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

Revised ANNEX D-1

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)

Ranked   Entry D-1

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:		

Kaisel Arturo 0-3

	Response Time					Report Time
Priority	Within 2 hours		P2	P3	P4	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

- o Impact: Severity of the security event to critical assets
- • Priority: Based on the impact and severity
- o Nature of threat
- o 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
- o Correlated Events Overview
- ▪ Correlated Events Graph Distribution Overtime
- o 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:
  • 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		

	COMPLIED (Y/N)	REMARKS
• 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.		

Keuued Anny 0-6

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

	COMPLIED Y/N	REMARKS
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		

Review Annex D - 7

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: • 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		

	COMPLIED Y/N	REMARKS
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: ▪ 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, authenticated and unauthenticated testing, if any and among others.		

2. The scope of VAPT shall be at least the following:

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: ▫ 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.		

Routed Annex B-9

5. The service provider shall have predefined fields/templates for the generation of reports, such as, but not limited to:
   • 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		

6. Common Vulnerability Scoring System values: • The service provider shall use CVSS v3.0 or later for risk ranking and prioritizing security vulnerabilities.		
• The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML.		

7. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to:
   • 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		

8. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:
   • 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		

Revised Annex D- IV

Batch Arrow D-II

C. Threat Intelligence	COMPLIED	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:		

		COMPLIED Y/N	REMARKS
	• Detect and take down servers launching phishing attacks		
	• Take down of fake applications that impersonate legitimate ones from app stores.		
	• 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: • 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		

Revised March 17-12

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: • 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).		

Page 14 of 55

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

Volku Annex II - 14

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.		

Ranked Array 0-15

C. Service Provider's Qualification and Requirements Note: Submission of required documents shall be during the submission of bids.	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		

Revised Annex B- IV

		COMPLIED y/n	REMARKS
	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
1.	The service provider must have at least Two (2) local Certified Engineer on each of the following security tools below: • SOAR • SIEM • Vulnerability Management The certification must be the same with the brand that is being proposed.		
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: • 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 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.		
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. • Resume/CV of the Proposed Personnel • Company ID • Certificate of employment		

4.	The service provider must have a dedicated 24x7x365 team assigned to the cluster, composed of at least:
	• 2-Tier 1 analyst who will be responsible for the following tasks:
	   1. Monitoring via existing SIEM/Analytics Platform
	   2. Funneling of alerts (noise elimination)
	   3. Incident Validation
	   4. Case Management		

Portal Annex D - D

    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.
    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.
    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.

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.

6. Qualifications

- Project Manager:
    - 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: - 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.		
- Team Lead/Tier 3 Analyst: - 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, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.			

Rorud Anam 17 · 10

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	

Philippine Deposit Insurance Corporation:

NAME	SIGNATURE
Ms. Maria Belinda San Jose	Digitally signed by San Jose Maria Belinda Cruz Date: 2023.09.27 20:17:47 +08'00'

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

DATE	September 11, 2023
PROJECT IDENTIFICATION NO.	ITB-GS-20230725-01 Shared Cyber Defense Solution for Insurance Cluster
PROJECT NAME	Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster
PROPONENT UNIT/TECHNICAL WORKING GROUP	Insurance Cluster

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by BlueVoyant)	TWG's RESPONSES
1.	Not specified in the submitted queries	May we request for a complete list of domains, social media accounts and thenumber of VIP emails that will be monitored?	This information will ONLY be provided to the winning bidder.
2	Not specified in the submitted queries	May we request for an asset list per agency?	This information will ONLY be provided to the winning bidder.
3	Not specified in the submitted queries	May we request for a list of the Operating Systems of the endpoints of each agency?	This information will ONLY be provided to the winning bidder.

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by Cloud 4C)	TWG's RESPONSES
1	p19 Annexes, Sec A.3.4	Daily Event Log Aggregate Size in Gigabytes (GB) includes both servers andlaptop/desktop?	Yes.
2.	p21 Annexes, Sec B.2.2	Insurance Commission (IC) is mentioned to be part VAPT scope but not in other scopes?. Is IC part of the scope of this bid?	IC is not part of the project anymore. The requirement shall be : 2 The scope of VAPT shall be at least the following
3.	p29, Annexes, D.4	Tier 1-4 Analysts outside or not part of the required pool of at least 20 IT or Information Security related certified onsite support engineers within Metro Manila?	Section D.4 specifies the minimum number of IT personnel with the required technical qualifications. The service provider must have a pool of at least 20 IT personnel with specified technical skills who are onsite support engineers within Metro Manila.
4	p29 Annexes, sec D.4	Are the required personnel like Tier 1-4 Analysts or Project Manager be shared across all	There will be at least 5 dedicated personnel assigned to the cluster, not per agency as required in the TOR. There will also be a dedicated PM to be assigned to

For item 2, the response table:

Agency	Scope
ETI	7 External resources, up to 60 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 60 IP addresses

