



Bank deposit mo, protektado!

NOTICE TO PROCEED

February 22, 2024

MR. WILFREDO N. AGUILAR
Accounts Manager
TRENDS & TECHNOLOGIES, INC.
6th Floor Trafalgar Plaza,
105 H.V. Dela Costa Street,
Salcedo Village, Makati City

Dear Mr. Aguilar:

The attached Contract having been approved, notice is hereby given to TRENDS & TECHNOLOGIES, INC. that work may commence on the Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster effective upon receipt of this notice.

Upon receipt of this notice, you shall be responsible for performing the services under the terms and conditions of the Contract and in accordance with the Implementation Schedule.

Should you have questions regarding the implementation of the contract, please communicate directly with Mr. Renar M. Gonzales, Officer-in-Charge of the IT Group. You may contact him at telephone number 8841-4305.

Please acknowledge receipt and acceptance of this notice by signing in the space provided below and in the attached copy of this notice. Keep one copy and return the other to PDIC.

Very truly yours,

[Handwritten signature]
ROBERTO B. TAN
President & CEO

I acknowledge receipt of this Notice on FEB. 28, 2024
Name of the Representative of the Bidder: LEAH P. APOSTOL
Signature of Representative: [Handwritten signature]

CONTRACT
(Procurement of Shared Cyber Defense Solution for the Insurance Cluster)

This Contract (hereinafter referred to as the "**Contract**") is made and entered into on this **FEB 20 2024** day of _____, 2024 at **MAKATI CITY**, by and between:

PHILIPPINE DEPOSIT INSURANCE CORPORATION (PDIC), a government instrumentality created and existing by virtue of Republic Act No. 3591, as amended, with principal office address at SSS Bldg., 6782 Ayala Avenue cor. Rufino St., Makati City, Metro Manila, hereinafter referred to as the "**PROCURING ENTITY**", represented herein by its President & CEO, **Mr. ROBERTO B. TAN**, duly authorized for the purpose of this Contract as evidenced by Board Resolution No. 2021-10-132, attached as **Annex "A"**

- and -

TRENDS AND TECHNOLOGIES, INC. (TTI), a corporation duly organized and existing by virtue of the laws of the Philippines, with principal office address at 6th Floor Trafalgar Plaza, 105 H.V. Dela Costa Street, Salcedo Village, Makati City, hereinafter referred as the **SUPPLIER**, duly represented herein by its Account Manager, **Mr. WILFREDO N. AGUILAR**, duly authorized for the purpose of this Contract as evidenced by Board Resolution No. 09-06-2023, attached as **Annex "B"**

The **PROCURING ENTITY** and the **SUPPLIER** shall be collectively referred to as the "**PARTIES**".

ANTECEDENTS:

The Secretary of Finance directed the members of the Insurance Cluster composed of the Bureau of the Treasury (BTR), Government Service Insurance System (GSIS), Social Security System (SSS), Insurance Commission (IC), Philippine Deposit Insurance Corporation (PDIC) to institutionalize a cost-effective defense strategy that will shield/protect their respective systems from potential cybersecurity threats along with other possible risks and data breaches in their respective digital landscape;

The members of the Insurance Cluster shared a common understanding that a shared defense strategy for cybersecurity will boost the resiliency against cyberattacks of each institution and the cluster as a whole, hence, the need to provide additional layer of protection to the information technology systems of the members of the Insurance Cluster through the implementation of Shared Cyber Defense Solution for the members of the Insurance Cluster (the "Project").

The Project aims to:

- establish a standard cybersecurity implementation, based on best practice;
- improve resilience against cyberattacks by being able to promptly detect, prevent and respond to any threats and attacks;
- share interagency threat intel and information; and
- profile and monitor the threat landscape the cluster is operating on.

(For more detailed requirements and description of the Project, refer to the Terms of Reference/Technical Specifications.)

To hasten implementation of the Project, and to ensure the procurement of a single solution for all the members of the Insurance Cluster, the members of the Insurance Cluster designated Land Bank Philippines (LANDBANK) to undertake the necessary procurement of the Project pursuant to Section 7.3.3 of the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act (R.A) No. 9184¹;

On 13 October 2023, a public bidding was conducted by LANDBANK for the Project pursuant to the provisions of R.A No. 9184 and its RIRR;

In the said public bidding, and after due evaluation and conduct of post-qualification, the **SUPPLIER's** bid in the amount of **PESOS: Twenty Three Million Six Hundred Eighty One Thousand Two Hundred Eighty and 00/100 (PhP23,681,280.00), Philippine currency**, for 1,200 endpoints was found to be the Lowest Calculated and Responsive Bid, and offered the most advantageous terms and conditions to the **PROCURING ENTITY**;

The procurement of PDIC's allotment in the Project was included in the 2023 PDIC Corporate Operating Budget pursuant to Board Resolution Nos. 2022-04-048 and 2022-11-156 dated 28 April 2022 and 24 November 2022, and the fund for the approved budget has been allotted, set aside, and made available for the said services, as evidenced by a Certification for Budget and Fund Availability, which is attached as **Annex "C"** of this Contract;

NOW, THEREFORE, for and in consideration of the foregoing premises and of the mutual covenants and stipulations hereinafter set forth, the parties hereto have agreed and do hereby agree, as follows:

1

In order to hasten project implementation, Procuring Entities which may not have the proficiency or capability to undertake a particular procurement, as determined by the HoPE concerned, may outsource the procurement tasks by:

(a) Requesting other GoP agencies to undertake such procurement for them, through the execution of a memorandum of agreement containing specific arrangements, stipulations and covenants, in accordance with government budgeting, accounting and auditing.

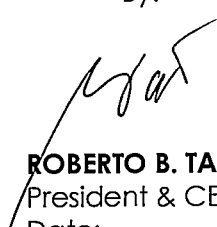


1. **Definitions** - In this Contract, words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to below;
2. **Documents Incorporated** - The following documents as required by the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of the Contract, viz:
 - Philippine Bidding Documents (PBDs);
 - Schedule of Requirements (Annex D);
 - Technical Specifications (Annex E);
 - General and Special Conditions of the Contract (Annexes F1, F2 & F3); and
 - Supplemental or Bid Bulletins (Annexes G1&G2), if any.
 - The winning bidder's bid, including the Eligibility requirements, Technical and Financial Proposals, and all other documents or statements submitted (Annexes H1&H2);
 - *Other Bid documents, including all the documents/statements contained in the Bidder's bidding envelopes, as annexes, and all other documents submitted (e.g., Bidder's response to request for clarifications on the bid), as well as corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;*
 - Performance Security (Annex I);
 - Notice of Award of Contract and the Bidder's *conforme* thereto (Annex J); and
 - Other contract documents that may be required by existing laws and/or the PE concerned in the PBDs. Winning bidder agrees that additional contract documents or information prescribed by the GPPB that are subsequently required for execution or submission after the contract execution, such as the Notice to Proceed, Variation Orders, and Warranty Security, shall likewise form part of the Contract.
3. In consideration of the payments to be made by the **PROCURING ENTITY** to the **SUPPLIER** in the amount of **PESOS: Twenty Three Million Six Hundred Eighty One Thousand Two Hundred Eighty and 00/100 (Php23,681,280.00)**, Philippine currency, the **SUPPLIER** hereby covenants with the **PROCURING ENTITY** to supply, deliver, install, and configure the Project, and to remedy defects therein in accordance with its Bid; and
4. The **PROCURING ENTITY** hereby covenants to pay the **SUPPLIER** in consideration of the supply, delivery, installation, and configuration of the Project and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract in accordance with the terms of the Bidding.



IN WITNESS WHEREOF, the PARTIES have hereunto affixed their signatures on the date and place as stated below their respective signatures.

**PHILIPPINE DEPOSIT
INSURANCE CORPORATION
PROCURING ENTITY**

By:



ROBERTO B. TAN
President & CEO
Date: _____
Place: _____


**TRENDS AND TECHNOLOGIES, INC.
SUPPLIER**

By:


WILFREDO N. AGUILAR
Account Manager
Date: _____
Place: _____

SIGNED IN THE PRESENCE OF:


RENAR M. GONZALES
Officer-in-Charge, IT Group


MARY ROSE S. HERNANDEZ
Sales Manager

ACKNOWLEDGEMENT

REPUBLIC OF THE PHILIPPINES)
MAKATI CITY) S.S

MAKATI CITY

BEFORE ME, a Notary Public, for and in the City of Makati on this FEB 20 2024 of _____, 2024, appeared personally the following:

<u>Name</u>	<u>Government ID Nos.</u>	<u>Date/Place Issued</u>
PHILIPPINE DEPOSIT INSURANCE CORPORATION Represented by: Roberto B. Tan President & CEO		
TRENDS AND TECHNOLOGIES, INC. Represented by: WILFREDO N. AGUILAR Account Manager	PASSPORT NO. P39572688	25 NOV 2019 DFA NCR SOUTH

Known to me and to me known to be the same persons who executed the foregoing instrument and they acknowledged to me that the same is their free and voluntary act and deed as well as the entities they represent, and that they are duly authorized to sign the same.

This instrument refers to a *CONTRACT (Procurement of Shared Cyber Defense Solution for the Insurance Cluster)* consisting of _____ (___) pages, including this page where the acknowledgment is written, signed on each and every page hereof by the parties and their instrumental witnesses and thereafter sealed with my notarial seal.

WITNESS MY HAND AND SEAL on the date and place first above-written.

Doc. No. 121 ;
Page No. 26 ;
Book No. 12 ;
Series of 2024.

ATTY. JOEL PERRER FLORES
Notary Public
Notary Public for Makati City
Until December 31, 2024
Appointment No. M-115 (2023-2024)
Roll Of Attorneys No. 77376
MCLE Compliance VHR No. 0001393-
Jan. 3, 2023 until Apr. 12, 2028
PTR NO. 10073945/ Jan. 2, 2024/ Makati City
IBP No. 330740/ Jan. 2, 2024/ Pasig City
1107 Bataan St., Guadalupe Nuevo, Makati City

Republic of the Philippines



Government Procurement Policy Board



Bank deposit mo, protektado!

CERTIFICATE OF ADOPTION OF RESOLUTION

I, PAMELA ANGELI M. SOLIS-TY, Corporate Secretary of the Philippine Deposit Insurance Corporation, do hereby certify that the following is an excerpt of the Minutes of the Regular Meeting of the Board of Directors of the Corporation held on October 13, 2021:

"After due deliberation and upon motion duly made and seconded, the following resolution was passed and unanimously carried:

RESOLUTION NO. 2021-10-132

RESOLVED, as it is hereby resolved, to grant authority to the President to represent and sign for the Corporation the Memorandum of Agreement Designating Land Bank of the Philippines (LANDBANK) as the Procurement Agent for the Procurement of the Shared Cyber Defense Solution (Annex A of the Board memo), including other pertinent documents necessary for the execution thereof."

Issued this 15th day of October 2021.

Pamela Angel M. Solis-Ty
PAMELA ANGELI M. SOLIS-TY
Corporate Secretary

Noted by:

[Signature]
ROBERTO B. TAN
President & CEO



[Handwritten mark]

Form No. 7

SECRETARY'S CERTIFICATE

I, FARAH CHRISTINE V. FARD, of legal age, Filipino, with office address at 6th Floor Trafalgar Plaza, 105 H.V. Dela Costa Street, Salcedo Village, Makati City, after being sworn to in accordance with law, do hereby certify that:

- 1. I am the incumbent and duly designated Corporate Secretary of Trends & Technologies, Inc., organized and existing in accordance with law, with principal office at the above-stated address;
- 2. As Corporate Secretary, I am the custodian of the corporate books and records, including the Minutes of Meetings and Resolutions of the Board of Directors;
- 3. The Board of Directors issued Board Resolution No. 09-06-2023 on September 14, 2023 to wit:

"RESOLVED, that Ms. Mary Rose S. Hernandez/Sales Manager or Mr. Wilfredo N. Aguilar/Account Manager or Ms. Gigi L. Velez/Sales Support Officer or Ms. Leah P. Apostol/Sales Assistant are our authorized signatories to represent our company, to sign and authenticate all the bidding documents for the **Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster with Project Identification Number LBP-HOBAC-ITB-GS-20230725-01** and to sign the resulting contract by affixing his/her signature thereon as required in the Instructions to Bidders and with full power and authority to do, execute and perform all acts necessary".

The above-cited authorization has not been amended, modified and/or superseded and is therefore still in full force and effect.

- 4. This Certification is being issued to attest to the truth of the foregoing.

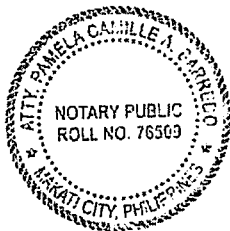
Signed this 05 OCT 2023 in Makati City, Philippines.



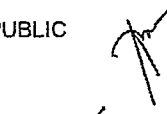
 FARAH CHRISTINE V. FARD
 Corporate Secretary

SUBSCRIBED AND SWORN to me before this _____ day of 05 OCT 2023 in Makati City, Philippines, with competent IDs represented.

Doc. No. 471
 Page No. 96
 Book No. II
 Series of 2023



NOTARY PUBLIC


 ATTY. PAMELA CAMILLE A. BARREDO
 Notary Public for and in the City of Makati
 Appointment No. M-041 (2021-2024)
 Until 31 December 2024
 Roll of Attorneys No. 76509, 5 May 2022
 PTR No. 8582131/12 January 2023/Makati City
 IBP No. 278885/0 January 2023/Passig City
 23/F Trafalgar Plaza Building
 105 H.V. Dela Costa St., Salcedo Village
 Makati City, Philippines 1227



CERTIFICATION FOR BUDGET AND FUND AVAILABILITY

This is to certify that the Project/Activity/Program (PAP) indicated below has been approved and the corresponding budget in the amount of **Twelve Million One Hundred Twenty Thousand Pesos (P12,120,000.00)** is included in the 2023 PDIC Corporate Operating Budget (COB) pursuant to Board Resolution Nos. 2022-04-048 and 2022-11-156 dated 28 April 2022 and 24 November 2022, respectively.

Responsibility Center	Budget Account	PAP	2023
ITG	Subscription Expenses	Shared Cyber Defense Solution	P 12,120,000.00


The aforesaid fund has been allotted, set aside and made available for the said PAP and shall not hereafter be made available for any other purpose.

CERTIFICATION OF BUDGET INCLUSION

This is to certify that the Project/Activity/Program (PAP) indicated below with a corresponding budget for 2024 in the amount of **Twelve Million Pesos (P12,000,000.00)** has been approved pursuant to Board Resolution No. 2022-11-156 dated 24 November 2022.

Responsibility Center	Budget Account	PAP	2024
ITG	Subscription Expenses	Shared Cyber Defense Solution	P 12,000,000.00

Issued this 15th day of December 2022, in Makati City.


EVANGELINE R. PANTALUNAN
Vice President
Comptrollership Group



**Section VI. Schedule of
Requirements**



Schedule of Requirements

The delivery schedule/contract period expressed as weeks/months/years stipulates hereafter a delivery/performance period which is the period within which to deliver the goods or perform the services in the project site/s.

Description	Quantity	Delivery Period
Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster		Phase 1 – one hundred twenty (120) working days from the issuance of Notice to Proceed;
1) Bureau of Treasury	1,600 endpoints	Phase 2 – ninety (90) working days from the issuance of Notice to Proceed.
2) Government Service Insurance System	4,400 endpoints	Commencement date will be from the receipt of Notice to Proceed by the winning bidder. The vendor must provide a project schedule, which should present the project milestones and deliverables at each milestone. License subscriptions will start upon contract implementation.
3) Social Security System	8,000 endpoints	
4) Philippine Deposit Insurance Corporation	1,200 endpoints	
Phase 1: <ul style="list-style-type: none"> ▪ Threat Intelligence ▪ Security Monitoring and Management ▪ Incident Response Phase 2: <ul style="list-style-type: none"> ▪ Vulnerability Management 		

Conforme:

TRENDS & TECHNOLOGIES INC.

Name of Bidder

WILFREDO M. AGUILAR

Signature over Printed Name of
Authorized Representative

ACCOUNT MANAGER AND AUTHORIZED REPRESENTATIVE


Position

Section VII. Technical Specifications



Technical Specifications

Specifications	Statement of Compliance								
<p>Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster</p> <table border="1" data-bbox="311 1276 837 1444"> <tr> <td>1. Bureau of Treasury</td> <td>1,600 endpoints</td> </tr> <tr> <td>2. Government Service Insurance System</td> <td>4,400 endpoints</td> </tr> <tr> <td>3. Social Security System</td> <td>8,000 endpoints</td> </tr> <tr> <td>4. Philippine Deposit Insurance Corporation</td> <td>1,200 endpoints</td> </tr> </table> <p>Phase 1.</p> <ul style="list-style-type: none"> ▪ Threat Intelligence ▪ Security Monitoring and Management ▪ Incident Response <p>Phase 2:</p> <ul style="list-style-type: none"> ▪ Vulnerability Management 	1. Bureau of Treasury	1,600 endpoints	2. Government Service Insurance System	4,400 endpoints	3. Social Security System	8,000 endpoints	4. Philippine Deposit Insurance Corporation	1,200 endpoints	<p>Statement of Compliance</p> <p>Bidders must state below either "Comply" or "Not Comply" against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered.</p> <p>Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false-either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.</p> <p>Please state here either "Comply" or "Not Comply"</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p> <p>- COMPLY</p>
1. Bureau of Treasury	1,600 endpoints								
2. Government Service Insurance System	4,400 endpoints								
3. Social Security System	8,000 endpoints								
4. Philippine Deposit Insurance Corporation	1,200 endpoints								


 WILFREDO N. AGUILAR
 ACCOUNT MANAGER
 TRENDS & TECHNOLOGIES, INC.

