



LANDBANK

SERVING
THE NATION

SUPPLEMENTAL/BID BULLETIN NO. 2
For LBP-HOBAC-ITB-GS-20230725-01

PROJECT : **Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster**

IMPLEMENTOR : **HOBAC Secretariat Unit**

DATE : **October 6, 2023**

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

- 1) The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.
- 2) The Terms of Reference (Annexes D-1 to D-25), Technical Specifications (Section VII) and Checklist of Bidding Documents (Item No. 12 of Technical Documents and Item Nos. 26 to 28 of Other Documents to Support Compliance with Technical Specifications) have been revised. Please see attached revised Annexes D-1 to D-25 and specific sections of the Bidding Documents.
- 3) The submission and opening of bids is re-scheduled on October 13, 2023 at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams.
- 4) Responses to bidder's queries/clarifications per Annex H-1 to H-21.


ATTY. HONORIO T. DIAZ, JR.
Head, HOBAC Secretariat Unit

Technical Specifications

Specifications	Statement of Compliance								
<p>Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster</p> <table border="1" data-bbox="220 1406 826 1601"> <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>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>
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								

Notes:

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.

Non-submission of the above requirements may result to post-disqualification of the bidder.

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.
- **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.
- **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:		

		Impact				
Response Time		High	Medium	Low	Very Low	Report Time
Priority	Within 2 hours		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

- 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

YN

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 		

<ul style="list-style-type: none"> • 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.		

4. The maximum aggregate daily data ingestion shall be as follows:

Agency	Daily Event Log Aggregate Size in Gigabytes (GB)
BTr	17 GB
GSIS	24 GB
SSS	48 GB
PDIC	15 GB

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.

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

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.

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.

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.

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.

A.4 Security Orchestration, Automation and Response (SOAR)

COMPLIED
Y/N

REMARKS

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

2. The solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting

3. The solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner

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	COMPLIED 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		

<p>scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV</p>												
<p>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.</p>												
<p>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.</p>												
<p>8. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum:</p> <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 												
<p>B.2 Vulnerability Assessment and Penetration Testing (VAPT)</p>	<p>COMPLIED Y/N</p>	<p>REMARKS</p>										
<p>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.</p>												
<p>2. The scope of VAPT shall be at least the following:</p> <table border="1" data-bbox="194 1167 1259 1424"> <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											
<p>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.</p>												
<p>4. The service provider shall provide online reporting and metrics capability:</p> <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)

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	

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: 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>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: <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 		

<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. 		

• Team Member/Tier 2 or Tier 1 Analyst:

- 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, GXP, 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	

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 Cust Date: 2023.06.27 20:17:47 +0800