ANNEX H-1

		four Insurance Cluster members? Or will there be separate & dedicated Tier 1-4 Analysts & PM for each of the four Insurance Cluster members?	the cluster who will be responsible for the project implementation.
5.	p28, Annexes, C.6	If the service provider's SOC will be implemented through a cloud service provider (CSP), will the Analysts be required to be in-country or on-premises?	The Analyst should be in- country since they should be in the same location where the SOC of the service provider, which is required to be a 24 x 7 x 365 local technology operation center per Section C.3
6	Not specified in the submitted queries	Out of the P304M ABC what is the respective budget of each of the four Insurance Cluster members?	The total ABC is proportional to the total number of endpoints per Insurance Cluster member.
7	Not specified in the submitted queries	Will Service Provider assume to replace any (or all) existing security tools that is required in this TOR (SIEM, EDR, TI, etc.) of each (or all) Insurance Cluster member?	No. The Service Provider shall install their solution without replacing the existing security tools of the Insurance Clusters members. In case, there will be conflict, the replacement of the existing tools will be subject to the evaluation of the member agency during implementation.
8.	Not specified in the submitted queries	Can BAC or the four Insurance Cluster members share their existing security tools that is required in this TOR (SIEM, EDR, TI, etc.)?	The bidder is expected to provide all required solutions in the project. Other security solutions that will be onboarded in the SOC will be provided during the implementation of the project.
9.	Not specified in the submitted queries	Project Manager must be onsite? a. Also With reference to the Technical Specification of the TOR under Personal Qualification/Requirements - May we request for the BAC to consider "local with hybrid support" This reference to the security analysts, certified engineers, SOC managers, and project managers. Benefits: IC agencies to ensure to receive the highest SLA quality of service with proactive contingency in place thus eliminating any potential disruption and/or risk(s) b. We also like to request for the extension of the submission to October 16, 2023.	The Project Manager should be able to visit any agency, when required. 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 The submission and opening of Bids is scheduled on October 13, 2023

ANNEX H-2

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by Crayon Software ExpertsPhilippines Inc.)	TWG's RESPONSES
1	On Billing and Payment	How is the treatment for the billing and payment. Do we do this separately per agency? Or do we bill Landbank?	Per member agency
2	On Payment Terms	May we request to have a separate payment term for the subscription instead of including it in the per milestone schedule? Usual payment terms for subscription are upfront and annual	No.
3.	Bid submission extension	Can we extend the bid submission on October 6, 2023?	The submission and opening of Bids is scheduled on October 13, 2023

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by EY Philippines)	TWG's RESPONSES
1	Not specified in the submitted queries	Technical Questions	
		SOC	
		1 Is there a CMDB in place with all the asset details, role and criticality?	1 This information shall ONLY be provided to the winning bidder. The non-availability of CMDB shall be addressed by the member agency during the implementation of the project in their respective agency
		2. Do you have any DR setup for Data center. If yes, does it comes under thescope of monitoring?	2. This information shall ONLY be provided to the winning bidder. The proposal of the service provider will be based on the number of endpointswithin the agency's corporate network regardless of their physical location.
		3. Post 1st year, the logs are to be shared with the agencies. Please confirm the mode of transfer and clarify who will own the infrastructure for the transfer of raw logs.	3. The storage of the raw logs after one (1) year will be the responsibility ofthe member agency. The mode of transfer shall be discussed during project implementation with the member agency.
		4 Average number of security incidents handled per day.	4 This information shall ONLY beprovided to the winning bidder.
		5 Will the license of SIEM be owned byyou?	5. The licenses for the SIEM and SOAR solutions shall be subscribed per agency during the term of the contract.

ANNEX H-3

			6. Is there a requirement to store all logs locally?	6 No, there is no requirement to store the logs locally.
			7. What are the Legacy assets that are inscope?	7. This information shall ONLY be provided to the winning bidder.
2.	Not specified in the submitted queries	**Vulnerability Management** 8 Is there any specific scanning requirement such as Authenticated / Unauthenticated? Authenticated scanning will require to provide credentials with specific privileges such as (Admin for Windows and equivalent to root permissions or 500 ÷ for UNIX/LINUX)	8. VAPT shall include authenticated and unauthenticated scans.	
			9 Does the client have any existing SLAfor fixing vulns of different severities? What expectation does the client havefor remediation of found vulnerabilities? (Remediation Consulting/ Remediation Tracking/ Remediation validation/ Complete remediation activities)?	9. This information shall only be provided to the winning bidder. Appropriate implementation of remediation, including monitoring/tracking and validation shall be established during project implementation per member agency
			10. Is there an internal threat data collection process in place?	10. This information shall ONLY be provided to the winning bidder.
3.	Not specified in the submitted queries	**Network** 11. What is the throughput per agency?	11. This information shall ONLY beprovided to the winning bidder.	
			12. What is the network interface required?	12-13. 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
			13. Do you require a dual PSU for theNDR appliance	

4.	Not specified in the submitted queries	**VAPT** 14. What is the approximate workload(number of web applications) for testing? 15. What is the approximate number ofservers, firewalls, routers, or othernetwork devices on the internal corporate network?	14. This information shall ONLY beprovided to the winning bidder 15 This information shall ONLY beprovided to the winning bidder
5.	Not specified in the submitted queries	**Non-technical questions** 1 Why is IC included in the list for VAPT Scanning?	1. IC is not part of the project anymore. The requirement shall be: 2. The scope of VAPT shall be at least the following:

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

		2 Where can we get Annex D1 toD25?	Can be provided by LANDBANK Procurement Department thru email
		3 Can we have the documents digitally signed or do we need tohave a wet signature?	Either of the two is acceptable
		4 Do we need to counter-sign eachpage?	No, only those portions as required in the bidding documents, must be signed by authorized representative/s as designated per Secretary's Certificate
		5 Is consortium allowed?	Yes, in the form of Joint Venture Agreement by and between multi-parties
		6. Kindly confirm indicate whether theprice mentioned is inclusive or exclusive of VAT	The ABC is VAT inclusive
		7 Can we request to insert our assignability clause? 8. Can we propose revisions in GCC 9. Clauses, like limitations on liability? 10. We propose to qualify as gross negligence and not mere negligence. 11. We request to include our standard provision on termination when already prohibited by law or professional obligations.	7-11 For the draft contract, if possible we do not accommodate any change inany provisions because this would entail further review of our Legal Sector and the OGCC.
		12. In the RFP document we see two pricing tables with detailed breakdowns asking	There are two (2) schedules provided in the bidding documents. however, the bidder may choose which is

ANNEX H-5

			for goods procured locally (Philippines) or goods procured from abroad. A quick check here this table is relevant for licenses and not for labor cost?	applicable.

for goods procured locally (Philippines) or goods procured from abroad. A quick check here this table is relevant for licenses and not for labor cost? — applicable.

