 2-B*** **In case there are more than one appointed/designated representatives, bidders must tick ONE of the checkboxes provided in the form to identify if acting ANY ONE OF THE SIGNATORIES, ALL OF THE SIGNATORIES, or ANY (NUMBER) OF THE SIGNATORIES.** **FAILURE TO TICK A CHECKBOX SHALL MEAN THAT ALL AUTHORIZED REPRESENTATIVES ARE SIGNING THE BIDDING FORMS.**
TAB 3	Valid and current Certificate of PhilGEPS Registration (Platinum Membership), in three (3) pages, including Annex "A" or the List of Class "A" Eligibility Documents required to be uploaded and maintained current and updated in PhilGEPS in accordance with section 8.5.2. of the IRR of RA 9184. **Only the current/updated Certificate of PhilGEPS Registration (Platinum Membership) shall be accepted during the opening of bids. Expired Certificate or any of the eligibility documents listed in Annex "A" shall be a ground for failure of the bidder.**
The following are the related provisions/requirements based on GPPB Resolution 15-2021 dated 14 October 2021 regarding submission of valid/current PhilGEPS Certificate of Registration (Platinum Membership): - ***LIFT the suspension on the implementation of mandatory submission of the PhilGEPS Certificate of Registration (Platinum Membership) in Competitive Bidding and Limited Source Bidding, thus, fully enforcing Sections 8.5.2 and 54.6 of the 2016 revised IRR of RA No. 9184 starting 01 January 2022;***	

<table>
<tr><th>Item</th><th>FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)</th></tr>
<tr><td colspan="2">- AMEND Sections 23.1(a)(ii) and 24.1(a)(ii) of the 2016 revised IRR of RA No. 9184 to reflect that the submission of the recently expired Mayor's Permit together with the official receipt as proof that the prospective bidder has applied for renewal within the period prescribed by the concerned local government unit shall be accepted by the PhilGEPS for the purpose of updating the PhilGEPS Certificate of Registration (Platinum Membership) in accordance with Section 8.5.2 of the 2016 revised IRR of RA 9184.</td></tr>
<tr><td colspan="2">TECHNICAL ELIGIBILITY DOCUMENTS</td></tr>
<tr><td>TAB 4</td><td>Statement by the bidder of ALL its ongoing government and/or private contracts (including those awarded but not yet started, if any), whether similar or not similar in nature and complexity to the contract to be bid (include all contracts with the DBP for the said period, if any (Template per FORM 3), duly signed by the bidder's authorized representative.

Note: For bidders who have no ongoing government and/or private contracts, kindly indicate in their statement "NONE" to comply with the requirement. Bidders will be rated "failed" if no document is submitted or if the document submitted is incomplete or patently insufficient (per GPPB NPM 094-2013 dtd. 2013-12-19).

Copies of the NOA, contract, NTP, or equivalent document for each ongoing contract listed in the statement shall be required to be submitted as part of post-qualification of the bidder declared as the Lowest or Single Calculated Bid.</td></tr>
<tr><td>TAB 5</td><td>Statement of single largest completed contract of similar nature (government or private contract) within the last five (5) years (Template per FORM 4), duly signed by the bidder's authorized representative, with the following options:

<table>
<tr><th>Options</th><th>SLCC Requirement</th></tr>
<tr><td>1</td><td>Single contract equivalent to at least fifty percent (50%) of the ABC for one year; OR</td></tr>
<tr><td>2</td><td>At least two (2) similar contracts, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for one year.</td></tr>
</table>

A contract similar to the project refers to any Cybersecurity Managed Services solutions which includes the delivery, subscription, installation, and/or maintenance and support.

The identified/listed single largest or at least two completed contract must be supported by the following:

a) Notice of Award (NOA), OR Notice to Proceed (NTP), OR Contract, OR Purchase Order (PO)

AND

b) Either one of the following documents:
• Copy of Certificate of Completion or Certificate of Acceptance or Certificate of Satisfactory Performance issued by the bidder's client or copy of Official Receipt/s or Sales Invoice/s issued by the bidder to the client (ORs/SIs must sum up to the full amount of total contract price of completed project).</td></tr>
</table>

<table>
<tr><th>Item</th><th>FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)</th></tr>
<tr><td colspan="2">FINANCIAL ELIGIBILITY DOCUMENTS</td></tr>
<tr><td>TAB 6</td><td>Completely accomplished computation of Net Financial Contracting Capacity (NFCC) which must be at least equal to the ABC (Template per FORM 5), duly signed by the bidder's authorized representative.

1) The values of the bidder's current assets and current liabilities shall be based on the AFS for CY 2024.
2) The value of the NFCC must at least be equal to the ABC of this project.