Notes:	
1. Technical specifications and other requirements per attached Terms of Reference (TOR) – revised Annexes D-1 to D-25.	COMPLY
2. The documentary requirements enumerated in Items 3.II.C and D of the TOR shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements.	COMPLY
Non-submission of the above requirements may result to post-disqualification of the bidder.	COMPLY

PLEASE SEE ATTACH DETAILED TOR RESPONSE

Conforme:

TRENDS & TECHNOLOGIES, INC.
Name of Bidder

WILFREDO N. AGUILAR
Signature over Printed Name of
Authorized Representative

ACCOUNT MANAGER & AUTHORIZED REPRESENTATIVE
Position



**SHARED CYBERDEFENSE SOLUTION
(REBIDDING)**

Terms of Reference (Insurance Cluster)

Version Number : 4.3
Date : 3 August 2023
Author : Government Service Insurance System
Bureau of the Treasury
Social Security System
Philippine Deposit Insurance Corporation



1. Name and Description of the Project

With the continued evolving nature of cybersecurity risks, the Secretary of Finance has mandated various agencies under the Department to establish a cost-effective defense strategy that will add a layer of defense for the agencies to shield their respective IT systems from potential cybersecurity threats, along with other possible risks and data breaches in the digital landscape.

For this Terms of Reference (TOR), it will cover the Insurance Cluster composed of the Bureau of the Treasury (BTr), Government Service Insurance System (GSIS), Social Security System (SSS), Philippine Deposit Insurance Corporation (PDIC).

2. Project Objective and Scope

The proposed Common Cyber Defense Solution shall require the vendor to provide a two (2) year subscription for the provision of Security Monitoring and Management, Vulnerability Management, Threat Intelligence, and Incident Response. This is primarily focused on the National Institute of Standards and Technology (NIST) Cybersecurity Framework – Identify, Protect, Detect, Respond and Recover.

The Approved Budget for the Contract (ABC) shall be the upper limit or ceiling for the proposal, and shall cover all project costs, including, but not limited to the following:

- Subscription cost that will be based on the number below:

Agency	Servers	Desktops/Laptops	Total
BTr	150	1450	1600
GSIS	400	4000	4400
SSS	200	7800	8000
PDIC	82	1118	1200

- The project shall include project management, consulting, requirements validation, customization, training, integration, training, production deployment, system integration, change management and other out-of-pocket expenses (e.g., transportation allowance, per diem, etc.);
- The Shared Defense subscription shall commence immediately after the Phase 1 implementation of the project.
- Post Go Live support starting from the implementation date; and
- All applicable taxes, service fees and charges (e.g., fund transfers fees, foreign exchange difference)

The proposed Common Cyber Defense Solution for the Insurance Cluster shall be procured in one lot which shall consist of sublots per agency. Likewise, this shall be the basis for awarding per agency.

The pricing shall be uniform for all agencies in the cluster.

Other Requirements

During procurement, the bidder is required to submit respective proposals for all the agencies concerned.

3. Functional and Non-Functional Requirements

The vendor shall respond to each requirement stated herein. Failure to conform to any of the specifications shall be sufficient grounds for disqualification.

I. Functional Requirements

A. Security Monitoring and Management		COMPLIED	REMARKS			
A.1 Security Operations Center (SOC)		Y/N				
1.	The service provider shall provide a cloud-based SOC for individual agencies with complete Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution that allows for two-way integration with the agencies data sources, capture of near real-time log data, and must perform correlation between data sources during investigation which shall also be accessible by the individual agencies.					
2.	The service provider shall set up a cluster level SOC dashboard to have an integrated and high level overview of the cluster agencies security posture.					
3.	The SOC, through the SIEM, shall detect and monitor threats, correlate with threat intelligence sources, generate alerts, conduct investigation, and escalate tickets to the agencies on a 24x7 basis, using the Security Operations Center (SOC) platform, inclusive of the security tools to be provisioned for the agencies.					
4.	There must be a proper onboarding and integration period between the service provider and the agencies prior to full SOC operation to ensure completeness of SOC visibility and familiarization with the agencies processes and network behavior.					
5.	The SOC solution shall have its own ticketing tool for incident ticket generation.					
6.	The SOC solution, through the SIEM, shall classify security events based on the following risk rating matrix containing the following information. The report method shall be thru call and/or e-mail:					
		Impact:				
	Response Time	High	Medium	Low	Very Low	Report Time
Priority	Within 2 hours	P1	P2	P2	P3	within 15 minutes
	Within 12 hours	P2	P2	P3	P4	within 30 minutes
	Within 24 hours	P2	P3	P3	P4	N/A
	24 hours	P3	P3	P4	P4	N/A
<ul style="list-style-type: none"> Impact: Severity of the security event to critical assets 						

<ul style="list-style-type: none"> • Priority: Based on the impact and severity • Nature of threat • Potential business impact • Remediation recommendations <p><i>*Response Time: How soon the security incident must be acknowledged by the service provider</i></p> <p><i>*Report Time: How soon a reference number/ problem ticket must be created by the service provider and received by the agency. The Report Time is included in the Response Time.</i></p>		
<p>7. Monthly monitoring service management:</p> <p>The service provider shall conduct regular meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement. Regular written reports must also be available to track the status of cases and the assistance needed. Monthly reports shall contain, but not limited to:</p> <ul style="list-style-type: none"> • SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Overtime • Correlated Events and Rules Triggered Summary • Summary of Incident Ticket per Use Cases Incident Management 		
<p>8. The service provider shall ensure flexibility and scalability of the agencies SOC platform and shall ingest and process all events sent by the agencies for the SIEM and SOAR requirements including its current and future needs.</p>		
<p>9. The service provider shall facilitate SOC security briefing at least once a month for the agencies to present the latest local and international news and updates in Cyber security.</p>		
<p>A.2 Managed Detection and Response</p>	<p>COMPLIED</p>	<p>REMARKS</p>
<p>A.2.1 Deployment and Management</p>	<p>Y/N</p>	
<p>1. The service provider shall supply Managed Detection and Response services, including the Endpoint Protection / Endpoint Detection and Response (EDR) licenses required for supported endpoints. Supported endpoints refer to Windows endpoints, Windows servers, major Unix and Linux distributions, MacOS, Mobile devices, that is still under support or extended support by the manufacturer.</p>		
<p>2. The solutions provider must be capable to deploy the endpoint technology to workstations and servers, including Windows, Mac, Unix and Linux assets, using the agencies or the solutions providers deployment tool, and must support both physical and virtual environments.</p>		
<p>3. For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided.</p>		

4. The solution shall detect and prevent attacks on-premise, for supported and unsupported endpoints, including agency deployments in public clouds, if any, such as, but not limited to Amazon Web Services (AWS), Azure, Oracle Cloud and Google Cloud.		
5. The solution shall be capable to block malicious indicators of compromise (IOCs) and behaviors of compromise (BOCs) automatically with expert review of detections by analysts to ensure there is always human oversight on technology.		
6. The solution shall allow custom enforcement policies to neutralize sophisticated malware and lateral movement utilizing "living off the land" techniques that can potentially evade standard detections, however, ensuring that these custom policies does not impede business operations.		
7. Update of Indicators of Compromise (IOC) and watchlist repository, whenever applicable		

A.2.2 Prevention and Detection	COMPLIED Y/N	REMARKS
1. The solution shall have integration with the SIEM for central monitoring and analysis, including the setup of relevant dashboards such as but not limited to, attacks, threats, endpoints at risk.		
2. The solution should utilize signature-based and/or signature-less detection techniques to protect against known and unknown attacks.		
3. The solution should have Machine Learning and Behavioral Pattern Indicator of Attack (IOA) detection capability.		
4. The solution must be able to detect and prevent the following: <ul style="list-style-type: none"> • exploitation behavior using IOAs and no signatures. • ransomware behavior using Behavior IOA patterns and no signatures. • file-less malware using Behavior IOA patterns. • malware-free tradecraft using Behavior IOA patterns. • BIOS level attacks • Privilege Escalation • Exfiltration • Connection to malicious command and control destinations 		
5. The solution must be able to enrich a detected event with its own threat intelligence and not any third-party Intelligence including mapping of the technique, tactic and procedure (TTP) against the MITRE ATT&ACK framework.		
A.2.3 Threat Hunting and Response	COMPLIED Y/N	REMARKS
1. The service provider must provide 24x7 Managed Threat Hunting Service, supported by experienced and certified analysts or incident responders for the remote response on endpoint incidents/events		

2. The service provider must have pre-built threat hunting applications and queries		
3. The service provider must be able to get context from indicators such as IP's, URL's, domains, or hashes using the tools within the platform, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others)		
4. The solution shall be able to isolate "at-risk" endpoints, including the blocking the launching of suspicious or malicious applications.		
5. The solution shall allow blacklisting and whitelisting of hashes manually through the solution.		
6. The solution shall provide remote response by administrators, analysts, or incident responders such as containment, deleting files, killing process among others without the need for additional tools or agents.		
7. The solution shall provide root cause analysis of all identified malicious activity.		
A.3 Security Information and Event Management (SIEM)	COMPLIED Y/N	REMARKS
1. The solution shall provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a time period. The agencies must be able to request customized dashboards and ad-hoc reports from the service provider.		
2. The solution shall be capable to support collection of different types of metadata (e.g., logs, security events, network flows, among others) from data sources and shall include log compression and industry standard encryption at rest and in transit to ensure security of captured data from disclosure to disinterested parties.		
3. The data sources ingested by the solution shall include at least the events from perimeter security tools, active directory logs, endpoint protection, and endpoint detection and response tools, including events from sensors that may be deployed by the solutions provider, if needed.		

<p>4. The maximum aggregate daily data ingestion shall be as follows:</p> <table border="1" data-bbox="169 456 1114 714"> <thead> <tr> <th data-bbox="169 456 403 506">Agency</th> <th data-bbox="403 456 1114 506">Daily Event Log Aggregate Size in Gigabytes (GB)</th> </tr> </thead> <tbody> <tr> <td data-bbox="169 506 403 555">BTr</td> <td data-bbox="403 506 1114 555">17 GB</td> </tr> <tr> <td data-bbox="169 555 403 604">GSIS</td> <td data-bbox="403 555 1114 604">24 GB</td> </tr> <tr> <td data-bbox="169 604 403 654">SSS</td> <td data-bbox="403 604 1114 654">48 GB</td> </tr> <tr> <td data-bbox="169 654 403 714">PDIC</td> <td data-bbox="403 654 1114 714">15 GB</td> </tr> </tbody> </table>	Agency	Daily Event Log Aggregate Size in Gigabytes (GB)	BTr	17 GB	GSIS	24 GB	SSS	48 GB	PDIC	15 GB		
Agency	Daily Event Log Aggregate Size in Gigabytes (GB)											
BTr	17 GB											
GSIS	24 GB											
SSS	48 GB											
PDIC	15 GB											
<p>5. The service shall have content packs that are prebuilt configurations for common security use cases that provide sets of rules, alarms, baselines, views, reports, variables, and watchlists.</p>												
<p>6. The service shall provide advanced security capabilities, such as User and Entity Behavioral Analytics (UEBA), natively within its own platform.</p>												
<p>7. The solution must integrate with the global threat intelligence subscription service for data enrichment to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.</p>												
<p>8. The solution must be able to generate and send actionable items to the automation and orchestration tool as well as generate and send alerts to both service provider and agency analysts and incident responders.</p>												
<p>9. The service provider shall ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidences of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required.</p> <p>The logs beyond the retention period shall be archived and given monthly to the agencies in an agreed format.</p>												
<p>10. The service provider shall ensure that the data ingested from the insurance cluster is not shared or disclosed to or accessed by parties not mentioned in the contract unless explicitly granted permission by the cluster.</p>												
<p>A.4 Security Orchestration, Automation and Response (SOAR)</p>	<p>COMPLIED Y/N</p>	<p>REMARKS</p>										
<p>1. The solution must be able to integrate with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass</p>												
<p>2. The solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting</p>												
<p>3. The solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner</p>												

4. The solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization		
5. The solution must be an open architecture that allows for easy connectivity and integrations to any existing system, bringing them all together into a single, contextual language. Integration with other solutions can either be out of the box or customized.		
6. The solution must be able to accelerate security incident processes by automating or semi automating workflows		
7. The solution must be include out of the box or customizable playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. Playbooks deployed shall include at least: <ul style="list-style-type: none"> • Phishing enrichment and response • Malware endpoint response • Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc) • Unusual browsing activity • Web attack profiling and blacklisting 		
8. The solution should provide pre-set and customizable KPI metrics to monitor threat response efficacy and team performance.		

B. Vulnerability Management and Penetration Testing		
B.1 Vulnerability Management	COMPLETED Y/N	REMARKS
1. The solution provided must be a cloud based service, integrated within the SIEM, that shall give immediate global visibility into where the Agency IT system might be vulnerable to the latest Internet threats and how to protect them.		
2. It should be able to continuously identify threats and monitor unexpected changes in the network before they turn into breaches. The solution can be agentless or agent-based if continuous monitoring is required on specific systems.		
3. The solution should be able to scan systems anywhere in the Agency environment, from the same console: whether the asset is on the perimeter, the internal network, or cloud environments (such as Amazon Web Services, Oracle Cloud, Microsoft Azure or Google Cloud) with the ability to create custom reports showing each audience just the level of detail it needs to see.		
4. The solution should be able to identify and prioritize critical vulnerabilities and risks to enable the agencies to prioritize the remediation of the highest business risks using trend analysis, zero-day and patch impact predictions.		
5. The solution should be able to track vulnerability data across hosts and time, to give a better understanding of the agencies security posture. The reports can be changed through existing pre-built templates, without the need to rescan. The reports can be generated on demand or		

scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV														
6. The solution should be able to automatically gather and analyze security and compliance data in a scalable backend, with provisioning additional capabilities as easy as checking a box.														
7. The solution should be able to proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify the agencies immediately, without the need to schedule scan windows or manage scanning credentials.														
8. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum: <ul style="list-style-type: none"> • Identification of the specific vulnerabilities, at risk, and/or compromised assets • Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results 														
B.2 Vulnerability Assessment and Penetration Testing (VAPT)	COMPLIED Y/N	REMARKS												
1. Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, if any and among others.														
2. The scope of VAPT shall be at least the following: <table border="1" data-bbox="167 1238 1259 1556" style="margin-left: 40px;"> <thead> <tr> <th style="text-align: center;">Agency</th> <th style="text-align: center;">Scope</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">BTr</td> <td style="text-align: center;">7 External resources, up to 80 IP addresses</td> </tr> <tr> <td style="text-align: center;">GSIS</td> <td style="text-align: center;">20 External resources, 2 mobile apps, up to 80 IP addresses</td> </tr> <tr> <td style="text-align: center;">SSS</td> <td style="text-align: center;">25 External resources, 1 mobile app up to 150 IP addresses</td> </tr> <tr> <td style="text-align: center;">IC</td> <td style="text-align: center;">20 External resources, up to 80 IP addresses</td> </tr> <tr> <td style="text-align: center;">PDIC</td> <td style="text-align: center;">8 External resources, up to 80 IP addresses</td> </tr> </tbody> </table>	Agency	Scope	BTr	7 External resources, up to 80 IP addresses	GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses	SSS	25 External resources, 1 mobile app up to 150 IP addresses	IC	20 External resources, up to 80 IP addresses	PDIC	8 External resources, up to 80 IP addresses		
Agency	Scope													
BTr	7 External resources, up to 80 IP addresses													
GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses													
SSS	25 External resources, 1 mobile app up to 150 IP addresses													
IC	20 External resources, up to 80 IP addresses													
PDIC	8 External resources, up to 80 IP addresses													
3. The service provider shall deliver and maintain a vulnerability database with relevant software version upgrades and security policy update recommendations, inclusive of changes to existing and new vulnerability and threat signatures.														
4. The service provider shall provide online reporting and metrics capability: <ul style="list-style-type: none"> • VAPT results/data (including risk, remediation status, and data compromised, if any) and access to historical test result and trend analysis delivered via the service provider's portal shall be accessible to the agencies. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations. 														