13. For labelling of archived/compressed files, please clarify if it should be the last six (6) digits or last seven (7) digits of the bidding reference number — Please refer to Bid data Sheet ITB Clause 15 of Bidding Documents

14. We request to reasonably discuss for any out-of-scope services — 14. The winning bidder is required to deliver the in-scope requirements

15. We request that additional scope of services should be mutually agreed — 15. The winning bidder is required to deliver the in-scope requirements

16. In the subcontracting there is discrepancy in the statement — 16. In Section III, under Clause 7, states that subcontracting is not allowed

17. Can we request an extension on the submission of the bidding proposal — 17. The submission and opening of Bids is scheduled on October 13, 2023

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by ePLDT)	TWG's RESPONSES
1.	Under A.2.1 Deployment and Management Item no. 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."	Part of our offer is to provide NDR solution for non-supported systems: 1. May we know how much throughout should we consider per agency? 2. What is the network interface required for NDR appliance? 3. Will you require dual PSU for the NDR appliance?	1. This was not specified in the TOR. This information should be assessed during the actual project implementation with the member agency. 2-3. 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.

ANNEX #-G

| 2 | Under A.3 Security Information and Event Management (SIEM). Item no.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." | Aside from the Daily Event Log Aggregate Size per agency. May we kindly request for the list of log/data sources per agency? (OS, server, firewall, etc.) | This information will ONLY be provided to the winning bidder |

ITEMNO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by Information TechnologySecurity Distribution, Inc.)	TWG's RESPONSES
1.	In Functional requirements, under Section 1 of A.4 Security Orchestration, Automation and Response (SOAR).	What are the technologies included in Security Operations? What is the level of automation that you are expecting?	The technologies are already stated in the TOR: 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. Level of automation should be subject to the actual project implementation per member agency.
2.	In non-functional requirements, statement number 1 of Access Management	Is there a need for single authentication system or can each major platform can have its own authentication system that can address the capabilities for the Access Management?	No.
3.	In non-functional requirements, statementnumbers 5 and 6 of C. Service Provider's Qualification and Requirements	May we request both statements to be combined into one statement and indicated that vendor can either comply with on premise or cloud platform requirements?	The requirements specified in Section 5& 6 under Non-Functional Requirements A. Access Management are clear. Thus,no need to combine them.

ANNEX H-7

4.	In non-functional requirements, statement numbers 9 of C. Service Provider's Qualification and Requirements	Since this is a post qualification requirement, may we request this statement to be removed and placed in the post-qualification documents?	Yes. This is a requirement to be complied with during the post-qualification. However, there is no need to transfer this requirement under post-qualification documents
5.		Part of the items to be submitted as included in the checklist are "List of Local Certified Engineers for the (i) SOAR, (ii) SIEM including their respective Certifications on the brand/solution being proposed" as well as "List of names, credentials, and projects they were involved in for the dedicated 24x7 x 365 team that will be assigned to the Insurance Cluster" Because of Data Privacy, we cannot initially disclose the details of our staff aswell as the projects they were involved in,not until the finalization of contract. Is it alright to just provide their certification and credentials without showing their names? And may we request as well to just provide the description of the project and not the company name?	The disclosure of the required information is critical for the proper assessment /evaluation of the bidder with the Lowest Calculated and Responsive Bid.

ITEMNO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by Micro D International)	TWG's RESPONSES
1	In reference to Section C Service Provider's Qualification and Requirements;	Item 2. May we request to relax this requirement to include non-leaders from Gartner & Forrester (3rd Party) solutions as the required deliverable of the project is based on Managed Services SLA offering and not the product market perception of a 3rd Party like that of Gartner. Our service offering is focused on building and packaging capabilities and service outcomes. and we believe that the products and technologies that underpin these offerings are secondary to the primary deliverable, which is to deliver a successful customer service outcome	No

2.	On Bid Submission	In reference to the bid submission on September 22, 2023, may we request for an extension to October 13, 2023?	The submission and opening of Bids is scheduled on October 13, 2023
3.	On Personnel Qualifications /Requirements	May we know if we can submit CV's of our Technology Partners, including Distributor engineers who will be deployed in the project	The personnel should be employed by the bidder.

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by Netpoleons)	TWG's RESPONSES
1	Not specified in the submitted queries	**Technical Questions:** 1 Will license need to be owned by each agency or by Managed Service Partner? 2 Start Date of license 3. Understand that "Third Party Queries" have been included as part of C1 - Threat Intelligence. We would like to clarify what details/use case is needed for this requirement.	1. The licenses for the SIEM and SOAR solutions shall be subscribed per agency during the term of the contract. 2. License subscriptions will start upon implementation of the Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response as indicated in the Project Milestone, which is expected to be delivered within, 120 working days from the issuance of the Notice to Proceed. This information shall ONLY be provided to the winning bidder. The details and use cases shall be discussed during the actual project implementation with the member agency.