<u>In case of Joint Venture, the partner responsible to submit the NFCC shall likewise submit the Statement of All its Ongoing Contracts and the latest Audited Financial Statements.</u>

If the prospective bidder opts to submit a committed Line of Credit, it must be at least equal to ten percent (10%) of the ABC to be bid. If issued by a foreign universal or commercial bank, it shall be confirmed or authenticated by a local universal or commercial bank.</td></tr>
<tr><td colspan="2">TECHNICAL COMPONENT</td></tr>
<tr><td>TAB 7</td><td>Original Bid Security issued in favor of the Development Bank of the Philippines (must be valid for at least 120 calendar days from the date of bid opening); <u>either one</u> of the following is acceptable:

a. Cashier's/manager's check issued by a Universal or Commercial Bank (at least 2% of the ABC).
b. Bank draft/guarantee or irrevocable letter of credit issued by a Universal bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank (at least 2% of the ABC).
c. Surety bond, callable upon demand, issued by a surety or insurance company (at least 5% of the ABC) and <u>a copy of certificate issued by the Insurance Commission certifying that the surety or insurance company is authorized to issue a surety bond.</u>
d. Duly <u>notarized</u> Bid Securing Declaration (Template per FORM 6) duly signed by the bidder's authorized representative.

<table>
<tr><th>Approved Budget for the Contract (ABC)</th><th>Cashier's/manager's check, Bank draft/guarantee or irrevocable letter of credit (2% of ABC)</th><th>Surety Bond (5% of ABC)</th><th>Bid Securing Declaration</th></tr>
<tr><td>165,000,000.00</td><td>3,300,000.00</td><td>8,250,000.00</td><td>No required percentage</td></tr>
</table>
The Bid Securing Declaration mentioned above is an undertaking which states, among others, that the bidder shall enter into contract with the Procuring Entity and furnish the performance security required under ITB Clause 31, within ten (10) calendar days from receipt of the Notice of Award, and commits to pay the corresponding amount as fine, and be suspended for a period of time from being qualified to participate in any government procurement activity in the event it violates any of the conditions stated therein as provided in the guidelines issued by the GPPB.</td></tr>
<tr><td>TAB 8</td><td>Accomplished Omnibus Sworn Statement (with ten [10] statements) (Template per FORM 7), duly signed by the bidder's authorized representative and notarized.</td></tr>
</table>

Item	FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)
TAB 9	Accomplished Data Privacy Consent Form ***per FORM 8,*** **duly signed by the bidder's authorized representative.**
TAB 10	Accomplished ***Certificate of Conformance to the Revised Terms of Reference*** **per** ***REVISED FORM 9 (attached in the Supplemental Bid Bulletin No. 1 dated 28 August 2025),*** **duly signed by the bidder's authorized representative.** The complete ***REVISED Terms of Reference and specifications*** are also attached as ***REVISED FORM 9-A (attached in the Supplemental Bid Bulletin No. 1 dated 28 August 2025),*** for reference.
TAB 11	Accomplished Summary of Technical Compliance **per** ***Annex A of FORM 9-A*** for the proposed solution, ensuring it is cross-referenced with all of DBP's Terms of Reference, **duly signed by the bidder's authorized representative**
TAB 12	Certificate issued by the manufacturer/principal stating that the bidder is an authorized partner/reseller of the solutions being offered (up to 2nd tier). The certificate must clearly indicate the bidder's authority to distribute, implement, and support the solution products and services being offered.
TAB 13	Certificate issued in the name the bidder/principal for each of the following: i. ISO 27001 (Information Security Management Systems) ii. ISO 27014 (Governance and Information Security) iii. ISO 27034 (Application Security) iv. System and Organization Controls (SOC) 2 v. System and Organization Controls (SOC) 3 vi. Payment Card Industry Data Security Standard (PCI DSS)
TAB 14	Certification from the solutions provider indicating that the solutions being offered can be integrated with on premise McAfee SIEM.
TAB 15	Documents for each of the local/global Support Engineers (at least two personnel): 3. Certificate of employment indicating that the personnel is a full-time employee. 4. Certification (at least one per Engineer) indicating Cybersecurity Support Engineer.
TAB 16	Documents for the Onsite Support Engineer (at least one personnel): 5. Certificate of employment indicating that the personnel is a full-time employee. 6. Curriculum Vitae indicating that the personnel have 2 years of work experience as an IT Security Support Engineer. 7. Certification on MDR Solution being offered. 8. At least two (2) training Certificates on IT Security Fundamentals.

Item	FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)
TAB 17	Documents for each of the Data Privacy Officers (at least two personnel): 3. Certificate of employment indicating that the personnel is a full-time employee 4. DPO Certification by an accredited provider.
TAB 18	Documents for the Technical Account Manager (at least one personnel): 3. Certificate of employment from the solutions provider/principal indicating full-time employee. 4. Curriculum Vitae indicating at least 2 years of experience as Technical Account Manager.
TAB 19	Documents for the Project Manager: 4. Certificate of employment for the assigned personnel indicating the date of hire. 5. Resume or Curriculum Vitae indicating the personnel assigned have at least three (3) years' of experience in Project Management and have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippines banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date). 6. Certification for Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

Item	SECOND ENVELOPE: FINANCIAL PROPOSAL (DULY SEALED AND MARKED)
TAB 1	Duly accomplished Financial Proposal Form (***Template per FORM 10***), **duly signed by the bidder's authorized representative.** **Note: Bid shall not exceed the ABC of PhP 165,000,000.00 for 3 years or PhP 55,000,000.00 per year (inclusive of taxes.)**
TAB 2	Detailed Financial Proposal/Price Schedule duly signed by the bidder's authorized representative. Bidders shall use either **FORM 11-A** or **FORM 11-B** as template. **The total detailed bid must not exceed the ABC and must be consistent with the financial bid per TAB 1.**