<p>5. The service provider shall have predefined fields/templates for the generation of reports, such as, but not limited to:</p> <ul style="list-style-type: none"> • VAPT Report (i.e., Executive Summary, Conclusion for Management Area, and Specific Action Plans) • Security Profiling Results (including reports from automated scanning tools) • Detailed observations and recommendations 		
<p>6. Common Vulnerability Scoring System values:</p> <ul style="list-style-type: none"> • The service provider shall use CVSS v3.0 or later for risk ranking and prioritizing security vulnerabilities. 		
<ul style="list-style-type: none"> • The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML. 		
<p>7. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to:</p> <ul style="list-style-type: none"> • Windows (all versions) • Linux and other Unix flavors (all versions) • Network and security related equipment, whether software or hardware-based • User profile settings • Advanced password analysis 		
<p>8. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:</p> <ul style="list-style-type: none"> • Application servers • Authentication servers • Backdoors and remote access services • Backup applications/tools • Database servers • Active Directory, Lightweight Directory Access Protocol (LDAP) • Domain Name Systems (DNS) • Mail servers and Simple Mail Transfer Protocols (SMTP) • Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS) • Network Time Protocols (NTP) • Remote Procedure Calls • Routing protocols • Simple Network Monitoring Protocol (SNMP) • Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) • Virtual Private Network (VPN) • Web and mobile applications • Web servers 		

C. Threat Intelligence	COMPLIED	REMARKS
1. The solution shall deliver threat intelligence on the following:		
<ul style="list-style-type: none"> • Brand protection - company names/domain 		
<ul style="list-style-type: none"> • Social media pages 		
<ul style="list-style-type: none"> • External Internet Protocol (IP) addresses 		
<ul style="list-style-type: none"> • Website and mobile application monitoring 		
<ul style="list-style-type: none"> • VIP e-mails 		
<ul style="list-style-type: none"> • Sector monitoring Financial, Government, Insurance, and Healthcare 		
<ul style="list-style-type: none"> • Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes 		
<ul style="list-style-type: none"> • Credit cards 		
<ul style="list-style-type: none"> • GitHub 		
<ul style="list-style-type: none"> • Custom queries 		
<ul style="list-style-type: none"> • 25 Site take downs for each agency during the duration of the contract(i.e., phishing, social media sites, and others) however, should the agency need additional takedowns, this will be provided by the service provider at no additional cost. 		
<ul style="list-style-type: none"> • Scraping databases that contain large amounts of data found in the deep and dark web 		
<ul style="list-style-type: none"> • Third party queries 		
<ul style="list-style-type: none"> • Investigation 		
<ul style="list-style-type: none"> • Threat library 		
2. The threat intelligence solution must, at minimally, harvest data from the following open, technical and closed sources types:		
<ul style="list-style-type: none"> • Mainstream Media (including news, information security sites, vendor research, blogs, vulnerability disclosures) 		
<ul style="list-style-type: none"> • Social Media 		
<ul style="list-style-type: none"> • Forums 		
<ul style="list-style-type: none"> • Paste Sites 		
<ul style="list-style-type: none"> • Code Repositories 		
<ul style="list-style-type: none"> • Threat lists (including spam, malware, malicious infrastructure) 		
<ul style="list-style-type: none"> • Dark Web (including multiple tiers of underground communities and marketplaces) 		
<ul style="list-style-type: none"> • Original research from in-house human intelligence analysts 		
3. The solutions provider must be able to:		

<ul style="list-style-type: none"> • Detect and take down servers launching phishing attacks 		
<ul style="list-style-type: none"> • Take down of fake applications that impersonate legitimate ones from app stores. 		
<ul style="list-style-type: none"> • Take immediate action on the agencies behalf and provide all the context to execute rapid take-down of malicious servers, websites or social media accounts. 		
4. The solution shall be capable to detect leaked Personally Identifiable Information (PIIs) and the agencies information from the deep and dark web, social media, and other forms of instant messaging platforms and provide recommended action plan.		
5. The threat intelligence solution must be able to identify fraudulent social media accounts that are impersonating the agencies and its executives		
6. The solution shall monitor the domains and IP addresses that have bad reputation.		
7. The service provider shall consume internal and external threat intelligence into its threat analysis process.		
8. The service provider shall deliver weekly intelligence summary reports on the latest cyber threats, including detected information on the intention to target agencies or other government industries, major activist campaigns, and indications of activism against the agencies, financial and health sector, and the government.		
9. The service provider shall provide a special report or notice to the agencies immediately, should there be any information or detection of targeted attacks against the agencies, the government or the sectors of the concerned agencies.		

D. Incident Response	COMPLIED Y/N	REMARKS
1. The service provider shall review the agencies Incident Response Plan (IRP), which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines, such as, but not limited to: <ul style="list-style-type: none"> • Escalation process • Incident containment process • Incident eradication process • Incident recovery process • Incident identification process • Process flow 		
2. The service provider shall act as the Incident Response (IR) Manager and facilitate the six (6) phases of IR. The service provider must be on-call and will conduct the IR activities onsite, as necessary (i.e., in cases of breach). The IRs per agency shall cover 200 accumulated hours per year. Beyond the required 200 hours, the agencies shall shoulder the cost. In case the 200 hours allotted for IR is not fully or not consumed, it can be converted to other services, such as training among others, that the provider can render for information security.		
3. The service provider shall conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness trainings to both technical and non-technical audiences of the agencies. The		

readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.		
4. The service provider shall conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.		
5. The Service Provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.		
6. The service provider shall deliver technical assistance to the agencies CSIRTs during emergency (successful) breach response.		
7. The Service Provider shall have a facility to receive client's reported incident (via authorized point of contact from client) for incidents not captured on the monitoring tool.		
8. The service provider shall deliver network/firewall/web applications breach response.		
9. The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.		
10. The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.		
11. The service provider shall identify indicators of compromise and scan the network to search for other related infected systems.		
12. The service provider shall deliver insider threat investigation, as needed.		
13. The service provider shall deliver employee misconduct investigations, as needed.		
14. The service provider shall deliver incident and investigation reports.		
15. The service provider shall have a certified and recently trained (at least in the past 12 months) in-house cyber security forensics specialist, to support advanced investigation.		
16. The service provider shall assist in the following: <ul style="list-style-type: none"> • Incident handling preparation and execution • Crisis management • Breach communication • Forensic analysis including preservation of evidence for chain of custody requirements • Remediation 		
17. The Service Provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).		

Service Level Agreement (SLA)																										
<p>1. Acknowledgement SLA - The Acknowledgement SLA Percentage shall be computed per month base on the total number of missed hours exceeding the Acknowledgement SLA guarantee of fifteen (15) minutes per incident</p> <table border="1"> <thead> <tr> <th>Service Level Target</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>98%</td> <td>Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.</td> </tr> </tbody> </table>			Service Level Target	Description	98%	Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.																				
Service Level Target	Description																									
98%	Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.																									
<p>2. Incident Response SLA - Time to respond or provide request from when incident or request is reported based on severity level.</p> <table border="1"> <thead> <tr> <th>Priority Level</th> <th>Incident Response Time</th> <th>Reference:</th> </tr> </thead> <tbody> <tr> <td>P1 - Catastrophic</td> <td>Within 60 minutes</td> <td rowspan="4">From the creation of service ticket up to triage. Triage is when the SOC L2 Incident Responder communicates with the client to further investigate and provide recommendation on how to contain, remediate, and recover from the security incident.</td> </tr> <tr> <td>P2 - Critical</td> <td>Within 90 minutes</td> </tr> <tr> <td>P3 – Marginal</td> <td>Within 120 minutes</td> </tr> <tr> <td>P4 - Negligible</td> <td>Within 160 minutes</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th></th> <th colspan="2">Target Response Time % per Month</th> </tr> <tr> <th>Incident Priority</th> <th>1 and 2</th> <th>3 and 4</th> </tr> </thead> <tbody> <tr> <td></td> <td>>=90%</td> <td>>=80%</td> </tr> <tr> <td></td> <td colspan="2">Sum of the number of incidents meeting required Response Time for all days in the month</td> </tr> </tbody> </table>			Priority Level	Incident Response Time	Reference:	P1 - Catastrophic	Within 60 minutes	From the creation of service ticket up to triage. Triage is when the SOC L2 Incident Responder communicates with the client to further investigate and provide recommendation on how to contain, remediate, and recover from the security incident.	P2 - Critical	Within 90 minutes	P3 – Marginal	Within 120 minutes	P4 - Negligible	Within 160 minutes		Target Response Time % per Month		Incident Priority	1 and 2	3 and 4		>=90%	>=80%		Sum of the number of incidents meeting required Response Time for all days in the month	
Priority Level	Incident Response Time	Reference:																								
P1 - Catastrophic	Within 60 minutes	From the creation of service ticket up to triage. Triage is when the SOC L2 Incident Responder communicates with the client to further investigate and provide recommendation on how to contain, remediate, and recover from the security incident.																								
P2 - Critical	Within 90 minutes																									
P3 – Marginal	Within 120 minutes																									
P4 - Negligible	Within 160 minutes																									
	Target Response Time % per Month																									
Incident Priority	1 and 2	3 and 4																								
	>=90%	>=80%																								
	Sum of the number of incidents meeting required Response Time for all days in the month																									

II. Non-functional Requirements

A. Access Management	COMPLIED Y/N	REMARKS
1. All credentials with the service provider shall be stored in a monitored central management system. These are leased to the agencies once strong authentication has been implemented and for the specific task for which it was authorized.		
2. The service provider's solution shall be accessed through a centralized portal, which enforces session timeouts, mandates the use of multi-factor authentication (MFA), and provides anomaly detection for monitoring user behavior.		
3. The service provider shall maintain logical access controls which are role-based, including principles of least privilege and segregation of duties.		
4. All passwords must have a minimum of fifteen (15) characters. Passwords must be changed every ninety (90) days and cannot be the same as the prior three (3) passwords. The service provider's system must mask passwords when entered and store password files separately from the application system data. Only encrypted hashes of passwords may be stored and transmitted.		
5. All access from the service provider's managed endpoints to sensitive resources shall be done via VPN configured with MFA. Opportunistic Transport Layer Security (TLS) is configured by default for e-mail. Remote hardware is managed by comprehensive enterprise management software that allows for maintenance and access control management.		
6. The service provider shall provide physical and environmental controls at the primary and secondary sites for this project.		
7. The agencies data shall be logically separated by using unique tagging to ensure segregation of data from the other agencies. The agencies should retain as the legal owner of the data processed and managed by the service provider.		

B. Training and Other Requirements	COMPLIED Y/N	REMARKS
1. The service provider should facilitate at least once a year Continual Service Improvement (CSI) workshop with client for possible improvement of service through process, people and technology.		
2. The service provider should provide security advisories with the client for the cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.		
3. The service provider shall conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on each Government Agency based on the NIST or CIS Controls.		

C. Service Provider's Qualification and Requirements <i>Note: Submission of required documents shall be during the submission of bids.</i>	COMPLIED Y/N	REMARKS
1. The service provider must be a certified/authorized reseller of the brand(s) being offered and shall submit a valid, certification from the manufacturer(s).		
2. The service provider must submit the following certifications: <ul style="list-style-type: none"> a. For Cloud based Security Operations Center (SOC), that this is hosted in a provider categorized as a leader either in the latest Forrester Wave™: Public Cloud Development And Infrastructure Platforms report or Gartner Magic Quadrant for Cloud Infrastructure and Platform Services; b. For Endpoint Detection and Response (EDR), that solution is categorized as a leader either in the latest Forrester Wave™ report for Enterprise Detection and Response or Gartner Magic Quadrant for Endpoint Protection Platforms; c. For Security Information and Event Management (SIEM), the solution provided is categorized as a leader in the latest Forrester Wave™ report for Security Analytics Platforms or Gartner Magic Quadrant for Security Information and Event Management (SIEM). 		
3. The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service), with a pool of at least 20 IT or Information Security related certified onsite support engineers within Metro Manila. A list of the support engineers shall be provided with their required qualifications, as stated in item D. Personnel Qualifications / Requirements.		
4. The service provider must have sales and technical offices located in the Philippines. The service provider should submit the list of their sales and technical offices in the Philippines, including the complete address and contact details. This is subject for actual site visit to the facility.		
5. The SOC can be provided on the cloud or within the premises of the service provider. Should the Security Operations Center (SOC) with their SOC analysts be on premise, they should be housed in a Data Center with TIA-942 Rated 3 Facility Certification or any equivalent third party assessment indicating the capability of the SOC to provide the required security, scalability, stability and high performance. The proof of compliance shall be submitted. 6. However, if the service provider's SOC will be implemented through a cloud service provider (CSP), the SOC platform must be guaranteed with at least 99.9% uptime or availability. The proof of compliance shall likewise be submitted.		
7. The service provider's SOC Analysts must have at least one or more of the following certifications: Certified Ethical Hacker (CEH), CyberSec First Responder, Information Technology Infrastructure Library (ITIL), or any relevant product certification to the security products of the platform offered by the Service Provider.		
8. The service provider must be at least five (5) years in Security and ICT Industry and must have more than three (3) years of experience in providing SOC services. The Service provider must have a SOC 2 Type II Attestation Report or ISO 27001 certification for		

Managed ICT Services or similar, done at least in 2021, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in place.		
9. The prospective bidders shall be required during the post qual evaluation to demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.		

D. Personnel Qualifications/Requirements	COMPLIED Y/N	REMARKS
<p>1. The service provider must have at least Two (2) local Certified Engineer on each of the following security tools below:</p> <ul style="list-style-type: none"> • SOAR • SIEM • Vulnerability Management <p>The certification must be the same with the brand that is being proposed.</p>		
<p>2. The service provider must assign a dedicated local SOC Manager that oversees the SOC and conducts regular monthly service performance review and reporting to client's management. A monthly service performance report shall be submitted and discussed by the SOC Manager. It shall contain the following:</p> <ul style="list-style-type: none"> • SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Over Time • Correlated Events and Rules Triggered Summary • Summary of Incident Ticket per Use Cases Incident Management 		
<p>3. The service provider must submit the following for all the personnel to be assigned to the cluster, and failure to submit the any of the requirement below is subject for disqualification.</p> <ul style="list-style-type: none"> • Resume/CV of the Proposed Personnel • Company ID • Certificate of employment 		
<p>4. The service provider must have a dedicated 24x7x365 team assigned to the cluster, composed of at least:</p> <ul style="list-style-type: none"> • 2-Tier 1 analyst who will be responsible for the following tasks: <ol style="list-style-type: none"> 1. Monitoring via existing SIEM/Analytics Platform 2. Funneling of alerts (noise elimination) 3. Incident Validation 4. Case Management 5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up 6. General Communication 7. Weekly Summary Reports 		

<ul style="list-style-type: none"> • 1-Tier 2 analyst who will be responsible to conduct further analysis and decides on a strategy for containment. <ol style="list-style-type: none"> 1. Proactive Searches/ Threat Hunting 2. Qualification of Incident Priority/Severity 3. Investigation via SIEM/Analytics Platform and other accessible sources 4. Rule Tuning 5. Ad hoc Vulnerability Advisory & Research 6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations • 1-Tier 3 senior analyst who will be responsible to manage critical incidents. Tier 3 analysts are also responsible for actively hunting for threats and assessing the vulnerability of the business. <ol style="list-style-type: none"> 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules • 1-Tier 4 analyst or the SOC manager, who will be in charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. The SOC manager will also be responsible for the management of the MSOC operations for the agency and cluster. 		
<p>5. The service provider should ensure that there will be alternate personnel deployed to the cluster should the primary personnel be unavailable for whatever reason.</p>		
<p>6. Qualifications</p>		
<ul style="list-style-type: none"> • Project Manager: <ul style="list-style-type: none"> • Must be with the service provider's organization at least one (1) year before the bid opening • Has handled project management for at least two (2) financial corporations or should have at least two (2) successful project implementations of at least Php 20M in amount in the last two (2) years. • Must provide a list of projects handled in the last 5 years, indicating the Project Name, Project Duration (Start date and end-date) and Contact Person with details for verification. • Must have a valid project management certification • SOC Manager/Tier 4 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening 		

<ul style="list-style-type: none"> • Has performed and managed three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least five (5) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience. • Has any two (2) of the following unexpired professional certifications: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), GIAC Security Essentials (GSEC), GIAC Continuous Monitoring (GMON), GIAC Certified Detection Analyst (GCDA), GIAC Web Application Penetration Tester (GWAPT), GIAC Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Intrusion Analyst (GCIA), Cisco Certified Network Associate (CCNA), Information Technology Infrastructure Library (ITIL), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Network Defense Architect (CNDA), CyberSec First Responder (CFR), CompTIA Security+, Certified Vulnerability Assessor (CVA), Offensive Security Certified Professional (OSCP), Certified Information System Security Professional (CISSP), Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), GIAC Exploit Researcher & Advanced Penetration Tester (GXPN), EC-Council Licensed Penetration Tester (LPT) Master, Certified Penetration Tester (CPT), Certified Expert Penetration Tester (CEPT), Certified Mobile and Web Application Penetration Tester (CMWAPT), CompTIA PenTest+, Certified Payment Card Industry Security Implementer (CPISI), or other security-related certifications. 		
<ul style="list-style-type: none"> • Team Lead/Tier 3 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening • Has functioned as lead in the performance of three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least five (5) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience • Has any two (2) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications. 		