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by TIM)	TWG's RESPONSES
1.	Under A.2 Managed Detection and Response > A.2.1 Deployment and Management > Item 2.	Regarding the deployment of MDR, may we know what deployment tool the agencies will provide to be used?	Agencies can use their available software deployment tool, if any, or deployment through AD GPO. Otherwise, the service provider can provide a tool to deploy agents faster.
2	Under B. Vulnerability Management and Penetration Testing > B.2 Vulnerability Assessment and Penetration Testing (VAPT) Item 2. "The scope of VAPT shall be at least the following:"	Can we request the "at least" to be omitted, so the stated numbers of External Resources and IP address is already defined.	No. Because the bidder can always provide more than the minimum requirements.

ANNEX H-9

3.	Under B.1 Vulnerability Management.	Can we request for the list of scan targets/asset (ex endpoints, servers, web apps, containers) and the total number of assets (per asset type)	This information will ONLY be provided to the winning bidder.
4.	Under D. Incident Response > item 15.	May we know what type of reference or document would you require to be provided?	The name of the personnel, including the Certificate of trainings attended related to cyber-security forensics, shall be submitted during post-qualification
5.	Under II. Non-Functional Requirements > A. Access Management > Item 1.	**Question 1:** What does it mean when you say "leased" to the agencies? Is there any specific solution you require for Access Management? **Question 2:** Since there are multiple solution stacks in this project, can we ask if "A. Access Management" in general is only referring to the SIEM?	The project is for the procurement of subscriptions to managed services. Thus, it is possible that the member agencies will just "lease" the accounts. This technical requirement applies to all services/system that will require user access.
6.	Under II Non-Functional Requirements > A. Access Management > Item 2.	We assume that MFA will be provided by the Insurance Cluster Agencies. May we know what is the MFA that will be used by the Agencies?	The MFA should be included in the proposed solution. During project implementation, the winning bidder may use/integrate the existing MFA of the member agency, if any, subject to approval of the member agency. This information shall ONLY be provided to the winning bidder, if needed during project implementation.
7.	Under II. Non-Functional Requirements > A. Access Management > Item 6.	Since the requirement is Cloud Based SOC, can this refer to the Cloud Based SOC as the Primary and the SOC Analyst location is the secondary site.	The requirement pertains to the physical and environmental controls at the offices/building where the primary and secondary SOC is located.
8.	Under C. Service Provider's Qualification and Requirements > Item 1	Is the Manufacturer's Certificate that will be provided only refers to the brand that will be provided to the agencies? Brands for (1) MDR, (2) SIEM, (3) VM, (4) SOAR and (5) Threat Intelligence	Yes
9.	Under C. Service Provider's Qualification and Requirements > Item 2	Can we provide either Forrester Wave Report or Gartner Magic Quadrant for the 3 requirements?	Yes. The requirement is Forrester Wave OR Gartner
10.	Under C. Service Provider's Qualification and Requirements > Item 3	For the pool of 20 IT personnel, what are the documents needs to be submitted? Can we submit at least their certifications only?	Please refer to the documents that will be submitted during post-qualification.
11	Under D. Personnel	Can we clarify what does "dedicated" means? Is he only should be assigned to the cluster and cannot handle any other customers?	Dedicated means "exclusively assigned" to the Insurance Cluster.

ANNEX H-10

	Qualifications/Requir em ents > Item 2		
12.	Under D Personnel Qualifications.	The 1 Tier-4 Analyst/SOC Manager, 2 Tier-1, 1 Tier-2, and 1 Tier-3 Analysts are dedicated for the whole Insurance Cluster already and not per agency?	Dedicated to the Insurance Cluster
13.	Under D. Personnel Qualifications/Requir em ents > Item 3	The submission of CV, Company ID and Certificate of Employment is only applicable to SOC Manager, Analyst and Project Manager? While for the 20 IT Personnel, Certificate will suffice?	Please refer to the documents that will be submitted during post-qualification.
14	Under D. Personnel Qualifications/Requir em ents > Item 6 > ProjectManager	For Project Manager Certificate, would either Certified Associate in Project Management (CAPM) or Project Management Professional (PMP) be acceptable?	PMP certification will be required as this certification ensures that the Project Manager has extensive experience and advanced project management skills and capabilities.
15.	Under B. Training and Other Requirements	How many attendees will be inclusive in the training?	The bidder should accommodate up to ten (10) attendees per agency in the training.
16	Not specified in the submitted queries	Will the implementation for each Agency start simultaneously?	Yes, more or less. The winning bidder should be able to complete the implementation of Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response for all the members of the Insurance Cluster within 120 working days from the issuance of the Notice to Proceed. Notice to Proceed shall be issued by each of the agencies.
17	Under 2. Project Objective and Scope > Bullet 3. "The Shared Defense subscription shall comme nce immediately after the Phase 1 implementation of the project."	Does this mean the 2 years subscription, will start on the day 1 of implementation?	Yes. Upon the implementation of Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response for all the members of the Insurance Cluster.
18.	Not specified in the submitted queries	Who will release the NTP? Each Agency? Or Just Landbank? We would request the NTP for all the Agency will start at the same time.	NTP shall be released by the member agencies at the same time.
19.	Not specified in the submitted queries	Due to the very high complexity of the project. Can we request for at least 3 weeks extension (October 13, 2023) for the bid submission?	The submission and opening of Bids is scheduled on October 13, 2023

ANNEX H-11

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (raised by Trends and Technologies Inc.)	TWG's RESPONSES
1	Page 3, Section VII Technical Specification. Terms of Reference under A.1 Security Operations Center (SOC) Item 2 The service provider shall set up a cluster level SOC dashboard to have an integrated and high- level overview of the cluster agenc iessecurity posture	*Does this dashboard pertain to the SOCDashboard that shall be used by analysts?*	Yes
2	Page 4, Section VII Technical Specification. Terms of Reference, under A.1 Security Operations Center (SOC) Item 7 Monthly monitoring serv icemanagement: The service provider shall conduct regular meetings with the agencies IT stakeholders to reviewSOC performance and discuss the overall IT security posture of theagencies, including fine-tuning of configurations and provision of best practices advice, to aidin continuous improvement. Regularwritten reports must also be available to track the status of cases and the assistance needed. Monthly reports shall contain, but not limitedto:	*. Is this face-to-face meeting? Who willattend this regular meeting?*	The meeting should be face-to-face, with option to attend online. At least (2) representatives from themember agencies should attend.

ANNEX H-R

		• SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Overtime • Correlated Eventsand Rules Triggered Summary • Summary of Incident Ticket perUse Cases Incident Management		
3		Page 4, Section VII. Technical Specification Terms of Reference, under A.1 Security Operations Center (SOC) Item 8. The service provider shall ensure flexibility and scalability of the agencies SOC platform and shall ingest and process allevents sent by the agencies for the SIEM and SOAR requirements including its current and future needs.	*3.1 Can you confirm that the futureneeds is considered already in the maximum aggregate daily ingestion stated Item 4 in page 7, under A.3 Security Information and Event Management (SIEM)?* ⁴ The maximum aggregate daily ingestion that set to 3.3 pet. 	Yes. However, the member agency mayprocess separately for possible increase, if needed.
			3.2 In the event that the ACTUAL INGESTION PER DAY is MORE and EXCEEDS the stated in Item 4 in page7, under A.3 Security Information and Event Management (SIEM), what is theexpectations of the agencies on how should this be treated? *Any additional INGESTION EXCEEDING the provided INGESTION PER DAY will still be ingested with additional cost to the agency and billableto the agency and agency will process the payment.*	The oldest logs/events shall be overwritten in case the allocated storagecapacity is not sufficient to maintain the aggregate daily data ingestion. If this becomes regular and there is adetermination that there is a need to increase capacity, the same can be discussed with the agency concernedfor additional billing.

		3.3 Will SIEM log sources be centralized or accessible in Head Office?	This is not specified in the TOR. The SIEM logs for all members of the Insurance Cluster can be ingested centrally by the service provider. While all logs of the agencies will be ingested in the bidders SOC, the access of the agencies shall be segregated and limited to their agency's alerts/logs only.
4.	Page 4, Section VII. Technical Specification, under A.1 Security Operations Center (SOC) Item 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.	Can you confirm that the security briefing is included with the other reporting and meeting set on a monthly basis?	Yes.
5.	Page 4, Section VII. Technical Specification, under A.1 Security Operations Center (SOC) Item 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.	How many mobile devices are we looking at? And what are the operating systems of these endpoints?	This information will ONLY be provided to the winning bidder.

6.	Page 4-5, Section VII. Technical Specification, under A.2.1 Deployment and Management Item 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.	6.1: Kindly confirm if the non-supportedsystems mentioned above pertain to servers that have non-supported OS client.	Not just servers. It also includes the other endpoints or workstations.
		6.2: May we know the distribution of theservers in each agency, with the detailsof their VLAN, network segments and physical locations (DR and HO)?	This information will ONLY be provided to the winning bidder
		6.3: Kindly list down as well per agency,all critical applications that are running ingeographically Active-active in HO and DR, this for monitoring tools, network scanners and log collectors consideration. Item 4. The solution shall detect and prevent attacks on-premise, for supported and unsupported endpoints, including agency deployments in publicclouds, if any, such as, but not limited to Amazon Web Services (AWS), Azure, Oracle Cloud and Google Cloud.	This information will ONLY be provided to the winning bidder.
		6.4: Can we request for the breakdownof the operating systems types and version for both on-premise and cloud?	This information will ONLY be provided to the winning bidder.
7.	Page 7, Section VII. Technical Specification,under A.3 Security Information and EventManagement (SIEM) Item 9. The service provider shall ensure the availability of the ingested raw logs twelve (12) months withcomprehensive searchability. The logs,including evidence of security incidents,should be tamper proofand made available for legal and regulatorypurposes.	7.1 What do you mean on the archiving requirement? Does this mean shall we keep on storing the logs after the 12 months or we can delete it once we've extracted it after the agreed contract? What is the expected file format of the logs? Raw file type or converted to otherfile types?	The bidder shall maintain the storage ofraw logs for 12 months. Raw logs that are more 12 months will be archived andwill be given to the member agency for storage and safekeeping. The file format of the logs shall be discussed during the actual project implementationwith the member agency.
		7.2 In the case of deletion it once we'veextracted, we assume that the agency will provide a log storage for this extracted logs beyond the retention period	Yes.

ANNEX H-15

		as required. The logs beyond the retention period shall bearchived and given monthly to the agenciesin an agreed format.	
8.	Page 7, Section VII. Technical Specification,under A.4 Security Orchestration, Automation and Response (SOAR) Item 2. The solution must have visibility into the security operation provided via dashboards, KPIs andcustomizable reporting	8.1 : What are your customizable reporting?	This information will ONLY be provided to the winning bidder, and will be discussed during the project implementation with the member agency.
9.	Page 8-9, Section VII. Technical Specification, under B.1 Vulnerability Management Item 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 mightbe vulnerable to the latest Internet threats and how to protect them.	9.1: Do we refer in the table in Item 2, page 9 for the scope/coverage of the vulnerability management? 	Yes.
10.	Page 8, Section VII. Technical Specification, under B.1 Vulnerability Management Item 3 The solution should be able to scan systems anywhere in the Agencyenvironment, 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	10.1: Do the agencies have workloads incloud? Please provide list of the cloud workloads?	This information will ONLY beprovided to the winning bidder