<ul style="list-style-type: none"> • Team Member/Tier 2 or Tier 1 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening • Has performed three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least three (3) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience • Has at least one (1) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications. 		
---	--	--

4. Delivery Time/Completion Schedule

The Project must be implemented by phases: Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response , 120 working days from the issuance of the Notice to Proceed, Phase 2- Vulnerability Management, 90 working days from the issuance of the Notice to Proceed . Commencement date will be from the receipt of Notice To Proceed (NTP) by the winning bidder. The vendor must therefore provide a project schedule which should present the project milestones and deliverables at each milestone. License subscriptions will start upon contract implementation.

All deliverables shall become the property of the concerned agencies.

5. Payment Milestone

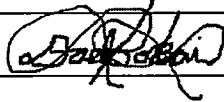
The Service provider shall be paid upon receipt of its deliverables, based on the submitted Project Schedule and issuance of the Certificate of Acceptance from the Insurance Cluster. The Service Provider shall be paid based on the following milestones:

Milestone	Percentage of the Total Contract Price
Year 1:	
Upon implementation of Threat Intelligence, Security Monitoring & Management, and Incident Response for the Insurance Cluster (Phase 1)	15%
After Phase 1 and upon implementation of Vulnerability Management for the Insurance Cluster (Phase 2)	15%
After Phase 2 and upon full implementation of the Shared Defense Solution and Insurance Cluster issuance of Certificate of Completion and Acceptance of the License subscription covering the first 12 months (1st Year)	20%
Year 2:	
Two (2) semi-annual payments at 25% each	50%
TOTAL	100%




SHARED CYBER DEFENSE SOLUTION Project

Bureau of the Treasury:

NAME	SIGNATURE
Mr. David Andrei P. de Mesa	




Government Service Insurance System:

NAME	SIGNATURE
Mr. Jonathan Pineda	

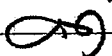


Social Security System:

NAME	SIGNATURE
Ms. Jocelyn Dela Peña	



Philippine Deposit Insurance Corporation:

NAME	SIGNATURE
Ms. Maria Belinda San Jose	
	Digitally signed by San Jose Maria Belinda Cusi Date: 2023.08.03 12:11:45 +08'00'



Section IV. General Conditions of Contract

Notes on the General Conditions of Contract

The General Conditions of Contract (GCC) in this Section, read in conjunction with the Special Conditions of Contract in Section V and other documents listed therein, should be a complete document expressing all the rights and obligations of the parties.

Matters governing performance of the SERVICE PROVIDER, payments under the contract, or matters affecting the risks, rights, and obligations of the parties under the contract are included in the GCC and Special Conditions of Contract.

Any complementary information, which may be needed, shall be introduced only through the Special Conditions of Contract.

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC)**.

2. Advance Payment and Terms of Payment

- 2.1. Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.
- 2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with

prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the SCC.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the SCC, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the SERVICE PROVIDER in writing, in a timely manner, of the identity of any representatives retained for these purposes.

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

5. Warranty

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

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

6. Liability of the SERVICE PROVIDER

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

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

Special Conditions of Contract

GCC Clause	
1.	<p>Scope of Contract:</p>
	<p>The Contract covers the supply, delivery, installation, configuration and administration by the SERVICE PROVIDER of a Shared Cyber Defense Security Solution (Project) for the Insurance Cluster, particularly the requirements of the PROCURING ENTITY under the Project as specified in the Terms of Reference comprising of a Cyber Defense Solution for 1,200 endpoints, with 2-year subscription for the provision of Security Monitoring and Management, Vulnerability Management, Threat Intelligence, and incident Response primarily focused on the National Institute Standards and Technology (NIST) Cybersecurity Framework – Identity, Protect, Detect, Response, and Recover (hereinafter referred to as the "Project").</p> <p>Incidental Services –</p> <p>The SERVICE PROVIDER shall, to the satisfaction of the Procuring Entity, undertake the following services:</p> <ul style="list-style-type: none"> • In-depth training of the Procuring Entity's IT personnel at the SERVICE PROVIDER's plant and/or onsite, relative to assembly, start-up, operation, maintenance, and/or repair of the Project; • Performance or supervision of on-site assembly and/or start-up of the Project; • Furnish detailed operations and maintenance manual for each appropriate unit of the Project; • Standard 24/7 on-site troubleshooting and repair of the Project within 2 hours response time, including weekend and holidays; • In case of defect within the warranty period, a service unit of the same or higher technical specification should be provided by the SERVICE PROVIDER, free of charge, if the unit is not repaired within 24 hours after the problem is reported; • Facilitate at least once a year Continual Service Improvement (CSI) workshop for possible improvement of the service through process, people and technology; • Provide security advisories for cybersecurity news and updates like the latest viruses, Trojans, worms, or other malicious programs; • Conduct an annual cyber security maturity assessment (i.e., people, process, and technology) based on the NIST or CIS controls; and • Render any and all assistance necessary towards the successful implementation of the Project.

Transportation –

Where the SERVICE PROVIDER is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the SERVICE PROVIDER, and related costs shall be included in the contract price.

Where the SERVICE PROVIDER is required under Contract to deliver the Goods CIF, CIP or DDP, goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, goods may be shipped by a carrier which is not of Philippine registry provided that the SERVICE PROVIDER obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the SERVICE PROVIDER in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. In any case, the SERVICE PROVIDER shall inform in writing the Procuring Entity within reasonable time or not later than three (3) calendar days of such delay and the expected date of shipment.

The Procuring Entity accepts no liability for the damage of Goods during transit. In the case of Goods supplied from within the Philippines or supplied by domestic provider, the risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination.

Delivery Time and Completion Schedule -

The Goods component of the Project shall be delivered by the SERVICE PROVIDER in accordance with the terms specified in Section VI (Schedule of Requirements).

Upon delivery of the Good, the SERVICE PROVIDER shall notify the **PROCURING ENTITY** and present the following documents:

1. Original copy of the SERVICE PROVIDER's Sales Invoice/Billing Statement/Statement of Account showing Goods' description, quantity, unit price, and total amount;
2. Original copy of the Manufacturer's and/or SERVICE PROVIDER's warranty certificate;
3. Delivery receipt, if any, detailing number and description of items received signed by the authorized receiving personnel; and
4. Certificate of Acceptance/Inspection Report signed by the Procuring Entity's representative at the Project Site.

Further, the SERVICE PROVIDER shall fully and faithfully perform, undertake, and accomplish to the satisfaction of Procuring Entity all deliverables herein required, including the Go Live support, as follows:

- Phase I (Threat Intelligence, Security Monitoring and Management, and Incident Response) – within forty-five (45) working days from receipt of the Notice to Proceed (NTP).
- Phase II (Vulnerability Management) – within sixty-five (65) working days from receipt of the NTP.

For this purpose, the SERVICE PROVIDER shall submit for the approval of the Procuring Entity a project schedule showing the project milestones and deliverables for each milestone.

Intellectual Property Rights –

The SERVICE PROVIDER shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.

Other Requirements -

- **Service Standard** - The SERVICE PROVIDER shall devote, with utmost efficiency and effectiveness, its skills/ knowledge, undivided attention, and the best of its ability to the performance/fulfillment of its obligations under this Project in accordance with the best professional standards. The SERVICE PROVIDER shall exercise all reasonable skills, care, and diligence in the discharge of its services, and shall always work in the best interests of the Procuring Entity. To this end, the SERVICE PROVIDER shall provide such personnel, with the required qualifications and experience, towards the efficient fulfillment of the services herein required.
- **Confidentiality** - The SERVICE PROVIDER agrees and acknowledges that the services covered by this Project may expose the Procuring Entity to confidential information and that any disclosure of such information may subject the Procuring Entity to financial, material and operational loss. Therefore, the Contractor hereby agrees as follows:
 - The SERVICE PROVIDER shall protect all confidential information which the Procuring Entity provides to it (whether orally, in writing or in any other form) using the same standards as the SERVICE PROVIDER applies to its own comparable confidential information, but in no event less than reasonable measures, and subject to the implementation of appropriate technical, physical, and organizational/administrative measures to protect personal data against accidental or unlawful destruction or accidental loss or unauthorized alteration, disclosure, or access.
 - The SERVICE PROVIDER, or any of its employees, agents, or representatives, shall not, either during the term of this Contract or at any time thereafter,

reveal, disclose, or furnish, in any manner, to any person, firm or corporation any information, document, method, design, or material relating to the Procuring Entity, or which otherwise are in the Procuring Entity's possession or custody, which the SERVICE PROVIDER or other members of its work staff/team, or its employees, agents, or representatives may have acquired or which came to its/ their knowledge or possession by reason of this Contract.

- If any of the SERVICE PROVIDER's employees, agents, or representatives, who has previously rendered services to the Procuring Entity, resigned or disengaged from the SERVICE PROVIDER during the subsistence of this contract, the SERVICE PROVIDER must inform the Procuring Entity of such fact within five (5) calendar days from resignation or disengagement of said employee, agent, or representative. The terms of confidentiality shall apply and bind the resigned or disengaged employee, agents, or representatives of the SERVICE PROVIDER who have acquired confidential information by reason of their previous relation with the SERVICE PROVIDER. The SERVICE PROVIDER shall be liable for damages or injury to the Procuring Entity resulting from disclosure by them of such information, document, method, design, or material.
- The SERVICE PROVIDER shall comply with the obligations imposed on personal information processor under Section 44(b) of the Implementing Rules and Regulations (IRR) of the Data Privacy Act, and all of the provisions of the Data Privacy Act, its IRR, and circulars issued by the National Privacy Commission pertaining to the processing and retention of personal information subject of this Project, as may be applicable. The SERVICE PROVIDER is strictly prohibited from accessing the records, making photocopies thereof, or transferring/allowing third parties access thereto without the prior written permission or instruction from the Procuring Entity.
- The SERVICE PROVIDER shall be liable for any disclosure of confidential information by its employees, agents, or representatives and other violations under the Data Privacy and Bank Secrecy Laws, without prejudice to other legal remedies available to the Procuring Entity.
- All data and information related to the Project furnished by the Procuring Entity to the SERVICE PROVIDER shall be treated with strict confidentiality and shall be returned to the Procuring Entity upon completion of the works without need of demand. The same shall not be released to third parties without the written consent of the Procuring Entity.
- The SERVICE PROVIDER agrees to assume sole responsibility and hereby undertakes to indemnify the Procuring Entity, for any damage, which the

Procuring Entity may sustain by reason of breach of any of the above conditions.

- Nothing in this Contract shall be deemed to limit or restrict the rights of the Procuring Entity to assert any claim for violation/infringement of patent, copyright, trade secrets or other intellectual property rights against the SERVICE PROVIDER.

The SERVICE PROVIDER and its project staff may be required by the Procuring Entity to sign a confidentiality or non-disclosure agreement.

- **Relation of the Parties** - Subject to the limitation imposed on the SERVICE PROVIDER with respect to the replacement of personnel as mentioned above, the SERVICE PROVIDER shall be free to use any means and methods not contrary to law, regulations and the provisions and the spirit of this Contract, which it believes will best enable it to perform its obligations under this Contract. The SERVICE PROVIDER shall not be subject to the control and supervision of the Procuring Entity insofar as the means and methods to be employed by the SERVICE PROVIDER to satisfactorily perform its deliverables under this Contract, it being understood that the Procuring Entity is interested only in the results of the SERVICE PROVIDER's performance of its duties and responsibilities under this Contract. The Procuring Entity shall have the exclusive right to decide any and all questions which may arise as to the quality or acceptability of the goods and services delivered/rendered by the SERVICE PROVIDER.
- **Event of Default** – The SERVICE PROVIDER shall be considered in default in the event that the SERVICE PROVIDER or any of its personnel assigned in the Procuring Entity violates or breaches any of the terms and conditions of the Contract, which includes neglecting to perform and deliver in a timely manner any of the goods, service, duties, functions, responsibilities or obligations stipulated herein, or fails for any reason whatsoever to carry out the tasks herein required in a satisfactory and acceptable manner.
- **Retention Right** – The Procuring Entity is hereby given a lien upon any and all monies or other properties of the SERVICE PROVIDER which are in the Procuring Entity's possession or with any third party acting on behalf of the Procuring Entity including, but not limited to, those left with the Procuring Entity by or for the account of the SERVICE PROVIDER. The Procuring Entity is hereby given the right to retain the same to guarantee the payment or performance of any obligation or liability, contingent or otherwise, on the part of the SERVICE PROVIDER under the Contract.
- **Exercise of Rights** –

➤ **Alternative Remedies** – The Procuring Entity shall have the right to exercise alternatively, concurrently or cumulatively all the rights and remedies now or hereafter available under the Contract, such as, but not limited to, the forfeiture of the SERVICE PROVIDER's Performance Security, as well as the availment by the Procuring Entity of other remedies under other applicable laws, rules and regulations.

➤ **Non-Waiver of Rights** – The failure of the Procuring Entity to insist upon the strict performance of any of the terms, conditions and covenants hereof shall not be deemed a relinquishment or waiver of any right or remedy that the Procuring Entity may exercise, nor shall it be construed as a waiver of any subsequent breach or default of the terms, conditions and covenants hereof, which shall continue to be in full force and effect.

No waiver by the Procuring Entity of any of its rights hereunder shall be binding or deemed to have been made unless expressed in writing and signed by the Procuring Entity through its duly authorized agents.

- **Representations and Warranties –**

The SERVICE PROVIDER represents and warrants to the Procuring Entity that:

TECHNICAL REPRESENTATIONS

- The hardware and software components supplied for this Project are brand new, unused, of the most recent models, and that they incorporate all recent improvements in design and materials.
- The SERVICE PROVIDER represents that the manpower complement that it will assign to the Procuring Entity to handle the Project have the qualifications, technical skills, and knowledge required in Item II (D) of the Terms of Reference, and that they shall perform their assigned tasks with undivided attention and with utmost efficiency and effectiveness and in accordance with the best professional standards and ethical considerations. Further, the SERVICE PROVIDER warrants that it shall exercise all reasonable skill, care and diligence in the discharge of its services, and shall always work to the best interests of the Procuring Entity. To this end, the SERVICE PROVIDER shall provide personnel with adequate qualifications and experience, and of such number as may be required for the efficient fulfillment of the required services.

- The SERVICE PROVIDER shall not replace key personnel without the consent of the Procuring Entity. Key personnel shall be understood to refer to the personnel specified in Item II (D) of the Terms of Reference.

The Procuring Entity, however, reserves the right to demand at any time, without need to present proof or substantiate its request, the immediate replacement of any of the SERVICE PROVIDER's personnel, staff or representative assigned to the Project who is wanting in competence, honesty, integrity, or whose services is deemed to be or will otherwise be prejudicial to the interest of the Procuring Entity.

Further, the SERVICE PROVIDER undertakes that it shall not employ, in any capacity whatsoever, the Procuring Entity's personnel involved in the project. This prohibition shall be enforceable up to a period of two (2) years from the date of acceptance of the project by the Procuring Entity.

- It has full knowledge of the extent of work needed for the successful implementation of the Project; and that, it shall conform strictly with all the terms and conditions of this Contract.

LEGAL REPRESENTATIONS

- It is a domestic corporation duly organized and registered, validly existing, and in good standing under the laws of the Republic of the Philippines.
- It has full legal power, authority, and right to carry on its present business. The SERVICE PROVIDER further represents that its representative Mr. WILFREDO N. AGUILAR has full legal power to sign, execute, and deliver this Contract; and that, the SERVICE PROVIDER will comply, perform and observe the terms and conditions hereof.
- All corporate and other actions necessary to validate or authorize the execution and delivery of this Contract have been taken.
- It has all the qualifications required in Item II (C) of the Terms of Reference, and met all the criteria required to participate in the Project.
- This Contract, when executed and delivered, will be legal, valid, and enforceable in accordance with its terms.
- The SERVICE PROVIDER is duly authorized by the manufacturer to provide, sell, configure and support the proposed product/solution. For this purpose, the SERVICE PROVIDER shall issue in favor of the Procuring Entity a certification in this regard during the submission of bids.