	to create custom reports showingeach audience just the level of detail it needs to see		
11.	Page 9, Section VII. Technical Specification. under B.2 Vulnerability Assessment and Penetration Testing (VAPT) Item 2. The scope of VAPT shall be at least the following:	*11.1. Can you confirm if the external resources are web applications or a mix of application servers?* *11.2. If the external resources pertain to web applications, can we assume that the number of external resources pertain to FQDNs? If not, kindly provide the total number of FQDNs.* *11.3. We noticed that the Insurance Commission (IC) was not considered on the number of servers and desktops under page 2 and daily event logs under page 7 but here in the VAPT it was included. Is IC included in the VA PT only?*	This information will ONLY be provided to the winning bidder. This information will ONLY be provided to the winning bidder IC is not part of the project anymore. The requirement shall be: 2. The scope of VAPT shall be at least the following: | Agency	Scope
---	---
BTr	7 External resources, up to 80 IP addresses
CISS	20 External resources, 2 mobile apps, up to 90 IP addresses
SSS	25 External resources, 1 mobile app up to 150 IP addresses
PDIC	8 External resources, up to 80 IP addresses	
12.	Page 11, Section VII. Technical Specification, under C. Threat Intelligence Item 1 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	*12.1: What do you mean by "however, should the agency need additional takedowns, this will be provided by the service provider at no additional cost."? Is this the same as unlimited take down?*	Yes
13.	Page 13, Section VII. Technical Specification, under D. Incident Response Item 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.	*13.1. Are you referring to specific certifications (e.g. Computer Hacking Forensic Investigator, CompTIA, ...)* *The current standard certification validity for IT manufacturers is 3 years. Kindly consider a certification valid at the time of bid opening instead of recently trained (at least in the past 12 months)?*	Any certification related to cyber-security forensics will be accepted. We will accept a valid certification, which should indicate a validity date. Otherwise it should be issued at least in the past 12 months.

14	Page 15, Section VII. Technical Specification, under A. Access Management Item 6. The service provider shall provide physica and Environmental controls at the primary and secondary sites for this project.	14.1. Normally, the service provider takes care of its own SOC facilities. Can you explain more about this requirement?	The requirement pertains to the physical and environmental controls at the offices/building where the primary and secondary SOC is located.
15	Page 16, Section VII. Technical Specification. under C Service Provider's Qualification and Requirements Item 3. The service provider must have 24x 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.	15.1. For the required qualifications, are we pertaining to the requirements stated on the Item no. 3 below D. Personnel Qualifications / Requirements? • The service provider must be certified and should have a pool of at least 20 IT or Information Security related certified onsite support engineers. • Resume CV of ex Proposed Personnel • Company ID • Certificate of training attained	Yes.
16.	Page 16, Section VII. Technical Specification, under C Service Provider's Qualification and Requirements Item 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	16.1. Is ISO 27001 considered as equivalent third-party assessment indicating the capability of the SOC to provide the required security, scalability, stability, and high performance?	Yes

ANNEX H-18

	OR any equivalent third party assessment indicating the capability of the SOC to provide the required security, scalability, stability andhigh performance. The proof of compliance shall be submitted.		
17.	Page 37 of 64 Section VI. Schedule of Requirement and Page21, Section VII. Technical Specification,under 4. Delivery Time/Completion Schedule	*17.1: It was discussed during the pre-bidby the LBP TWG team that the license subscription will start on Day 1 of the project implementation or upon installation of the license. We wish to confirm this.*	Upon the Implementation of Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response for all the members of the Insurance Cluster.
	Phase 1 – one hundredtwenty (120) working days from the issuanceof Notice to Proceed; Phase 2 – ninety (90) working days from the issuance of Notice to Proceed. Commencement date will be from the receipt of Notice to Proceed by the winning bidder. The vendor must provide a project schedule, whichshould present the project milestones and deliverables at each milestone. License subscriptions will start upon contract implementation. Item 1. 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	*17.2: Since the ABC is a challenge, canwe request that the insurance cluster agencies consider the uniform release date of the NTP? With this, all the startand end dates of the licenses will be uniform Further, the different release dates of the NTP will have a big effect on the final cost.*	NTP shall be released by the member agency on the same date.

ANNEX H-19

	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.		
18.	Page 18 of the Terms of Reference, 6. Qualifications for Project manager Project Manager. Must have a valid project management certification	*18.1: Is this Project Management Professional Certification?*	Any valid project management certification will be accepted
19.	Others	*19.1 Due to a lot of supporting documents needed to complete the bid, can we request a 2-week extension on the bid submission and bid opening?*	The submission and opening of Bids is scheduled on October 13, 2023
20.	Others	*20.1 Aside from the Incident Manager, will you need an ITIL-certified Service Delivery engineer who will be your contact person during the 2-year contract?*	No.

ANNEX H-20

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS (OTHER BIDDERS / NAME NOT SPECIFIED)	TWG's RESPONSES
1	A.3 - SIEM, item 9.	If the raw log retention period is 12 months, what is the desired archivingperiod? 1yr	The logs beyond the retention period shall be archived and given monthly tothe agencies in an agreed format.
2.	B.1 - Vulnerability Management	Is the solution intended to be managedby the agencies? The related requirement in the TOR onlytalks about an annual VAPT, not a continuous vulnerability management service. Does it mean that the vulnerability management solution will then be operated by the agencies' respective teams?	The proposed solutions shall bemanaged by the bidder. The member agencies will manage theremediation activities to address the identified vulnerabilities. B.1.2 also states: The service providershould be able to continuously identifythreats and monitor unexpected changes in the network before they turninto breaches.
3	B.2 - VAPT, item 2.	Do all "external resources" refer to external applications? If so, how manyweb, how many mobile? Do all "IP addresses" refer to external servers? Please provide a breakdown of the types and quantities of assets to be tested.	This information is provided in B.2.2, excluding IC scope Details however, should ONLY be provided to the winningbidder.
4.	D - Incident Response,item 8.	Please clarify expected action/outputfrom "deliver network/firewall/web applications breach response".	Recommended actions/playbook for anyincident or security breach.
5.	A - Access Management. Item 1	For reconsideration. IAM must be separate from the managed securityprovider.	The requirement is not for an IAM. The specifications under Access Management pertains to the minimumrequirements on how to secure the access of the member agencies to the proposed solutions of the bidder.