- The continuous use of the Project by the Procuring Entity would not amount to infringement of any patent or copyright therein. For this purpose, the SERVICE PROVIDER shall issue in favor of the Procuring Entity a proof of entitlement, which entitlement shall encompass the entire warranty period.
- To the knowledge of the SERVICE PROVIDER, there are no pending or threatened actions or proceedings before any court or administrative agency of any jurisdiction, which may materially or adversely affect the financial condition or operation of the SERVICE PROVIDER or the SERVICE PROVIDER's ability to comply with the terms and conditions of this Contract. If the SERVICE PROVIDER should thereafter learn of the existence or occurrence of the same, the SERVICE PROVIDER undertakes to report such fact to the Procuring Entity within five (5) calendar days therefrom. Failure to do so shall constitute sufficient ground for the cancellation of this Contract and the enforcement of remedies which the Procuring Entity may exercise under this Contract, pertinent laws, rules, and regulations.
- The obligation of the SERVICE PROVIDER under this Contract, and other ancillary documents which may be executed in connection herewith, shall constitute its direct, absolute, and unconditional obligation.
- In line with Executive Order No. 398, Series of 2005, the SERVICE PROVIDER warrants and certifies that it is free and clear of all tax liabilities to the government. Further, it binds itself to pay taxes in full and on time; and that its failure to do so shall entitle the Procuring Entity to suspend payment for any goods and services delivered by the SERVICE PROVIDER. Towards this, the SERVICE PROVIDER shall regularly present to the Procuring Entity its tax clearance from the Bureau of Internal Revenue (BIR), as well as a copy of its income and business tax returns duly stamped and received by the BIR and duly validated with the tax payments made thereon.

WARRANTIES

- It warrants to the Procuring Entity, in an unconditional, unqualified, absolute, full, and direct manner, the Project against incompatibilities or any defect, hidden, inherent, or otherwise, which would render them unfit for the use for which it is intended, or which would diminish the fitness of its use to the extent that, had the Procuring Entity been aware thereof, it would not have acquired/accepted the same.

It also warrants to the Procuring Entity, in an unconditional, unqualified, absolute, full, and direct manner, that the Project upon its completion, shall be free from any defects arising from poor design/ workmanship, inferior/substandard materials, or from any negligent act or omission of the SERVICE PROVIDER that may develop during the normal use of the same.

- It warrants that, unless authorized in writing by the Procuring Entity, any updates/upgrades, algorithm or code associated with the services provided to the Procuring Entity, regardless if pre-existing or developed for the Procuring Entity, shall:
 - contain no code and/or services, catering for unauthorized functionality, e.g., malware, backdoor, unauthorized remote access to or from the Procuring Entity's Network;
 - not alter, damage, or erase any data or computer programs without control of the authorized person; and
 - contain no key, node lock, time-out, or other functions, whether implemented by electronic, mechanical, or other means, that restricts or may restrict the Procuring Entity's use or access to any programs or data developed relative to the project.
- The acceptance of the Project by the Procuring Entity shall not, at any given time, be deemed a waiver of any causes of action which the Procuring Entity may subsequently exercise by reason of any defect maintenance and support services provided by the SERVICE PROVIDER.
- **Miscellaneous Provisions –**
 - **Severability** – If any provision of the Contract should, for any reason, be held void or unenforceable, the legality and enforceability of the remaining provisions contained herein shall not in any way be affected or impaired, and shall remain in full force and effect.
 - **Binding Effect/Assignment of Rights** – The Contract shall be binding upon the SERVICE PROVIDER, its partners, successors-in-interest, legal representatives and assigns. The foregoing notwithstanding, the SERVICE PROVIDER shall not in any way assign, subcontract, or transfer its rights and obligations under the Contract without the written approval of the Procuring Entity.
 - **Entire Agreement** – The provisions of this SCC, together with all the documents attached and/or incorporated thereto, and/or referred to therein, constitutes the entire obligation of the parties with respect to the subject matter hereof and shall supersede any prior expression of intent or understanding, whether verbally or in writing, with respect to this transaction.
For this reason, the parties shall endeavor to interpret the various provisions of this SCC and other related Bid Documents in a manner that will render all of those provisions valid and enforceable. In case

of conflict between the provisions of the Bid Documents and the provisions laid out in this SCC, the latter shall prevail.

- **Other Documents** – The parties agree to provide further assistance and execute such documents as may be necessary or reasonably desirable to accomplish the intents and purposes of the Contract.
- **Transfer of Location** - The transfer of the principal office of either party to any place, area or building in Metro Manila shall not affect the terms and conditions of the Contract.
- **OGCC Review** - The provisions of this SCC shall be submitted to the Office of the Government Corporate Counsel (OGCC) for its review prior to execution pursuant to Memorandum Circular No. 2018-02 issued by the Governance Commission for Government Owned and Controlled Corporations. Any and all comments of the OGCC as a result of its review shall be deemed incorporated in this SSC, as may be appropriate.
- **Contra Preferentem** – This Contract is not to be interpreted or construed against the interest of the Procuring Entity merely because the latter prepared and drafted the Contract.
- **Dispute Resolution** – In case any dispute or disagreement of any kind whatsoever arises between the Procuring Entity and the SERVICE PROVIDER in connection with or arising out of this Contract, the parties shall make every effort to resolve such dispute or disagreement amicably by mutual consultation.

If after thirty (30) calendar days, the parties have failed to resolve their dispute or difference by mutual consultation, then either the Procuring Entity or the SERVICE PROVIDER may give notice to other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

Any dispute or disagreement in respect of which a notice to commence arbitration has been given in accordance with this Clause shall be settled by arbitration.

Arbitration may be commenced prior to or after the delivery of the services under this Contract.

In the case of a dispute between the Procuring Entity and the SERVICE PROVIDER, the dispute shall be resolved in accordance with Republic Act 9285 (RA 9285), otherwise known as the "Alternative Dispute Resolution Act of 2004".

Notwithstanding any reference to arbitration herein, the parties shall perform their respective obligations under the Contract unless they otherwise agree; and the Procuring Entity shall pay the SERVICE PROVIDER any monies due the SERVICE PROVIDER unless the issue involved will render the Contract void.

- **Attorney's Fee** - In the event that the Procuring Entity is compelled to commence arbitration or to seek judicial relief to enforce the provisions of this Contract, it shall be entitled to attorney's fees and liquidated damages equivalent to ten percent (10%) and fifteen percent (15%), respectively, of the contract price or the amount claimed in the arbitration, whichever is higher, aside from the costs of arbitration or litigation, whichever is applicable, and other expenses incidental thereto.
- **Venue for Suit** - Whenever necessary to promote Arbitration or to seek judicial relief, the Procuring Entity and the SERVICE PROVIDER agree that any legal action, suit or proceeding arising out or relating to the Contract may be instituted in any competent court in Makati City, to the exclusion of all other courts of equal jurisdiction.
- **Governing Law and Language** - This Contract shall be interpreted in accordance with the laws of the Republic of the Philippines.

This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract. All correspondence and other documents pertaining to this Contract exchanged by the parties shall be written in English.

- **Notices** - Any notice, request, report, and such other matters related to this Contract which are required or permitted to be given hereunder shall be in writing and shall be personally delivered or transmitted by registered mail with postage prepaid to the parties as follows:

➤

To the **Procuring Entity** : Mr. Renar M. Gonzales
Officer- in-Charge, IT Group

To the **SERVICE PROVIDER** : Mr. Wilfredo N. Aguilar
Account Manager

- **Termination for Convenience and Insolvency.** The Procuring Entity may terminate this Contract, in whole or in part, at any time for its convenience, subject to procedures laid down in 2016 RIRR of R. A No. 9184 on termination of contract, if it has been determined by the Procuring Entity that the continuance of this Contract would be economically, financially or technically impractical and/or unnecessary on the part of the Procuring Entity such as, but not limited to fortuitous event(s), changes in law or the Procuring Entity's or the national government policies.

Further, the Procuring Entity shall terminate this Contract if the SERVICE PROVIDER is declared bankrupt or insolvent as determined with finality by a court of competent jurisdiction. In this event, termination will be without compensation to the SERVICE PROVIDER, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Entity.

2.2

Terms of Payment:

- a. In consideration of the goods and the required services to be provided by the SERVICE PROVIDER to the Procuring Entity by reason of this Contract, as well as its compliance with all the terms and conditions of this Contract, the Procuring Entity agrees to pay the SERVICE PROVIDER the total amount of **Twenty Three Million Six Hundred Eighty One Thousand Two Hundred Eighty and 00/100 (PhP23,681,280.00)**, Philippine currency, inclusive of all applicable taxes (EVAT and all other related taxes) and other government mandated fees and other applicable fees and charges, for the execution and completion of the Project, including the incidental services, materials, equipment, accommodation, and operational expenses, and the remedying of any defects therein.
- b. The consideration/contract price referred to above shall be paid through progress billing. Each and every payment herein specified shall be net of any and all amounts required by law or this Contract to be retained or deducted by the Procuring Entity or paid by or charged against the SERVICE PROVIDER under the terms of this Project. Payment shall be made according to the following schedule:

Milestone	Percentage of the Total Contract Price
Year 1:	
Upon implementation of Threat Intelligence, Security Monitoring & Management, and Incident Response for the Insurance Cluster (Phase 1)	15%
After Phase 1 and upon implementation of Vulnerability Management for the Insurance Cluster (Phase 2)	15%

After Phase 2 and upon full implementation of the Shared Defense Solution and Insurance Cluster issuance of Certificate of Completion and Acceptance of the License subscription covering the first 12 months (1st Year)	20%
Year 2:	
Two (2) semi-annual payments at 25% each	50%
TOTAL	100%

- c. Payment shall be made by the Procuring Entity not later than seven (7) working days from receipt of the billing statement, and after issuance by the Procuring Entity of the certificate of completion for the Project. Completion shall be understood to mean compliance by the SERVICE PROVIDER of all of the standards/requirements set for the Project as determined by the members of the Insurance Cluster. For purposes of this provision, the SERVICE PROVIDER hereby acknowledges that the Procuring Entity together with the other members of the Insurance Cluster shall be the final arbiter on the acceptability and sufficiency of the SERVICE PROVIDER's deliverables and completed outputs.
- d. All payments made under this Contract shall be subject to any and all amounts required by law or this Contract to be retained or deducted by the Procuring Entity or paid by or charged against the SERVICE PROVIDER under the terms of this Contract, and subject to the Procuring Entity's and government accounting rules and regulations which shall include, among others, the Commission on Audit (COA) Circular No. 2012-001 (Prescribing the Revised Guidelines and Documentary Requirements for Common Government Transaction).
- e. The Procuring Entity, at no additional cost to it, has the option to amend or modify the schedule provided above.

3.

Performance Security:

The performance security posted in favor of the Procuring Entity in the form prescribed by law must be valid, sufficient, and effective for the entire Contract/Project Duration, inclusive of change order/extra work order/variation order, if any. The SERVICE PROVIDER shall cause the extension of the validity of the performance security and its sufficiency to cover the approved contract time extension, if any, until the issuance by the Procuring Entity of the certificate of completion of the Project. The SERVICE PROVIDER shall furnish the Procuring Entity with the corresponding proof thereof prior to the commencement of the contract time extension/change order/extra work/variation order, as the case may be.

The SERVICE PROVIDER shall cause the extension of the validity of the performance security to cover the approved contract time extension, if any, and furnish the Procuring Entity with the corresponding proof thereof.

In the event that the performance security posted by the SERVICE PROVIDER would be deemed inadequate, unacceptable, or otherwise rendered unenforceable or invalid at any time prior to the issuance of the Certificate of Completion, the Procuring Entity shall have the right to require the SERVICE PROVIDER, and the SERVICE PROVIDER shall have the obligation, to post another performance security in the form and amount determined by the Procuring Entity and allowed under existing laws and regulations.

If the performance security falls below the minimum amount required at any time prior to the issuance of the certificate of full completion, the SERVICE PROVIDER shall post additional performance security to bring it to the required level.

The performance security shall answer for any damage that the Procuring Entity may suffer by reason of the SERVICE PROVIDER's default of any of its obligations and/or breach of the terms and conditions of this Contract and shall likewise guarantee payment for any loss, damage, or injury that may be caused by the SERVICE PROVIDER to the Procuring Entity, its employees and guests. Any changes made in this Contract shall in no way annul, release or affect the liability of the SERVICE PROVIDER and the performance security.

The performance security shall only be released upon the Procuring Entity's issuance of the Certificate of Completion, which Certificate shall be issued only after the SERVICE PROVIDER's full and faithful performance of its obligations under this Contract, and subject to the following conditions:

- The Procuring Entity has no claim against the SERVICE PROVIDER or the surety company;
- The Procuring Entity has no claim for labor and materials against the SERVICE PROVIDER; and
- The SERVICE PROVIDER has faithfully and completely performed its obligations under this Project.

The Procuring Entity is hereby given a lien upon any and all monies or other properties of the SERVICE PROVIDER, which are in the Procuring Entity's possession or with any third party acting on behalf of the Procuring Entity, including without limitation to those left with the Procuring Entity by or for the account of the SERVICE PROVIDER. The Procuring Entity is given the right to retain the same to guarantee the payment or performance of any and all liability of the SERVICE PROVIDER under this Project, contingent or otherwise, which the Procuring Entity may be held jointly or solidarily liable.

4.	<p>Inspection and Test:</p> <p>The inspections and tests shall be conducted at the Project Site by the Procuring Entity's Information Technology Group to determine whether the output faithfully meets the minimum requirements specified for the Project.</p>
5.	<p>Warranty:</p> <p>To assure that defects on the Project shall be corrected by the SERVICE PROVIDER, the SERVICE PROVIDER shall provide a two (2) year warranty on the Project, reckoned from the date of the issuance by the Procuring Entity of the Certificate of Completion for the Project.</p> <p>To ensure the full and faithful compliance by the SERVICE PROVIDER of all the terms and conditions of this Contract as well as to cover for any defects on the Project, a retention money or a special bank guarantee equivalent to at least one percent (1%) of the total amount due to the SERVICE PROVIDER shall be deducted/retained or posted in favor of the Procuring Entity by the SERVICE PROVIDER.</p> <p>The retention money or the special bank guarantee shall be released to the SERVICE PROVIDER only after the Procuring Entity shall have issued a Certificate of Full Acceptance for the Project, which Certificate shall be issued only after three (3) years from issuance of the Certificate of Completion of the Project; and provided, further, that the Project delivered and supplied under this Contract, are free from patent and latent defects, and all conditions imposed under this Contract have been fully met.</p>
C	<p>Liability of the SERVICE PROVIDER:</p> <p>In the event that the SERVICE PROVIDER violates or breaches any of the terms and conditions of the contract, which includes neglecting to perform and deliver within the prescribed period any of the works, duties, functions, responsibilities or obligations stipulated herein, inclusive of the duly granted time extension, if any, or fails for any reason whatsoever to carry out the tasks herein required in a satisfactory and acceptable manner, the SERVICE PROVIDER shall be liable in any or all of the following consequences of default:</p> <ul style="list-style-type: none"> a. Forfeiture of Performance Security - The performance security shall be forfeited in favor of the Procuring Entity in the event that the SERVICE PROVIDER is in default or breach of its obligations under the contract and shall answer for any loss, damage or injury caused to the Procuring Entity as a result of the willful, unlawful or negligent act or omission of the SERVICE PROVIDER or any of the SERVICE PROVIDER's representative. b. Liquidated Damages and Penalties - The SERVICE PROVIDER shall, without need of demand, be liable for damages for such default and shall pay the Procuring Entity liquidated damages in an amount equivalent to one-tenth (1/10) of one percent (1%) of the cost of the unperformed portion for every day of delay or breach. In the event that the total sum of liquidated damages or the total cost

to the Procuring Entity of any such delay or inability by the SERVICE PROVIDER to deliver its obligations reaches 10% of the contract price, the Procuring Entity may, at its option, (i) proceed to terminate the contract in accordance with the procedures laid down in Annex I of the Implementing Rules and Regulations (IRR) of Republic Act (RA) 9184, or (ii) allow the SERVICE PROVIDER to continue and complete the Project subject to continuous accrual and imposition of liquidated damages at the rate herein prescribed until such services are finally delivered and accepted by the Procuring Entity.

The Procuring Entity need not prove that it has incurred actual damages to be entitled to remedies above provided. Furthermore, the Procuring Entity reserves the right to deduct any and all of the damages/penalties from any money due or payments which may become due to the SERVICE PROVIDER under the terms of the contract and/or from the securities/warranties filed/submitted by the SERVICE PROVIDER as the Procuring Entity may deem convenient and expeditious under the prevailing circumstances.

- c. **Stoppage of Work/Payment** - The Procuring Entity shall have the right to stop, in whole or in part, any of the work or payment due under the contract in the event of default on the part of the SERVICE PROVIDER to perform its obligations under the contract.
- d. **Take-over of Contract** - The Procuring Entity shall have the right to procure/engage, upon such terms and manners as the Procuring Entity shall deem appropriate, the services of another SERVICE PROVIDER to undertake the unperformed/undelivered service(s) of the SERVICE PROVIDER pursuant to the provisions of the IRR of R.A No. 9184. Any expenses that may be incurred to engage another SERVICE PROVIDER shall be for the exclusive account of the SERVICE PROVIDER. The SERVICE PROVIDER shall likewise be liable to pay for all the incremental expenses that the Procuring Entity may incur to fully complete the Project.
- e. **Termination of Contract** - In the event that such delay, default, failure or refusal to deliver or perform any or all of the goods or services within the limit prescribed herein, including with any extension thereof granted, if any, the Procuring Entity shall have the right to terminate the contract, subject to provisions of Annex I of the IRR of R.A No. 9184.

Upon the commencement of the termination, the SERVICE PROVIDER shall stop the work immediately, in case no prior work stoppage has been issued by the Procuring Entity against the SERVICE PROVIDER. The SERVICE PROVIDER shall also turn over all documents/records which came to its possession by reason of the contract.

- f. **Blacklisting of the SERVICE PROVIDER** - Upon termination of the contract due to default of the SERVICE PROVIDER, the Procuring Entity shall have the right to issue

a Blacklisting Order disqualifying the SERVICE PROVIDER from participating in the bidding of all government projects during the period of suspension.

- g. **Non-exclusivity** - The sanctions and remedies mentioned herein shall be understood to be without prejudice to other rights that the Procuring Entity may exercise under the contract, pertinent laws, rules, and regulations.
- h. **Indemnity** - The SERVICE PROVIDER agrees to indemnify the Procuring Entity against any and all loss, injury or damage either to person or property which the Procuring Entity may suffer by reason of the willful misconduct, unlawful or negligent act or omission of the SERVICE PROVIDER or any of its personnel or representative.

The indemnity required herein shall be in addition to the foregoing remedies and sanctions which the Procuring Entity may exercise under the contract, pertinent laws, rules, and regulations.

Force Majeure:

The SERVICE PROVIDER shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that the SERVICE PROVIDER's delay in performance or other failure to perform its obligations under the Contract is the result of a *force majeure*.

For purposes of this Contract the terms "*force majeure*" and "fortuitous event" may be used interchangeably. In this regard, a fortuitous event or *force majeure* shall be interpreted to mean an event which the SERVICE PROVIDER could not have foreseen, or which though foreseen, was inevitable. It shall not include ordinary unfavorable weather conditions; and any other cause the effects of which could have been avoided with the exercise of reasonable diligence by the SERVICE PROVIDER. Such events may include, but not limited to, acts of the Procuring Entity in its sovereign capacity, wars or revolutions, fires, floods, epidemics, pandemic, quarantine restrictions, and freight embargoes.

If a *force majeure* situation arises, the SERVICE PROVIDER shall promptly notify the Procuring Entity in writing of such condition and the cause thereof. Unless otherwise directed by the Procuring Entity in writing, the SERVICE PROVIDER shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the *force majeure*.



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF JUSTICE
OFFICE OF THE GOVERNMENT CORPORATE COUNSEL
3rd Floor MWSS Administration Building, Katipunan Avenue
Balara, Quezon City
Tel. Nos. 927-0030 / 920-7477 • Fax No. 436-4405
www.ogcc.gov.ph

CONTRACT REVIEW

No. 553
Series of 2022

FOR: PHILIPPINE DEPOSIT INSURANCE CORPORATION
ATTENTION: ATTY. MA. ANTONETTE BRILLANTES-BOLIVAR
General Counsel
RE: CONTRACT FOR THE PROCUREMENT OF SHARED CYBER
DEFENSE SOLUTION FOR THE MEMBERS OF THE
INSURANCE CLUSTER
DATE: 4 MAY 2022

I. Preliminary Statement:

We respond to your 4 April 2022 letter requesting for our review of the draft Contract to be entered into by the Philippine Deposit Insurance Corporation (PDIC) with a prospective Service Provider for the procurement of shared cyber defense solution for the members of the Insurance Cluster. Also, attached are the Terms of Reference, the General and Special Conditions of the Contract for our reference.

II. Antecedents:

Per your letter, the PDIC, Government Services Insurance System, Social Security System, Insurance Commission, and the Bureau of Treasury (collectively referred to as "Insurance Cluster") were directed by the Secretary of Finance to institutionalize a cost-effective defense strategy that will shield/protect their respective systems from potential cybersecurity threats along with other possible risks and data breaches in their respective digital landscape.

..... committed to uphold justice
under the rule of law



The Insurance Cluster agree that a shared defense strategy for cybersecurity will boost the resiliency of each institution and the cluster as a whole against cyberattacks. Thus, the need to provide an additional layer of protection to the information technology systems of each agency under the Insurance Cluster through the joint acquisition of a Shared Cyber Defense Solution (the Project").

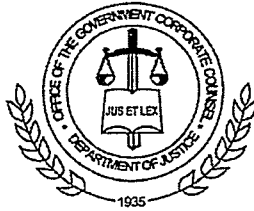
The Project aims to: establish a standard cybersecurity implementation, based on best practice; improve resilience against cyberattacks by being able to promptly detect, prevent and respond to any threats and attacks; share interagency threat intel and information; and profile and monitor the threat landscape the cluster is operating on.

To hasten the Implementation of the Project, and to ensure the procurement of a single solution for all the members of the Insurance Cluster, the members of the Insurance Cluster designated Land Bank of the Philippines (LBP) to undertake the necessary procurement of the Project pursuant to Section 7.3.3 of the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act (R.A) No. 9184).

The OGCC, in Contract Review No. 1273, Series of 2021, recognized the authority of a government agency to request another government agency to undertake the procurement process for it or outsource the procurement tasks under Section 7.3.3, paragraph (a), Rule II of the RIRR. Further, the GPPB-Technical Support Office (TSO), in its 16 June 2021 letter for LBP, responded to the latter's 17 May 2021 query by stating that outsourced procurement tasks may be performed by another government entity.

The members of the Insurance Cluster are in the process of completing – the procurement process. Each agency, including the PDIC shall have a separate contract with the winning bidder which will cover the specific deliverables of each agency under the Terms of Reference for the Project.

A handwritten signature or set of initials in the bottom left corner of the page.



III. Discussion:

The procurement of goods, infrastructure projects and consulting services by any branch, agency, department, bureau, office, or instrumentality of the Government of the Philippines, including government-owned and/or -controlled corporations (GOCCs), government financial institutions (GFIs), state universities and colleges (SUCs), and local government units (LGUs), must comply with the guidelines of Republic Act (RA) 9184 and its Revised Implementing Rules and Regulations (RIRR). Thus, PDIC should comply with the requirements of RA 9184 and the RIRR particularly on the conduct of public bidding.

Likewise, this Office consistently emphasizes that PDIC should strictly use the standard forms issued by the Government Procurement Policy Board (GPPB) and comply with GPPB Circular 04-2020,¹ issued last 16 September 2020, in the preparation of the bidding documents.

Section 6, Article 1 of RA 9184 likewise provides:

SEC. 6. Standardization of Procurement Process and Forms. - To systematize the procurement process, avoid confusion and ensure transparency, the procurement process, including the forms to be used, shall be standardized insofar as practicable.

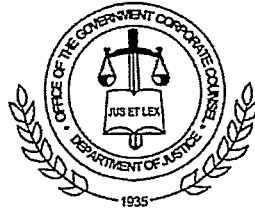
For this purpose, the GPPB shall pursue the development of generic procurement manuals and standard bidding forms, the use of which once issued shall be mandatory upon all Procuring Entities. (Boldfacing supplied).

By way of guidance, the contents of the standard bidding forms are enumerated in Section 17, RA 9184 as follows:

SEC. 17. Form and Contents of Bidding Documents. - The Bidding Documents shall be prepared by the Procuring Entity following the

¹ Guidelines in the Preparation of the Simplified Philippine Bidding Documents for Goods and Infrastructure Projects and the Submission of the Required Forms to be included in the Procurement of Goods, Infrastructure Projects, and Consulting Services.

A handwritten signature or set of initials, possibly "RQ", is located in the bottom left corner of the page.



standard forms and manuals prescribed by the GPPB. The Bidding Documents shall include the following:

- (a) Approved Budget for the Contract;
- (b) Instructions to Bidders, including criteria for eligibility, bid evaluation and post-qualification, as well as the date, time and place of the pre-bid Conference (where applicable), submission of bids and opening of bids;
- (c) Terms of Reference;
- (d) Eligibility Requirements;
- (e) Plans and Technical Specifications;
- (f) Form of Bid, Price Form, and List of Goods or Bill of Quantities;
- (g) Delivery Time or Completion Schedule;
- (h) Form and Amount of Bid Security;
- (i) Form and Amount of Performance Security and Warranty; and,
- (j) Form of Contract, and General and Special Conditions of Contract.

The Procuring Entity may require additional document requirements or specifications necessary to complete the information required for the bidders to prepare and submit their respective bid.

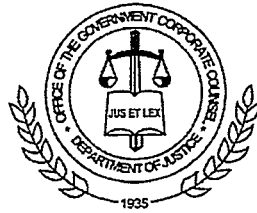
Pursuant to Section 6 of RA 9184 and its 2016 RIRR, the Procuring Entities (PEs) are mandated to use the latest approved Philippine Bidding Documents (PBDs)² and the standard forms to be submitted by the Bidders under Sections 17 and 23. The said standard forms shall be referred to herein as the Required Forms.

The GPPB has issued templates for the recommended forms, which are contained in the PBDs for the procurement of (1) Goods; (2) Infrastructure Projects; and (3) Consulting Services. In addition, Section 6 of the 2016 RIRR provides that once issued by the GPPB, the use of the Generic Procurement Manuals (GPMs), PBDs and other standard forms shall be mandatory upon all PEs.³ This applies to the proposed Terms of Reference, Technical Specifications, and to the General Conditions of Contract (GCC) and Special Conditions of Contract (SCC).

After a careful study of the terms and conditions of the draft Contract and other related documents, this Office finds it generally in order. Nevertheless, the following are our further comments and suggestions:

² GPPB Resolution No. 15-2020 dated 28 July 2020.

³ https://gppb.gov.ph/GPPBTSO_Non-Policy/891. Accessed and retrieved on 3 May 2021.



1. In the SCC:

- a) Relating to Transportation, delete 2nd paragraph as this appears to have only repeated the 1st paragraph which relates to the Service Provider shouldering the costs of transporting goods.
- b) Relating to Transportation, 3rd paragraph (now 2nd paragraph), include the following: "In any case, the SERVICE PROVIDER shall inform in writing the Procuring Entity within reasonable time or not later than three (3) calendar days of such delay and the expected date of shipment."
- c) Relating to Transportation, last paragraph, delete "other than those prescribed by INCOTERMS for DDP deliveries" as usually under the Delivered Duty Paid (DDP) Incoterm rules, the seller assumes all responsibilities and costs for delivering the goods to the named place of destination.
- d) Relating to Legal Representations, merge 8th, 9th and 10th paragraphs into one as they are related to read as:

"To the knowledge of the SERVICE PROVIDER, there are no pending or threatened actions or proceedings before any court or administrative agency of any jurisdiction, which may materially or adversely affect the financial condition or operation of the SERVICE PROVIDER or the SERVICE PROVIDER's ability to comply with the terms and conditions of this Contract. If the SERVICE PROVIDER should thereafter learn of the existence or occurrence of the same, the SERVICE PROVIDER undertakes to report such fact to the Procuring Entity within five (5) calendar days therefrom. Failure to do so shall constitute sufficient ground for the cancellation of this Contract and the enforcement of remedies which the Procuring Entity may exercise under this Contract, pertinent laws, rules, and regulations."

- e) Relating to Attorney's Fee, kindly correct the clerical error from ";" to ""
- f) Relating to Notices, ensure that these details are completely filled out.



g) Relating to Terms of Payment, ensure that the blank spaces are likewise filled out, particularly as to the total amount and the percentage of the Contract Price.

2. Please comply with Executive Order (EO) 398, series of 2005, which requires the mandatory submission of current tax clearances for all entities, natural or juridical, which intend to enter into a contract with the government, including government-owned and/or controlled corporations for a full and timely payment of taxes to ensure that the private contracting party is free and clear from tax liabilities to the government.

3. Likewise, we enjoin PDIC to comply with GPPB Circular 01-2021 which reminds all PEs, including government-owned and controlled corporations, to strictly comply with existing rules on transparency, accountability and good governance policies and measures in the procurement process.

4. Ensure also that the purchase is in the Information Systems Strategic Plan (ISSP) duly submitted to and approved by the Department of Information and Communications Technology (DICT).

5. Prior to the due execution of the Contract, kindly ensure that: (a) all blank spaces are properly filled out; (b) the respective written authorizations of the duly authorized representatives of each party are attached, verified to be genuine, and duly executed; and (c) all documents referred to in the draft Contract are properly attached and made integral parts thereof.

6. Further, as stated in the endorsement letter, each member of the Insurance Cluster, including PDIC, shall have a separate contract with the winning bidder. We remind PDIC that pursuant to Section 37.2, the bidding documents which includes the TOR shall form part of the contract. Thus, all members of the Insurance Cluster may simply be given a copy of the signed bidding documents together with those documents enumerated in Section 37.2.3. Nonetheless, given that the decision to execute different contracts with the winning bidder is the decision of the members, this requirement should be clearly stated in the SCC and

A handwritten signature or set of initials in the bottom left corner of the page.



that the separate contract to be executed should strictly be based on the TOR and will be strictly governed by the GCC and SCC.


Please be advised that our review is being rendered solely based on the documents you have provided us. There may be other facts, documents, and circumstances not made known to us, which may materially affect our review.

IV. Conclusion:

Upon strict compliance with the requirement on public bidding under RA 9184, the use of the standard forms issued by the GPPB, and with GPPB Circular 04-2020 (pursuant to Section 6 of RA 9184 and its 2016 RIRR), as well as this Office's additional comments, the draft Contract for the procurement of shared cyber defense solution for the members of the Insurance Cluster may be given due course.

It is understood that this review does not pass upon the financial and technical aspects of the contract, nor the propriety of PDIC entering into it, as these are matters which should be assessed by PDIC Management in the exercise of its business judgment.

Please be guided accordingly.


MARILYN G. ESTARIS
Deputy Government Corporate Counsel
Officer-in-Charge

.....committed to uphold justice
under the rule of law

Handwritten initials or signature at the bottom left corner of the page.

Technical Specifications

Specifications	Statement of Compliance								
<p style="text-align: center;">Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 10px;"> <tbody> <tr> <td style="padding: 2px;">1. Bureau of Treasury</td> <td style="padding: 2px; text-align: center;">1,600 endpoints</td> </tr> <tr> <td style="padding: 2px;">2. Government Service Insurance System</td> <td style="padding: 2px; text-align: center;">4,400 endpoints</td> </tr> <tr> <td style="padding: 2px;">3. Social Security System</td> <td style="padding: 2px; text-align: center;">8,000 endpoints</td> </tr> <tr> <td style="padding: 2px;">4. Philippine Deposit Insurance Corporation</td> <td style="padding: 2px; text-align: center;">1,200 endpoints</td> </tr> </tbody> </table> <p>Phase 1:</p> <ul style="list-style-type: none"> ▪ Threat Intelligence ▪ Security Monitoring and Management ▪ Incident Response <p>Phase 2:</p> <ul style="list-style-type: none"> ▪ Vulnerability Management 	1. Bureau of Treasury	1,600 endpoints	2. Government Service Insurance System	4,400 endpoints	3. Social Security System	8,000 endpoints	4. Philippine Deposit Insurance Corporation	1,200 endpoints	<p style="text-align: center;">Bidders must state below either "Comply" or "Not Comply" against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered.</p> <p>Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.</p> <p style="text-align: center;">Please state here either "Comply" or "Not Comply"</p>
1. Bureau of Treasury	1,600 endpoints								
2. Government Service Insurance System	4,400 endpoints								
3. Social Security System	8,000 endpoints								
4. Philippine Deposit Insurance Corporation	1,200 endpoints								

<p>Notes:</p> <ol style="list-style-type: none">1. Technical specifications and other requirements per attached Terms of Reference (TOR) – revised Annexes D-1 to D-25.2. The documentary requirements enumerated in Items 3.II.C and D of the TOR shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements. <p>Non-submission of the above requirements may result to post-disqualification of the bidder.</p>	
---	--

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position



Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Components (PDF File)

- *The Eligibility and Technical Component shall contain documents sequentially arranged as follows:*

- **Eligibility Documents – Class “A”**

Legal Eligibility Documents

1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages).

Technical Eligibility Documents

2. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).
3. Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).
4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar to the contract to be bid within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

Financial Eligibility Documents

5. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

6. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.
- o **Eligibility Documents – Class “B”**
7. Duly signed valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.
 8. For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos, Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
 9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder.
- o **Technical Documents**
10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
 11. Section VI – Schedule of Requirements with signature of bidder's authorized representative.
 12. Revised Section VII – Technical Specifications with response on compliance and signature of bidder's authorized representative.
 13. Duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

Note: During the opening of the first bid envelope (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary "pass/fail" criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.