ANNEX H-21

Form No. 1

BID FORM

Date : _OCTOBER 13, 2023_

Project Identification No.: LBP-HOBAC-ITB-GS-20230725-01

To: Land Bank of the Philippines
LANDBANK Plaza Building
1598 M.H. Del Pilar corner Dr. J. Quintos Streets
1004 Malate, Manila

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers *[insert numbers]*, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster in conformity with the said PBDs for the sum of:

Total Bid Amount in Words (VAT Inclusive)	Total Bid Amount in Figures (VAT Inclusive)
TWO HUNDRED NINETY-NINE MILLION NINE HUNDRED SIXTY-TWO THOUSAND EIGHT HUNDRED EIGHTY PESOS ~~ONLY~~	Php 299,962,880.00

or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: *[specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties]*, which are itemized herein or in the Price Schedules.

If our Bid is accepted, we undertake:

a. to deliver the services in accordance with the delivery period specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);

b. to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;

c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements pursuant
to the PBDs.

TRENDS & TECHNOLOGIES, INC.

The undersigned is authorized to submit the bid on behalf of *[name of the
bidder]* as evidenced by the attached/enclosed *[state the written authority]*.

NOTARIZED SECRETARY CERTIFICATE

We acknowledge that failure to sign this Bid Form, including the attached
Schedule of Prices, shall be a ground for the rejection of our bid.

Name:
WILFREDO H. AGUILAR

Legal capacity:
ACCOUNT MANAGER

Signature:

Duly authorized to sign the Bid for and on behalf of:
TRENDS & TECHNOLOGIES, INC.

Date: OCTOBER 13, 2023

Form No. 2

SCHEDULE OF PRICES
For Goods Offered from Within the Philippines

Name of Bidder _TRENDS & TECHNOLOGIES, INC._

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of Origin	Quantity	Unit Price (EXW)	Transportation and Insurance and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)
1	Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster: Bureau of Treasury	USA & PH	1,600 endpoints	₱17,620.00	₱ 0	₱2,114.40	₱ 0	₱19,734.40	₱31,575,040.00
2	Government Service Insurance System	USA & PH	4,400 endpoints	₱17,620.00	₱ 0	₱2,114.40	₱ 0	₱19,734.40	₱86,831,360.00
3	Social Security System	USA & PH	8,000 endpoints	₱17,620.00	₱ 0.	₱2,114.40	₱ 0	₱19,734.40	₱157,875,200.00

| 4 | Philippine Deposit Insurance Corporation | USG & PH | 1,200 endpoints | ₱ 17,620.00 | ₱ 0 | ₱ 2,114.40 | ₱ 0 | ₱ 19,734.40 | ₱ 23,681,280.00 |
| | TOTAL AMOUNT | | | | | | | | ₱ 209,962,880.00 |

Note: Breakdown of cost using the cost elements specified in this form should be provided.

TRENDS & TECHNOLOGIES, INC.
_____
Name of Bidder

WILFREDO N. AGUILAR
_____
Signature over Printed Name of
Authorized Representative

ACCOUNT MANAGER
_____
Position

Please credit payment to:

Account Name: TRENDS & TECHNOLOGIES, INC.
_____

Account Number: 0051-5022-56
_____

LBP Branch: BUENDIA
_____

Page 46 of 64

BILL OF QUANTITIES FORM
PROJECT: **TWO (2) YEARS SHARED CYBER DEFENSE SOLUTION FOR THE INSURANCE CLUSTER**

ITEM NO.	DESCRIPTION	QTY.	UNIT	UNIT COST	TOTAL COST
1	Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster: Bureau of Treasury Government Service Insurance System Social Security System Philippine Deposit Insurance Corporation	15,200	endpoints	₱ 19,734.40	₱ 299,962,880.00
					.
			Total Cost inclusive of VAT:		₱ 299,962,880.00

Submitted by:

TRENDS & TECHNOLOGIES INC.
Supplier

WILFREDO N. AGUILAR
Printed Name of Authorized Representative with Signature

OCTOBER 13, 2023
Date

Bank deposit mo, protektado!

NOTICE OF AWARD

15 January 2024

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

Dear **Mr. Aguilar:**

We are pleased to inform you that the financial bid for the Procurement of Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster under Project No. ITB-GS-20230725-01 is hereby awarded to **Trends and Technologies, Inc.** in the amount of Pesos: Twenty-Three Million Six Hundred Eighty-One Thousand Two Hundred Eighty and 00/100 (₱23,681,280.00).

Within ten (10) calendar days from receipt of this Notice, please submit to us the performance security in the form and amount stipulated in the Instructions to Bidders. Failure to do so shall constitute a ground for the cancellation of this award and forfeiture of your bid security.
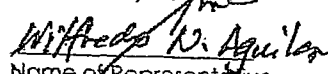
Please coordinate with Mr. Renar M. Gonzales, Department Manager, Technical Support Department, for the execution of the contract. You may reach him at rmgonzales@pdic.gov.ph or at telephone number 8841-4305.