- **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**
 - 14. Current Certifications from the manufacturer that Service Provider is a certified/authorized reseller of the brands being offered.
 - 15. Data Sheets and Documentations of the brands and/or services being offered.
 - 16. Latest Forrester Leaders and Gartner Magic Quadrant report for brands offered that has such requirement.
 - 17. List of local sales and technical offices in the Philippines.
 - 18. TIA-942 Rated 3 Facility Certification.
 - 19. Valid SOC 2 Type II Attestation Report or ISO27001 Certification for Managed ICT Services or similar services.
 - 20. Information Security-related certifications of the onsite support engineers.
 - 21. Certifications of the SOC analysts.
 - 22. Certifications of the network and security engineers.
 - 23. List of Local Certified Engineers for the (i) SOAR, (ii) SIEM and (iii) Vulnerability Management, including their respective Certifications on the brand/solution being proposed.
 - 24. List of names of the dedicated 24x7x365 team that will be assigned to the Insurance Cluster, which shall be composed of the following:
 - a. Tier 1 Analyst
 - b. Tier 2 Analyst
 - c. Tier 3 Senior Analyst/Team Lead
 - d. Tier 4 Analyst/SOC Manager
 - 25. Documents regarding the Project Manager:
 - Company ID
 - Certificate of employment
 - List of projects handled.
 - End-User/Client company name of the projects handled.
 - Project Name and Project Duration (Start date and end date).
 - Project Management Certification

26. Documents regarding the SOC Manager/Tier 4 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any two (2) of the unexpired professional certifications in the Insurance Cluster revised Terms of Reference

27. Documents regarding the Team Lead/Tier 3 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any two (2) of the unexpired professional certifications in the Insurance Cluster revised Terms of Reference

28. Documents regarding the Team Member/Tier 2 or Tier 1 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any one (1) of the unexpired professional certifications in the Insurance Cluster revised Terms of Reference

- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**
 1. Business Tax Returns per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.
 2. Latest Income Tax Return filed manually or through EFPS.
 3. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
 4. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
 5. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

Financial Component (PDF File)

- ***The Financial Component shall contain documents sequentially arranged as follows:***
 1. Duly filled out Bid Form signed by the Bidder's authorized representative (sample form - Form No.1).
 2. Duly filled out Schedule of Prices signed by the Bidder's authorized representative (sample form - Form No.2).

Note: The forms attached to the Bidding Documents may be reproduced or reformatted provided the information required in the original forms and other requirements like signatures, if applicable, are complied with in the submittal.

**SHARED CYBERDEFENSE SOLUTION
(REBIDDING)**

Terms of Reference (Insurance Cluster)

Version Number : 4.4

Date : 27 September 2023

Author : Government Service Insurance System
Bureau of the Treasury
Social Security System
Philippine Deposit Insurance Corporation

1. Name and Description of the Project

With the continued evolving nature of cybersecurity risks, the Secretary of Finance has mandated various agencies under the Department to establish a cost-effective defense strategy that will add a layer of defense for the agencies to shield their respective IT systems from potential cybersecurity threats, along with other possible risks and data breaches in the digital landscape.

For this Terms of Reference (TOR), it will cover the Insurance Cluster composed of the Bureau of the Treasury (BTr), Government Service Insurance System (GSIS), Social Security System (SSS), Philippine Deposit Insurance Corporation (PDIC).

2. Project Objective and Scope

The proposed Common Cyber Defense Solution shall require the vendor to provide a two (2) year subscription for the provision of Security Monitoring and Management, Vulnerability Management, Threat Intelligence, and Incident Response. This is primarily focused on the National Institute of Standards and Technology (NIST) Cybersecurity Framework – Identify, Protect, Detect, Respond and Recover.

The Approved Budget for the Contract (ABC) shall be the upper limit or ceiling for the proposal, and shall cover all project costs, including, but not limited to the following:

- Subscription cost that will be based on the number below:

Agency	Servers	Desktops/Laptops	Total
BTr	150	1450	1600
GSIS	400	4000	4400
SSS	200	7800	8000
PDIC	82	1118	1200

- The project shall include project management, consulting, requirements validation, customization, training, integration, training, production deployment, system integration, change management and other out-of-pocket expenses (e.g., transportation allowance, per diem, etc.);
- The Shared Defense subscription shall commence immediately after the Phase 1 implementation of the project.
- Post Go Live support starting from the implementation date; and
- All applicable taxes, service fees and charges (e.g., fund transfers fees, foreign exchange difference)

The proposed Common Cyber Defense Solution for the Insurance Cluster shall be procured in one lot which shall consist of sublots per agency. Likewise, this shall be the basis for awarding per agency.

The pricing shall be uniform for all agencies in the cluster.

Other Requirements

During procurement, the bidder is required to submit respective proposals for all the agencies concerned.

3. Functional and Non-Functional Requirements

The vendor shall respond to each requirement stated herein. Failure to conform to any of the specifications shall be sufficient grounds for disqualification.

I. Functional Requirements

A. Security Monitoring and Management	COMPLIED	REMARKS
A.1 Security Operations Center (SOC)	Y/N	
1. The service provider shall provide a cloud-based SOC for individual agencies with complete Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution that allows for two-way integration with the agencies data sources, capture of near real-time log data, and must perform correlation between data sources during investigation which shall also be accessible by the individual agencies. The licenses for the SIEM and SOAR solutions shall be subscribed per agency during the term of the contract.		
2. The service provider shall set up a cluster level SOC dashboard to have an integrated and high level overview of the cluster agencies security posture.		
3. The SOC, through the SIEM, shall detect and monitor threats, correlate with threat intelligence sources, generate alerts, conduct investigation, and escalate tickets to the agencies on a 24x7 basis, using the Security Operations Center (SOC) platform, inclusive of the security tools to be provisioned for the agencies.		
4. There must be a proper onboarding and integration period between the service provider and the agencies prior to full SOC operation to ensure completeness of SOC visibility and familiarization with the agencies processes and network behavior.		
5. The SOC solution shall have its own ticketing tool for incident ticket generation.		
6. The SOC solution, through the SIEM, shall classify security events based on the following risk rating matrix containing the following information. The report method shall be thru call and/or e-mail:		

Priority	Response Time					Report Time
	Within 2 hours	P1	P2	P3	P4	P5
Within 12 hours	P1	P2	P3	P4	P5	within 30 minutes
Within 24 hours	P1	P2	P3	P4	P5	N/A
24 hours	P1	P2	P3	P4	P5	N/A

- Impact: Severity of the security event to critical assets
- Priority: Based on the impact and severity
- Nature of threat
- Potential business impact
- Remediation recommendations

*Response Time: How soon the security incident must be acknowledged by the service provider

*Report Time: How soon a reference number/ problem ticket must be created by the service provider and received by the agency. The Report Time is included in the Response Time.

7. Monthly monitoring service management:

The service provider shall conduct regular meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement. Regular written reports must also be available to track the status of cases and the assistance needed. Monthly reports shall contain, but not limited to:

- SLA Performance
- Correlated Events Overview
- Correlated Events Graph Distribution Overtime
- Correlated Events and Rules Triggered Summary
- Summary of Incident Ticket per Use Cases Incident Management

8. The service provider shall ensure flexibility and scalability of the agencies SOC platform and shall ingest and process all events sent by the agencies for the SIEM and SOAR requirements including its current and future needs.

9. The service provider shall facilitate SOC security briefing at least once a month for the agencies to present the latest local and international news and updates in Cyber security.

A.2 Managed Detection and Response

COMPLIED

REMARKS

A.2.1 Deployment and Management

Y/N

1. The service provider shall supply Managed Detection and Response services, including the Endpoint Protection / Endpoint Detection and Response (EDR) licenses required for supported endpoints. Supported endpoints refer to Windows endpoints, Windows servers, major Unix and Linux distributions, MacOS, Mobile devices, that is still under support or extended support by the manufacturer.

2. The solutions provider must be capable to deploy the endpoint technology to workstations and servers, including Windows, Mac, Unix and Linux assets, using the agencies or the solutions providers deployment tool, and must support both physical and virtual environments.		
3. For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided. The NDR shall use a standard network interface which may be 1G or 10G. The service provider, however, is expected to make the necessary adjustments during the actual project implementation with the member agency. For NDR with throughput 5G and above, a dual power supply unit (PSU) shall be required.		
4. The solution shall detect and prevent attacks on-premise, for supported and unsupported endpoints, including agency deployments in public clouds, if any, such as, but not limited to Amazon Web Services (AWS), Azure, Oracle Cloud and Google Cloud.		
5. The solution shall be capable to block malicious indicators of compromise (IOCs) and behaviors of compromise (BOCs) automatically with expert review of detections by analysts to ensure there is always human oversight on technology.		
6. The solution shall allow custom enforcement policies to neutralize sophisticated malware and lateral movement utilizing "living off the land" techniques that can potentially evade standard detections, however, ensuring that these custom policies does not impede business operations.		
7. Update of Indicators of Compromise (IOC) and watchlist repository, whenever applicable		

A.2.2 Prevention and Detection	COMPLIED Y/N	REMARKS
1. The solution shall have integration with the SIEM for central monitoring and analysis, including the setup of relevant dashboards such as but not limited to, attacks, threats, endpoints at risk.		
2. The solution should utilize signature-based and/or signature-less detection techniques to protect against known and unknown attacks.		
3. The solution should have Machine Learning and Behavioral Pattern Indicator of Attack (IOA) detection capability.		
4. The solution must be able to detect and prevent the following: <ul style="list-style-type: none"> • exploitation behavior using IOAs and no signatures. • ransomware behavior using Behavior IOA patterns and no signatures. • file-less malware using Behavior IOA patterns. • malware-free tradecraft using Behavior IOA patterns. • BIOS level attacks • Privilege Escalation • Exfiltration 		

• Connection to malicious command and control destinations		
5. The solution must be able to enrich a detected event with its own threat intelligence and not any third-party intelligence including mapping of the technique, tactic and procedure (TTP) against the MITRE ATT&ACK framework.		
A.2.3 Threat Hunting and Response	COMPLETED Y/N	REMARKS
1. The service provider must provide 24x7 Managed Threat Hunting Service, supported by experienced and certified analysts or incident responders for the remote response on endpoint incidents/events		
2. The service provider must have pre-built threat hunting applications and queries		
3. The service provider must be able to get context from indicators such as IP's, URL's, domains, or hashes using the tools within the platform, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others)		
4. The solution shall be able to isolate "at-risk" endpoints, including the blocking the launching of suspicious or malicious applications.		
5. The solution shall allow blacklisting and whitelisting of hashes manually through the solution.		
6. The solution shall provide remote response by administrators, analysts, or incident responders such as containment, deleting files, killing process among others without the need for additional tools or agents.		
7. The solution shall provide root cause analysis of all identified malicious activity.		
A.3 Security Information and Event Management (SIEM)	COMPLETED Y/N	REMARKS
1. The solution shall provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a time period. The agencies must be able to request customized dashboards and ad-hoc reports from the service provider.		
2. The solution shall be capable to support collection of different types of metadata (e.g., logs, security events, network flows, among others) from data sources and shall include log compression and industry standard encryption at rest and in transit to ensure security of captured data from disclosure to disinterested parties.		
3. The data sources ingested by the solution shall include at least the events from perimeter security tools, active directory logs, endpoint protection, and endpoint detection and response tools, including events from sensors that may be deployed by the solutions provider, if needed.		

<p>4. The maximum aggregate daily data ingestion shall be as follows:</p> <table border="1" data-bbox="220 539 1058 772"> <thead> <tr> <th data-bbox="225 546 427 589">Agency</th> <th data-bbox="432 546 1053 589">Daily Event Log Aggregate Size in Gigabytes (GB)</th> </tr> </thead> <tbody> <tr> <td data-bbox="225 595 427 638">BTr</td> <td data-bbox="432 595 1053 638">17 GB</td> </tr> <tr> <td data-bbox="225 645 427 687">GSIS</td> <td data-bbox="432 645 1053 687">24 GB</td> </tr> <tr> <td data-bbox="225 694 427 736">SSS</td> <td data-bbox="432 694 1053 736">48 GB</td> </tr> <tr> <td data-bbox="225 743 427 786">PDIC</td> <td data-bbox="432 743 1053 786">15 GB</td> </tr> </tbody> </table>	Agency	Daily Event Log Aggregate Size in Gigabytes (GB)	BTr	17 GB	GSIS	24 GB	SSS	48 GB	PDIC	15 GB		
Agency	Daily Event Log Aggregate Size in Gigabytes (GB)											
BTr	17 GB											
GSIS	24 GB											
SSS	48 GB											
PDIC	15 GB											
<p>5. The service shall have content packs that are prebuilt configurations for common security use cases that provide sets of rules, alarms, baselines, views, reports, variables, and watchlists.</p>												
<p>6. The service shall provide advanced security capabilities, such as User and Entity Behavioral Analytics (UEBA), natively within its own platform.</p>												
<p>7. The solution must integrate with the global threat intelligence subscription service for data enrichment to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.</p>												
<p>8. The solution must be able to generate and send actionable items to the automation and orchestration tool as well as generate and send alerts to both service provider and agency analysts and incident responders.</p>												
<p>9. The service provider shall ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidences of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required. The logs beyond the retention period shall be archived and given monthly to the agencies in an agreed format.</p>												
<p>10. The service provider shall ensure that the data ingested from the insurance cluster is not shared or disclosed to or accessed by parties not mentioned in the contract unless explicitly granted permission by the cluster.</p>												
<p>A.4 Security Orchestration, Automation and Response (SOAR)</p>	<p>COMPLETED Y/N</p>	<p>REMARKS</p>										
<p>1. The solution must be able to integrate with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass</p>												
<p>2. The solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting</p>												
<p>3. The solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner</p>												

4. The solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization		
5. The solution must be an open architecture that allows for easy connectivity and integrations to any existing system, bringing them all together into a single, contextual language. Integration with other solutions can either be out of the box or customized.		
6. The solution must be able to accelerate security incident processes by automating or semi automating workflows		
7. The solution must include out of the box or customizable playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. Playbooks deployed shall include at least: <ul style="list-style-type: none"> • Phishing enrichment and response • Malware endpoint response • Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc) • Unusual browsing activity • Web attack profiling and blacklisting 		
8. The solution should provide pre-set and customizable KPI metrics to monitor threat response efficacy and team performance.		

B. Vulnerability Management and Penetration Testing		
B.1 Vulnerability Management	COMPLIED	REMARKS
1. The solution provided must be a cloud based service, integrated within the SIEM, that shall give immediate global visibility into where the Agency IT system might be vulnerable to the latest Internet threats and how to protect them.		
2. It should be able to continuously identify threats and monitor unexpected changes in the network before they turn into breaches. The solution can be agentless or agent-based if continuous monitoring is required on specific systems.		
3. The solution should be able to scan systems anywhere in the Agency environment, from the same console whether the asset is on the perimeter, the internal network, or cloud environments (such as Amazon Web Services, Oracle Cloud, Microsoft Azure or Google Cloud) with the ability to create custom reports showing each audience just the level of detail it needs to see.		
4. The solution should be able to identify and prioritize critical vulnerabilities and risks to enable the agencies to prioritize the remediation of the highest business risks using trend analysis, zero-day and patch impact predictions.		
5. The solution should be able to track vulnerability data across hosts and time, to give a better understanding of the agencies security posture. The reports can be changed through existing pre-built templates, without the need to rescan. The reports can be generated on demand or		

scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV												
6. The solution should be able to automatically gather and analyze security and compliance data in a scalable backend, with provisioning additional capabilities as easy as checking a box.												
7. The solution should be able to proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify the agencies immediately, without the need to schedule scan windows or manage scanning credentials.												
8. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum: <ul style="list-style-type: none"> ▪ Identification of the specific vulnerabilities, at risk, and/or compromised assets ▪ Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results 												
B.2 Vulnerability Assessment and Penetration Testing (VAPT)	COMPLETED	REMARKS										
1. Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, authenticated and unauthenticated testing, if any and among others.												
2. The scope of VAPT shall be at least the following: <table border="1" data-bbox="231 1232 1193 1467"> <thead> <tr> <th>Agency</th> <th>Scope</th> </tr> </thead> <tbody> <tr> <td>BTr</td> <td>7 External resources, up to 80 IP addresses</td> </tr> <tr> <td>GSIS</td> <td>20 External resources, 2 mobile apps, up to 80 IP addresses</td> </tr> <tr> <td>SSS</td> <td>25 External resources, 1 mobile app, up to 150 IP addresses</td> </tr> <tr> <td>PDIC</td> <td>8 External resources, up to 80 IP addresses</td> </tr> </tbody> </table>	Agency	Scope	BTr	7 External resources, up to 80 IP addresses	GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses	SSS	25 External resources, 1 mobile app, up to 150 IP addresses	PDIC	8 External resources, up to 80 IP addresses		
Agency	Scope											
BTr	7 External resources, up to 80 IP addresses											
GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses											
SSS	25 External resources, 1 mobile app, up to 150 IP addresses											
PDIC	8 External resources, up to 80 IP addresses											
3. The service provider shall deliver and maintain a vulnerability database with relevant software version upgrades and security policy update recommendations, inclusive of changes to existing and new vulnerability and threat signatures.												
4. The service provider shall provide online reporting and metrics capability: <ul style="list-style-type: none"> ▪ VAPT results/data (including risk, remediation status, and data compromised, if any) and access to historical test result and trend analysis delivered via the service provider's portal shall be accessible to the agencies. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations. 												