Very truly yours,

ROBERTO B. TAN
President

Received by:

Name of Representative
Trends and Technologies, Inc.
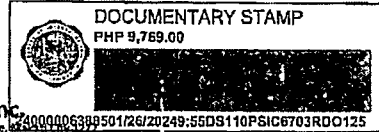Date: Jan 19, 2024

PHILIPPINE DEPOSIT INSURANCE CORPORATION
3rd - 10th Floor SSS Bldg., 6/82 Ayala Ave. corner V.A. Rufino St., Makati City 1226 Philippines

MAA General Assurance Phils., Inc.
9th, 10th & 11th Floors, Pearlbank Centre, 146 Valero Street, Salcedo Village, Makati City
TEL: (+632) 8867-2452 to 55; (+632) 7751-5759 FAX: (+632) 8893-2230

G(13) 29046

MAAGAP No.: 2024-01-00511

PERFORMANCE BOND
(For Government Project)

KNOW ALL MEN BY THESE PRESENTS:

That we, TRENDS & TECHNOLOGIES, INC. of 6th Floor Trafalgar Plaza, 105 H.V. Dela Costa St., Salcedo Village Makati City as Principal, and MAA GENERAL ASSURANCE PHILS., INC., a corporation duly organized and existing under and by virtue of the laws of the Philippines, as Surety, are held and firmly bound unto PHILIPPINE DEPOSIT INSURANCE CORPORATION as Obligee, in the sum of PESO: SEVEN MILLION ONE HUNDRED FOUR THOUSAND THREE HUNDRED EIGHTY-FOUR PESOS (PHP 7,104,384.00) ONLY, Philippine Currency; CALLABLE ON DEMAND by the Obligee for the payment of which sum, well and truly to be made, we bind ourselves, our heirs, executors, administrators, successors, and assigns jointly and severally, firmly by these presents.

WHEREAS, the Principal has been declared to fully and faithfully guarantee principals performance in connection with the Procurement of Two (2) Years Shared Cyber Defense System Solution for the Insurance Cluster under Project No. ITB-GS-20230725-01, as mentioned in the Notice of Award dated Jan. 15, 2024., copy of which is hereto attached for reference

WHEREAS, said OBLIGEE requires Principal upon receipt of the Notice of Award to post Performance Security to guarantee the faithful performance by the winning bidder of its obligations under the Contract and in accordance with the provision of R.A. No. 9184 and its implementing rules and regulations;

NOW THEREFORE, if the Principal shall well and truly perform and fulfill all the undertakings, covenants, terms, condition and agreements stipulated in the contract with the Obligee, then this obligation shall be null and void, otherwise it shall remain in full force and effect.

IN WITNESS WHEREOF, we have set our hands and signed our names on 22nd day of January, 2024 in the City of Makati, Philippines.

TRENDS & TECHNOLOGIES, INC.
TIN: 002-035-961-000
(Principal)

By: _____
SAMUEL FARO
Chairman And Chief Executive Officer

Witness to Principal

MAA GENERAL ASSURANCE PHILS., INC.
TIN: 000-801-332-000
(Surety)

By: _____
ANDRES N. VILLEGAS
Bonds Manager

ATTEST:
JAFINY TABADA
Witness to Surety

Republika ng Pilipinas
Republic of the Philippines
Kagawaran ng Pananalapi
Department of Finance
INSURANCE COMMISSION

ITO AY PATUNAY na ang *MAA GENERAL ASSURANCE PHILIPPINES, INC.*
(This is to certify that)

NG LUNGSOD NG MAKATI, PILIPINAS

na isang   pang   **DI-BUHAY**
a   *NON-LIFE*
(FIRE, MARINE, CASUALTY & SURETY)*

na kompanya ng seguro ay nakatugon sa lahat ng mga kailangang itinakda ng batas
insurance company, has complied with all requirements of law

ng Pilipinas kaugnay sa gayong mga kompanya ng seguro, kung kaya pinagkakalooban
of the Philippines relative to such insurance companies, and it is hereby granted

nitong **KATIBAYAN NG PAGKAMAYKAPANGYARIHAN** upang makipagnegosyo ng
this CERTIFICATE OF AUTHORITY to transact

uri ng seguro na itinakda sa itaas hanggang ikalabingdalawa ng hatinggabi, ng ikatatlumpu't isang
the class of insurance business above set forth until twelve o'clock midnight, on the thirty-first

araw ng Disyembre, taong dalawang libo't dalawampu't apat
day of December 2024

maliban kung agad na bawiin o pigilin ng may makatuwirang dahilan.
unless sooner revoked or suspended for cause.
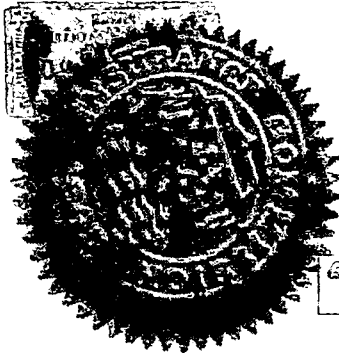
Bilang **KATUNAYAN NITO**, inilagda ko ang aking pangalan
(In WITNESS WHEREOF, I have hereunto subscribed my name

at ikinintal ang Opisyal na Tatak ng aking Tanggapan
and caused my Official Seal to be affixed

sa Lungsod ng Maynila, Pilipinas. Ito ay may bisa
at the City of Manila, Philippines. This becomes

simula ika-isa ng Enero 2022.
effective on 1 January 2022.

ANDRES N. VILLEGAS
Bonds Manager

DENNIS B. FUNA
Insurance Commissioner

*AO No. 122 issued on
July 5, 1950

Date Issued _____