<p>5. The service provider shall have predefined fields/templates for the generation of reports, such as, but not limited to:</p> <ul style="list-style-type: none"> ▪ VAPT Report (i.e., Executive Summary, Conclusion for Management Area, and Specific Action Plans) ▪ Security Profiling Results (including reports from automated scanning tools) ▪ Detailed observations and recommendations 		
<p>6. Common Vulnerability Scoring System values:</p> <ul style="list-style-type: none"> • The service provider shall use CVSS v3.0 or later for risk ranking and prioritizing security vulnerabilities. 		
<ul style="list-style-type: none"> • The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML. 		
<p>7. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to:</p> <ul style="list-style-type: none"> • Windows (all versions) • Linux and other Unix flavors (all versions) • Network and security related equipment, whether software or hardware-based • User profile settings • Advanced password analysis 		
<p>8. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:</p> <ul style="list-style-type: none"> • Application servers • Authentication servers • Backdoors and remote access services • Backup applications/tools • Database servers • Active Directory, Lightweight Directory Access Protocol (LDAP) • Domain Name Systems (DNS) • Mail servers and Simple Mail Transfer Protocols (SMTP) • Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS) • Network Time Protocols (NTP) • Remote Procedure Calls • Routing protocols • Simple Network Monitoring Protocol (SNMP) • Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) • Virtual Private Network (VPN) • Web and mobile applications • Web servers 		

C. Threat Intelligence	COMPLETED	REMARKS
1. The solution shall deliver threat intelligence on the following:		
• Brand protection - company names/domain		
• Social media pages		
• External Internet Protocol (IP) addresses		
• Website and mobile application monitoring		
• VIP e-mails		
• Sector monitoring Financial, Government, Insurance, and Healthcare		
• Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes		
• Credit cards		
• GitHub		
• Custom queries		
• 25 Site take downs for each agency during the duration of the contract(i.e., phishing, social media sites, and others) however, should the agency need additional takedowns, this will be provided by the service provider at no additional cost.		
• Scraping databases that contain large amounts of data found in the deep and dark web		
• Third party queries		
• Investigation		
• Threat library		
2. The threat intelligence solution must, at minimally, harvest data from the following open, technical and closed sources types:		
• Mainstream Media (including news, information security sites, vendor research, blogs, vulnerability disclosures)		
• Social Media		
• Forums		
• Paste Sites		
• Code Repositories		
• Threat lists (including spam, malware, malicious infrastructure)		
• Dark Web (including multiple tiers of underground communities and marketplaces)		
• Original research from in-house human intelligence analysts		
3. The solutions provider must be able to:		

<ul style="list-style-type: none"> • Detect and take down servers launching phishing attacks 		
<ul style="list-style-type: none"> • Take down of fake applications that impersonate legitimate ones from app stores. 		
<ul style="list-style-type: none"> • Take immediate action on the agencies behalf and provide all the context to execute rapid take-down of malicious servers, websites or social media accounts. 		
4. The solution shall be capable to detect leaked Personally Identifiable Information (PIIs) and the agencies information from the deep and dark web, social media, and other forms of instant messaging platforms and provide recommended action plan.		
5. The threat intelligence solution must be able to identify fraudulent social media accounts that are impersonating the agencies and its executives		
6. The solution shall monitor the domains and IP addresses that have bad reputation.		
7. The service provider shall consume internal and external threat intelligence into its threat analysis process.		
8. The service provider shall deliver weekly intelligence summary reports on the latest cyber threats, including detected information on the intention to target agencies or other government industries, major activist campaigns, and indications of activism against the agencies, financial and health sector, and the government.		
9. The service provider shall provide a special report or notice to the agencies immediately, should there be any information or detection of targeted attacks against the agencies, the government or the sectors of the concerned agencies.		

D: Incident Response	COMPLETED	REMARKS
1. The service provider shall review the agencies Incident Response Plan (IRP), which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines, such as, but not limited to: <ul style="list-style-type: none"> • Escalation process • Incident containment process • Incident eradication process • Incident recovery process • Incident identification process • Process flow 		
2. The service provider shall act as the Incident Response (IR) Manager and facilitate the six (6) phases of IR. The service provider must be on-call and will conduct the IR activities onsite, as necessary (i.e., in cases of breach). The IRs per agency shall cover 200 accumulated hours per year. Beyond the required 200 hours, the agencies shall shoulder the cost. In case the 200 hours allotted for IR is not fully or not consumed, it can be converted to other services, such as training among others, that the provider can render for information security.		
3. The service provider shall conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness trainings to both technical and non-technical audiences of the agencies. The		

readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.		
4. The service provider shall conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.		
5. The Service Provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.		
6. The service provider shall deliver technical assistance to the agencies CSIRTs during emergency (successful) breach response.		
7. The Service Provider shall have a facility to receive client's reported incident (via authorized point of contact from client) for incidents not captured on the monitoring tool.		
8. The service provider shall deliver network/firewall/web applications breach response.		
9. The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.		
10. The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.		
11. The service provider shall identify indicators of compromise and scan the network to search for other related infected systems.		
12. The service provider shall deliver insider threat investigation, as needed.		
13. The service provider shall deliver employee misconduct investigations, as needed.		
14. The service provider shall deliver incident and investigation reports.		
15. The service provider shall have a certified and recently trained (at least in the past 12 months) in-house cyber security forensics specialist, to support advanced investigation.		
16. The service provider shall assist in the following: <ul style="list-style-type: none"> • Incident handling preparation and execution • Crisis management • Breach communication • Forensic analysis including preservation of evidence for chain of custody requirements • Remediation 		
17. The Service Provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).		

Service Level Agreement (SLA)

1. Acknowledgement SLA - The Acknowledgement SLA Percentage shall be computed per month base on the total number of missed hours exceeding the Acknowledgement SLA guarantee of fifteen (15) minutes per incident

Service Level Target	Description
98%	Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.

2. Incident Response SLA - Time to respond or provide request from when incident or request is reported based on severity level.

Priority Level	Incident Response Time	Reference:
P1 - Catastrophic	Within 60 minutes	From the creation of service ticket up to triage. Triage is when the SOC L2 Incident Responder communicates with the client to further investigate and provide recommendation on how to contain, remediate, and recover from the security incident.
P2 - Critical	Within 90 minutes	
P3 - Marginal	Within 120 minutes	
P4 - Negligible	Within 160 minutes	

Incident Priority	Target Response Time % per Month		Sum of the number of Incidents meeting required Response Time for all days in the month
	1 and 2	3 and 4	
	>=90%	>=80%	

II. Non-functional Requirements

A. Access Management	COMPLIED Y/N	REMARKS
1. All credentials with the service provider shall be stored in a monitored central management system. These are leased to the agencies once strong authentication has been implemented and for the specific task for which it was authorized.		
2. The service provider's solution shall be accessed through a centralized portal, which enforces session timeouts, mandates the use of multi-factor authentication (MFA), and provides anomaly detection for monitoring user behavior.		
3. The service provider shall maintain logical access controls which are role-based, including principles of least privilege and segregation of duties.		
4. All passwords must have a minimum of fifteen (15) characters. Passwords must be changed every ninety (90) days and cannot be the same as the prior three (3) passwords. The service provider's system must mask passwords when entered and store password files separately from the application system data. Only encrypted hashes of passwords may be stored and transmitted.		
5. All access from the service provider's managed endpoints to sensitive resources shall be done via VPN configured with MFA. Opportunistic Transport Layer Security (TLS) is configured by default for e-mail. Remote hardware is managed by comprehensive enterprise management software that allows for maintenance and access control management.		
6. The service provider shall provide physical and environmental controls at the primary and secondary sites for this project.		
7. The agencies data shall be logically separated by using unique tagging to ensure segregation of data from the other agencies. The agencies should retain as the legal owner of the data processed and managed by the service provider.		
B. Training and Other Requirements	COMPLIED Y/N	REMARKS
1. The service provider should facilitate at least once a year Continual Service Improvement (CSI) workshop with client for possible improvement of service through process, people and technology.		
2. The service provider should provide security advisories with the client for the cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.		
3. The service provider shall conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on each Government Agency based on the NIST or CIS Controls.		

C. Service Provider's Qualification and Requirements <i>Note: Submission of required documents shall be during the submission of bids.</i>	COMPLETED Y/N	REMARKS
1. The service provider must be a certified/authorized reseller of the brand(s) being offered and shall submit a valid, certification from the manufacturer(s).		
2. The service provider must submit the following certifications: a. For Cloud based Security Operations Center (SOC), that this is hosted in a provider categorized as a leader either in the latest Forrester Wave™: Public Cloud Development And Infrastructure Platforms report or Gartner Magic Quadrant for Cloud Infrastructure and Platform Services; b. For Endpoint Detection and Response (EDR), that solution is categorized as a leader either in the latest Forrester Wave™ report for Enterprise Detection and Response or Gartner Magic Quadrant for Endpoint Protection Platforms; c. For Security Information and Event Management (SIEM), the solution provided is categorized as a leader in the latest Forrester Wave™ report for Security Analytics Platforms or Gartner Magic Quadrant for Security Information and Event Management (SIEM).		
3. The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service), with a pool of at least 20 IT or Information Security related certified onsite support engineers within Metro Manila. A list of the support engineers shall be provided with their required qualifications, as stated in item D. Personnel Qualifications / Requirements.		
4. The service provider must have sales and technical offices located in the Philippines. The service provider should submit the list of their sales and technical offices in the Philippines, including the complete address and contact details. This is subject for actual site visit to the facility.		
5. The SOC can be provided on the cloud or within the premises of the service provider. Should the Security Operations Center (SOC) with their SOC analysts be on premise, they should be housed in a Data Center with TIA-942 Rated 3 Facility Certification or any equivalent third party assessment indicating the capability of the SOC to provide the required security, scalability, stability and high performance. The proof of compliance shall be submitted. 6. However, if the service provider's SOC will be implemented through a cloud service provider (CSP), the SOC platform must be guaranteed with at least 99.9% uptime or availability. The proof of compliance shall likewise be submitted.		
7. The service provider's SOC Analysts must have at least one or more of the following certifications: Certified Ethical Hacker (CEH), CyberSec First Responder, Information Technology Infrastructure Library (ITIL), or any relevant product certification to the security products of the platform offered by the Service Provider.		
8. The service provider must be at least five (5) years in Security and ICT Industry and must have more than three (3) years of experience in providing SOC services. The Service provider must have a SOC 2 Type II Attestation Report or ISO 27001 certification for		

Managed ICT Services or similar, done at least in 2021, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in place.		
9. The prospective bidders shall be required during the post qual evaluation to demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.		

D: Personnel Qualifications/Requirements	COMPLETED	REMARKS
<p>1. The service provider must have at least Two (2) local Certified Engineer on each of the following security tools below:</p> <ul style="list-style-type: none"> • SOAR • SIEM • Vulnerability Management <p>The certification must be the same with the brand that is being proposed.</p>		
<p>2. The service provider must assign a dedicated local SOC Manager that oversees the SOC and conducts regular monthly service performance review and reporting to client's management. A monthly service performance report shall be submitted and discussed by the SOC Manager. It shall contain the following:</p> <ul style="list-style-type: none"> • SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Over Time • Correlated Events and Rules Triggered Summary • Summary of Incident Ticket per Use Cases Incident Management <p>The service provider must also assign a dedicated Project Manager that will oversee the project implementation. A monthly project monitoring report shall be submitted and discussed by the Project Manager until the completion of the Phase I and Phase II of the project as defined in the Delivery Time/Completion Schedule. The Project Manager shall be required to be onsite in any agency by schedule, if necessary.</p>		
<p>3. The service provider must submit the following for all the personnel to be assigned to the cluster, and failure to submit the any of the requirement below is subject for disqualification.</p> <ul style="list-style-type: none"> • Resume/CV of the Proposed Personnel • Company ID • Certificate of employment 		
<p>4. The service provider must have a dedicated 24x7x365 team assigned to the cluster, composed of at least:</p> <ul style="list-style-type: none"> • 2-Tier 1 analyst who will be responsible for the following tasks: <ul style="list-style-type: none"> 1. Monitoring via existing SIEM/Analytics Platform 2. Funneling of alerts (noise elimination) 3. Incident Validation 4. Case Management 		

<ul style="list-style-type: none"> 5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up 6. General Communication 7. Weekly Summary Reports • 1-Tier 2 analyst who will be responsible to conduct further analysis and decides on a strategy for containment. <ul style="list-style-type: none"> 1. Proactive Searches/ Threat Hunting 2. Qualification of Incident Priority/Severity 3. Investigation via SIEM/Analytics Platform and other accessible sources 4. Rule Tuning 5. Ad hoc Vulnerability Advisory & Research 6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations • 1-Tier 3 senior analyst who will be responsible to manage critical incidents. Tier 3 analysts are also responsible for actively hunting for threats and assessing the vulnerability of the business. <ul style="list-style-type: none"> 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules • 1-Tier 4 analyst or the SOC manager, who will be in charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. The SOC manager will also be responsible for the management of the MSOC operations for the agency and cluster. 		
<p>5. The service provider should ensure that there will be alternate personnel deployed to the cluster should the primary personnel be unavailable for whatever reason. The service provider shall be allowed to augment the dedicated personnel with foreign support staff from partners (hybrid) as long as the minimum staffing requirements are met.</p>		
<p>6. Qualifications</p> <ul style="list-style-type: none"> • Project Manager: <ul style="list-style-type: none"> • Must be with the service provider's organization at least one (1) year before the bid opening • Has handled project management for at least two (2) financial corporations or should have at least two (2) successful project implementations of at least Php 20M in amount in the last two (2) years. • Must provide a list of projects handled in the last 5 years, indicating the Project Name, Project Duration (Start date and end-date) and Contact Person with details for verification. • Must have a valid project management certification 		

<ul style="list-style-type: none"> • SOC Manager/Tier 4 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening • Has performed and managed three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least five (5) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience. • Has any two (2) of the following unexpired professional certifications: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), GIAC Security Essentials (GSEC), GIAC Continuous Monitoring (GMON), GIAC Certified Detection Analyst (GCDA), GIAC Web Application Penetration Tester (GWAPT), GIAC Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Intrusion Analyst (GCIA), Cisco Certified Network Associate (CCNA), Information Technology Infrastructure Library (ITIL), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Network Defense Architect (CNDA), CyberSec First Responder (CFR), CompTIA Security+, Certified Vulnerability Assessor (CVA), Offensive Security Certified Professional (OSCP), Certified Information System Security Professional (CISSP), Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), GIAC Exploit Researcher & Advanced Penetration Tester (GXPN), EC-Council Licensed Penetration Tester (LPT) Master, Certified Penetration Tester (CPT), Certified Expert Penetration Tester (CEPT), Certified Mobile and Web Application Penetration Tester (CMWAPT), CompTIA PenTest+, Certified Payment Card Industry Security Implementer (CPISI), or other security-related certifications. 		
<ul style="list-style-type: none"> • Team Lead/Tier 3 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening • Has functioned as lead in the performance of three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least five (5) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience • Has any two (2) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications. 		

<ul style="list-style-type: none"> • Team Member/Tier 2 or Tier 1 Analyst: <ul style="list-style-type: none"> • Must be with the service provider's organization one (1) year before the bid opening • Has performed three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least three (3) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience • Has at least one (1) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications. 		
---	--	--

4. Delivery Time/Completion Schedule

The Project must be implemented by phases. Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response , 120 working days from the issuance of the Notice to Proceed, Phase 2- Vulnerability Management, 90 working days from the issuance of the Notice to Proceed . Commencement date will be from the receipt of Notice To Proceed (NTP) by the winning bidder. The vendor must therefore provide a project schedule which should present the project milestones and deliverables at each milestone. License subscriptions will start upon implementation.

All deliverables shall become the property of the concerned agencies.


5. Payment Milestone

The Service provider shall be paid upon receipt of its deliverables, based on the submitted Project Schedule and issuance of the Certificate of Acceptance from the Insurance Cluster. The Service Provider shall be paid based on the following milestones:

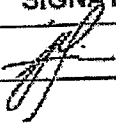
Milestone	Percentage of the Total Contract Price
Year 1:	
Upon implementation of Threat Intelligence, Security Monitoring & Management and Incident Response for the Insurance Cluster (Phase 1)	15%
After Phase 1 and upon implementation of Vulnerability Management for the Insurance Cluster (Phase 2)	15%
After Phase 2 and upon full implementation of the Shared Defense Solution and Insurance Cluster Issuance of Certificate of Completion and Acceptance of the License subscription covering the first 12 months (1st Year)	20%
Year 2:	
Two (2) semi-annual payments at 25% each	50%
TOTAL	100%

SHARED CYBER DEFENSE SOLUTION Project

Bureau of the Treasury:

NAME	SIGNATURE
Mr. David Andrei P. de Mesa	


Government Service Insurance System:

NAME	SIGNATURE
Mr. Jonathan Pineda	




Revised March 10-13

Social Security System:

NAME	SIGNATURE
Ms. Jocelyn Dela Peña	



Philippine Deposit Insurance Corporation:

NAME	SIGNATURE
Ms. Maria Belinda San Jose	 Digitally signed by San Jose Maria Belinda Lani Data: 2023.03.27 20:17:47 +0800

